

"This book will help you get the most out of your computer and serves a real need. Make sure you read it and don't just put it on the shelf!"
—Michael Schwartz, Director of Training and Certification, The Cyber Center

How to Do *Everything* with

Windows[®] XP Home Networking

Set up a wired
or wireless home
network easily

Protect your PC
from viruses, spam,
worms, and other
attacks

Keep your
personal
information
private and
secure

COVERS
WINDOWS XP
SERVICE
PACK 2



Dave Field
Andrew Brandt



Osborne

How to Do
Everything
with

Windows® XP Home Networking



This page intentionally left blank

How to Do
Everything
with

Windows® XP Home Networking

Dave Field
Andrew Brandt



McGraw-Hill/Osborne

New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
San Juan Seoul Singapore Sydney Toronto

Copyright © 2004 by McGraw-Hill Companies. All rights reserved. Manufactured in the United States of America. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

0-07-226434-9

The material in this eBook also appears in the print version of this title: 0-07-225809-8.

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill eBooks are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. For more information, please contact George Hoare, Special Sales, at george_hoare@mcgraw-hill.com or (212) 904-4069.

TERMS OF USE

This is a copyrighted work and The McGraw-Hill Companies, Inc. ("McGraw-Hill") and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." MCGRAW-HILL AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

DOI: 10.1036/0072258098



Professional



Want to learn more?

We hope you enjoy this McGraw-Hill eBook! If you'd like more information about this book, its author, or related books and websites, please [click here](#).

Dedication

To Amy, Marissa, and Shaylee
—DF

To —C, >^..^< and >(8*=
—AB

About the Authors

In the daytime **Dave Field** is a mild-mannered systems engineer. In this role he has directed the installation of entire network infrastructures at Camp Snoopy in the Mall of America using technologies such as Active Directory, Microsoft Exchange, and Microsoft SQL Server. He has been the principal architect of point-of-sale implementations, ERP roll-outs, and e-commerce initiatives.

After hours Dave becomes an author, freelance trainer, and presenter. A certified MCSA and MCSE, Dave is expert at networking technologies and support desk topics. He has delivered training at Microsoft Certified Technical Education Centers and has authored content for Microsoft and McGraw-Hill/Osborne for the MCSE, MCSA, and MCDST certifications.

By day, **Andrew Brandt** works for a major, metropolitan technology monthly. He is a Senior Associate Editor for *PC World*, where he covers the security beat, writes his monthly *Privacy Watch* column, and writes and edits numerous feature articles, news stories, and product reviews. His work has earned him awards from the American Society of Business Press Editors, the Western Publication's Association, and American Business Media.

By night, Andrew blogs, codes, and fights crime like all true geeks, in online games. In his spare moments, he operates Amishrabb.it.com, a blog site named for an over-the-top PR gimmick that dates back to the dot-com boom era. He's also a prolific science and technology pundit, and acts as spokeshuman for Bunbun, the rabbit-in-residence at Amishrabb.it. He's a part-time audio technician for Rocketwars, an Unreal 2004 mod based on the classic Segasoft game, Rocket Jockey, and he teaches pottery on Saturday afternoons. You may have also seen him playing such games as Tribes Football, Planetside, Battlefield 1942, and Tribes: Vengeance, where he uses the *nom de guerre* Spike.

About the Technical Editor

Jon L. Jacobi is a freelance technology writer, long-time *PC World* and *CNET* contributor, and software/human interface consultant. When not analyzing storage industry products or other techno-toys, he plays baseball, indulges in cross-country drives with the top down, and plays the guitar—well.

Contents at a Glance

PART I	Set Up Your Home Network	
1	Learn about Home Networks	3
2	Design Your Own Home Network	31
3	Install a Wired Network	49
4	Install a Wireless Network	79
PART II	Shut the Door on Hackers	
5	Keep Your Internet Connections Secure	107
6	Secure Your Wireless Networks	139
7	Keep Your Systems Secure with System Updates	169
8	Set Up an Effective Antivirus Solution	195
PART III	Communicate Securely	
9	Fight the Junk E-Mail Plague	231
10	Chat and Send Instant Messages Safely	263
11	Shop and Socialize Securely	293
12	Prevent Identity Theft and Protect Yourself	315
	Index	339

This page intentionally left blank

Contents

	Foreword	xv
	Acknowledgments	xvii
	Introduction	xix
PART I	Set Up Your Home Network	
CHAPTER 1	Learn about Home Networks	3
	Learn What a Home Network Is	4
	A Quick Visual Tour of a Home Network	5
	The Network You Don't See	7
	Connect Computers and More with Your Network	8
	The Role of the Internet	8
	Other Uses in the Home	12
	Home Networking Challenges	12
	Cutting Network Cost	12
	Reducing Network Complexity	13
	Components of a Network in More Detail	14
	The Three Types of Modems You'll Find Today	14
	Network Concentrators: The Heart of a Network	16
	Tie It All Together with Cables and Connectors	19
	Use Your Electrical or Telephone Cabling for Data	27
CHAPTER 2	Design Your Own Home Network	31
	Determine Your Requirements	32
	List Your Computers	32
	List Your Other Network Devices	35
	Plan for Future Expansions	35
	Select the Best Network Type for Your Home	36
	Planning Cable Routes	36
	Why Building Materials Matter	37
	Security Implications for Network Selection	38
	Distance Criteria in Network Selection	38
	When You Feel the Need for Speed	38

X How to Do Everything with Windows XP Home Networking

	Create a Physical Map of Your Network	39
	Sketch the Outline	40
	Add Your Devices to the Map	40
	Get the Numbers Right	42
	Visualize Your Signal	43
	Create a Logical Map of Your Network	45
	Determine the Placement of Concentrators	45
	Create a Network Utilization Plan	47
CHAPTER 3	Install a Wired Network	49
	Install Your Network Cabling	50
	Select Your Installation Tools	50
	Cable Pulling Techniques	54
	Connect the Cable Ends	60
	When You Just Can't Get a Cable There	61
	Connect Your Networking Equipment	62
	Configure Your Computers for Home Networking	63
	Manage TCP/IP Addressing	63
	Set Up Workgroup Networking	70
	Share Your Files and Printers	71
	Connect Your Network to the Internet	76
	Configure and Share a Direct Internet Connection	76
CHAPTER 4	Install a Wireless Network	79
	Select the Proper Wireless Ethernet Equipment	80
	Choose the Device Types for Your Home Network	80
	Choose Your Wireless Ethernet Protocol	83
	Place Your Wireless Network Devices	
	for Best Reception	85
	Sources of Radio Interference	85
	Causes of Signal Attenuation	85
	Strategies for Extending Signal Range	86
	Configure Your Wireless Network Devices	86
	Find a Clear Channel	87
	Configuring a Service Set ID (SSID)	88
	Enabling Encryption	88
	Connect Your Wireless Network to the Internet	89
	Configure Your Internet Gateway	90
	Going Online Without a Gateway	92
	Configure Your Computers for Home Networking	94
	Manage TCP/IP Addressing	94
	Set Up Workgroup Networking	99
	Share Your Files and Printers	100

PART II	Shut the Door on Hackers	
CHAPTER 5	Keep Your Internet Connections Secure	107
	Internet Security Risks for Home Networks	108
	Attacks by Viruses, Worms, Spies, and Zombies	109
	Direct Attacks from Internet Sources	110
	Use Windows XP Security Tools	
	to Protect Your Network	113
	Manage Your System's Protection with Windows XP	
	Security Center (New in SP2)	113
	Keep Patched with Updates	116
	Protect Your Addresses with Internet	
	Connection Sharing	117
	Block Hackers with Windows Firewall	118
	Analyze Your Security with the Microsoft Baseline	
	Security Analyzer	123
	Use Third-Party Security Tools	
	to Protect Your Network	128
	Use Antivirus Applications to Stop Viruses	128
	Use Antispyware Applications to Terminate Spyware	129
	Use Third-Party Internet Firewalls to Block Hackers	132
	Evaluate Your Security with Third-Party Auditing Tools	135
	Use Defense in Depth to Protect Your Systems	137
	Establish a Layered Defense	137
	Keep All Systems Up to Date	137
CHAPTER 6	Secure Your Wireless Networks	139
	Cap That Data Gusher You Call a Gateway	141
	Configure Your Wireless Network for Security	142
	Install Your Wireless Hardware with Security in Mind	143
	Configure Your Wireless Hardware	146
	Keep Your Data Secure over Your Wireless Connections	156
	WiFi Protected Access (WPA)	156
	Wired Equivalent Privacy (WEP)	160
	Filter MAC Addresses	163
CHAPTER 7	Keep Your Systems Secure with System Updates	169
	Why We Patch	170
	Types of Flaws in Computer Programs	171
	The Design/Test/Exploit/Patch/Hack Cycle	174
	Use Windows Update to Maintain	
	Your Operating System Security	175
	How Windows Update Works	175
	Use Internet Explorer to Access Windows Update	175

	Automate Operating System Patching	
	with Automatic Updates	179
	How Automatic Updates Work	180
	Configuring Automatic Updates	180
	Maintain Microsoft Applications with Updates	183
	Locate and Download Updates	
	for Microsoft Applications	183
	Use Internet Explorer to Download Office Updates	185
	Maintain Non–Microsoft Application Security	190
	Locate Security Updates for Non–Microsoft Software	190
	Apply Security Updates for Non–Microsoft Software	194
CHAPTER 8	Set Up an Effective Antivirus Solution	195
	The Role of Antivirus Solutions and Services	196
	Viruses, Worms, and Trojan Horses	196
	How Antivirus Applications Protect Your System	199
	Choose an Antivirus Solution	201
	Antivirus Solution Ratings	202
	Select the Appropriate Feature Set for Your System	202
	Trial Versions	203
	Other Antivirus Solution Purchase Options	207
	Install and Configure Your Antivirus Application	209
	Initial Installation	209
	Operate and Maintain Your Antivirus Solution	225
	Perform Manual Virus Sweeps When	
	You Suspect Malicious Activity	225
	React to Virus Outbreaks with Manual Updates	226
	What to Do When You Find a Live Virus	226
	What to Do When You Suspect a Virus	227
PART III	Communicate Securely	
CHAPTER 9	Fight the Junk E-Mail Plague	231
	Put an End to Your Spam Problem	232
	Defend Your Inbox, Lest You Drown in Spam	232
	Fight Spam on Your Terms, on Your Turf	233
	Avoid Getting Spam in the First Place	233
	Develop Habits That Will Protect Your E-Mail Address	234
	Skip Online Activities That Make You More Likely	
	to Get Spam	235
	Ditch Your Extremely Spammy Identity	236
	Filter Spam on Your PC	236
	Try the Software That’s Free,	
	or That You’ve Already Got	237
	Shop Around for a Good Spam Filter	240

	Get Started with Cloudmark's SpamNet	241
	Install and Run Sunbelt Software's iHateSpam	244
	Get Rid of Spam with Less Effort	249
	Let Your ISP Filter Your Mail for You	249
	Report Spam to the Authorities	251
	Spam Fighting Looks Toward the Future	256
	Antispam Legislation Gets Tough	256
	Spam Fighters Take Legal Action	257
	Spammers Turn Up the Heat, and Fight Back	258
CHAPTER 10	Chat and Send Instant Messages Safely	263
	Use Instant Messaging and Chat Wisely	264
	Evaluate the Risk IM and IRC Pose to You	265
	Determine Whether the Risk of Chatting Is Worth the Benefits	265
	Secure Your Instant Messaging (IM) and Chat Applications	266
	Get an IM or Chat Client Application	266
	Stop Viruses, Trojans, and Worms	270
	Prevent Spim from Reaching Your IM Buddy List	275
	Update Your IM Client when New Software is Available ...	277
	Preserve Your IM Settings, Contact Lists, and Conversation Logs	279
	Defend Your Privacy in Chat and IM	281
	Who Wants Your Name?	282
	Apply Common Sense Liberally	283
	Handle Chat and IM Security Issues	285
	Avoid Chat- and IM-Borne Malware	285
	Prevent Stalking and Threats in Chat and IM	291
CHAPTER 11	Shop and Socialize Securely	293
	Shop Online Safely	294
	Verify Security Before You Shop	294
	Read and Understand Web Site Privacy Policy Legalese ...	301
	Protect Your Credit Cards Online	307
	Safely Socialize Online	309
	Rules of the Road for Social Networks	310
	Maintain Your Privacy While Job Hunting	311
	Know Your Résumé Site	311
	Dos and Don'ts for Self-Hosted Résumés	313
CHAPTER 12	Prevent Identity Theft and Protect Yourself	315
	Keep Identity Thieves Away from Your Data	316
	Safeguard Your Information Before Thieves Strike	317

Terminate an Identity Theft Case	325
Protect Your Identity if Fraud Hits Your Accounts	325
Protect Your Sensitive Data Online	
and on Your PC	329
Keep Private Information about Yourself to Yourself	329
Perform “Vanity Searches” and Unlist Yourself	330
Steer Clear of Phishing Scams	333
Index	339

Foreword

Windows XP has evolved from more than a decade of continued windows development. During this time, Microsoft has been committed to understanding and meeting the diverse needs of its customers, and XP is a truly usable operating system with unsurpassed functionality. Windows XP is the foremost desktop operating system all over the world. If one thing is missing though, it would be proper security. One of the most common things I hear from government and industry leaders is that there needs to be clear guidance, especially security guidance, for home and small office users for their PCs. By the time this book is printed, XP Service Pack 2 will be released and that will be a major step to meet the needs of Microsoft's customers to make their lives better, safer, and their work easier.

David Field proposed a textbook to Osborne to cover Internet security topics including anti-virus, personal firewalls, spam, and spyware. The original concept for the book was to be all security. Upon further reflection, Osborne felt readers wanted a broader coverage, covering topics such as home networking. The Windows XP operating system easily adapts to most networking solutions, but it helps to have a design or recipe showing technologies and tools such as wireless, cable, and DSL modems.

Andy Brandt from *PC World* joined the project to help make the book richer than just security, to be a real how-to for home and small-office users. Andy adds tremendous enthusiasm and knowledge to the project also, and the combination is a great team.

I'd like to extend congratulations to David and Andy for producing a truly useful book, a book that goes beyond telling the reader *about* things, but one that tells the reader *how to do* things. This book is an invaluable resource for both beginners and computing professionals and all levels in between. There's no better guide for learning and mastering how to put Windows XP to work. It will be another fine book in Osborne's "How to do Everything" series.

What this has evolved into is 12 chapters ranging from anti-spyware to wiring the walls to privacy and identity protection. The chapters are written in a modular fashion—the information you need is right there, so you don't have to keep skipping around. The book was written to the soon-to-be-released Service Pack 2, so it will be up to date for more than a year.

This is a book that will find a place within arms reach of your computer. I've been using Windows operating systems since Windows 3.1 and XP is by far my favorite; everything is intuitive. This book will help you get the most out of your computer, and serves a real need. Make sure you read it and don't just put it on the shelf!

*Essentially yours,
Stephen Northcutt,
Director of Training and Certification
The SANS Institute
August 2004*

Acknowledgments

Let me begin by thanking the ones who helped me the most with this work. Without the encouragement, support, and tolerance of my wife and girls, I would not have been able to do this. They inspire me to do the best job I can and find me the time to do it.

To Megg, Agatha, Julie, Carolyn, Jody, Bob, and the others at Osborne: Thanks for helping us shape this work into something we can all learn from. Thanks to my co-author Andy Brandt for his advice, assistance, and especially his contacts. Thanks to Jon Jacobi of *PC World* for keeping our facts straight and to Bob Hillery of IntelGuardians for lending his voice to our work. Thanks, Stephen Northcutt of Sans Institute for your time and encouragement. Finally, thanks to Laura, Stacey, Sherry, Jackie, Katrina, and the others at Studio B for letting me keep writing on my mind.

—Dave Field

I've got to thank Clare, not only for tolerating extended late-night writing sessions, but for doing a hundred different supportive things a day, and for being the supra-genius editor-writer-designer that she is. I'd also like to thank *PC World* for paying me to do, and write about, some of the fun, offbeat technology stuff I also happen to love.

My editors at OMH have been a terrific source of insight and a fount of ideas for which I'm grateful. I also want to thank Bob Garza for giving me a shove into the world of tech books (and indoor skydiving), and Dave Field for being such a networking *mensch*. Michael Lasky let me put sample chapters on the *PC World* cover disc, fulfilled my incessant battery requests, and repeatedly told me my second-favorite joke, which still makes me smile.

Finally, I've got a huge list of family, friends, and Internet acquaintances to thank, not only for their support and enthusiasm over this project, but also for putting up with my absence while I spent my every waking moment working on this book. I can't name every one of you, just out of the environmental considerations of using all that ink, but you know who you are. I owe each of you a cookie (or, depending on what species you are, a carrot).

—Andrew Brandt

Introduction

You have more than one computer. You wanted to get some work done one night and the kids were playing a game or doing homework. Next thing you know, you have a PC in the office, one in the kids' room, and your spouse is beginning to bring a laptop home from work. The kids want to use your printer, you wouldn't mind working from home more and not being chained in the office, and everyone wants the Internet. You need a home network. You've been to various computer stores to look for ways to accomplish this. The boys (and girls) in blue/red/yellow have varying opinions on what you should do, and you have decided it may be wise to do a bit of research before you dive in.

We have all been there; some from the consumer side, some from the information technology side. We write this for all those who have asked us over the years to give advice on "Which is the best network equipment to buy?", "How do I install a wireless gateway?," "Which anti-virus should I get?" We also write this for those who don't have a computer guy next door to ask. Most of all we write this to begin a groundswell of resistance to the forces that are damaging the Internet and rendering it less useful due to their antics. If enough home users learn to protect their systems, some of the tools the hackers use will be less effective and Internet weather patterns will improve for everyone.

This book is written in chapters that can be taken alone or read from front to back. You will begin by learning the basic network concepts and terminologies. Then you'll design a network from the ground up, both wired and wireless. You'll install the network and connect it to the Internet. We will help you with Internet and wireless network security, show you how to keep your systems and data safe from hackers and viruses while you're online, help you defeat junk e-mail, and give you tips on how to protect your privacy and your identity while shopping and communicating with others.

To bring important information to your attention, we've included short Notes, Tips, and Cautions throughout the book. In addition, "Voices from the Community" sidebars are interviews featuring normal people discussing topics related to security

XX How to Do Everything with Windows XP Home Networking

and home networking. Finally, the spotlight section in the center of this book profiles the latest developments in wireless networking and describes the best ways to create, protect, and manage your passwords.

If you are beginning from scratch, just work your way through with us, and we will give you advice and guidance as you go. If you need to solve a specific problem, find it in the index and we should be able to help you. Most of all, feel free to skip around to what interests you most. You understand best what your needs are and what you are most interested in, and we will be here with the rest when the need arises.

Part I

Set Up Your Home Network



This page intentionally left blank

Chapter 1

Learn about Home Networks



How to...

- Explain what a network is
- Define what a network does
- Identify components of a network
- Meet the challenges of home networking
- Understand home networking in greater detail

In this book we will help you learn the best way to network computers and peripherals in your home or small office. You may already know in broad terms how a network works. You may, in fact, already know in specific terms how a network works and want to brush up on networking technologies that have been specifically designed for the home user. Whatever your prior knowledge of this topic, prepare to fill in the blanks and along the way learn what works best for your specific networking needs.

You'll begin by learning the role of a network in a home and how it accomplishes its work. Next, we'll dig into networking components, describing each type of component and where it is to be used. By the end of this chapter, we will have demystified networks somewhat. Prepare in following chapters to drill in on specific technologies and deepen your understanding of how they can be used in your home network.

Learn What a Home Network Is

In its most elemental sense, a computer network is simply a collection of computers connected together to share files and peripherals such as printers. Many among us have heard accounts of the complex systems of electronic components and miles of cabling that go into creating corporate networks. There are some of us (present company included) that have even devoted the better part of their careers to getting these colossal rat's nests to do meaningful work.

Everybody knows someone who "works with computers." We have called him or her in the evening to ask how the kids are doing, how the car is running, how to rig an Ethernet hub... Having been on the receiving end of these calls, we appreciate the frustration of those who have made them. If you wanted to make a career of this, you would have done so long before buying the component you are calling about. It should not be this hard.

In recent years manufacturers of networking equipment have made great strides in creating devices that work well together and are easier to set up and operate. For example, network protocols support automatic configuration, computer operating systems automatically configure basic network settings, and networking devices come with big illustrated posters showing how they fit in with the other devices already resident on the network.

You will build on this new technology to gain the knowledge and confidence to help you make the most of it and possibly even become one of those who get the evening telephone calls!

A Quick Visual Tour of a Home Network

As we zoom in on the network, we see it is merely a collection of computers or PDAs (personal digital assistants) that connect to each other or to a central network device called a *concentrator*. The connections may be by means of cable or, more recently, by radio waves. An example of this may be seen in Figure 1-1. This drawing depicts a small home network installation that allows a personal computer, a notebook computer, and a PDA to share a printer and an Internet connection.

Networks allow individuals and corporations to connect computers to each other to share data and peripheral devices. Sharing a single printer among the members of a family can save hundreds of dollars that would have to be spent if each computer

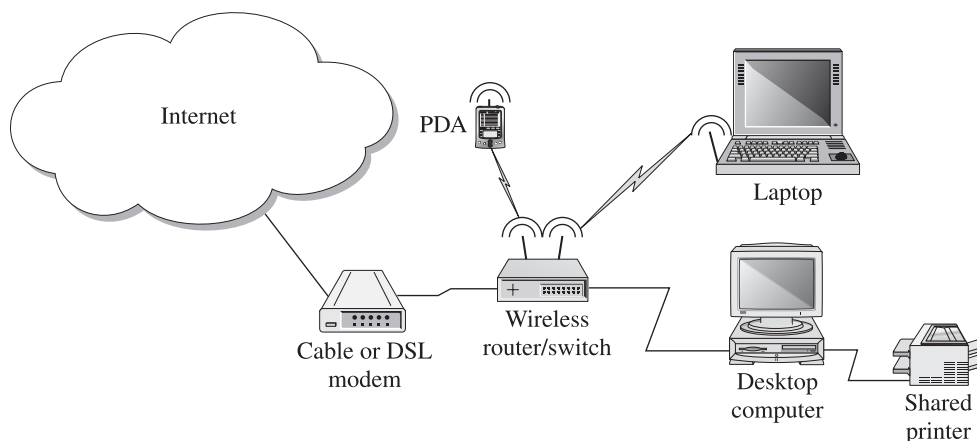


FIGURE 1-1 A thumbnail sketch of a network

6 How to Do Everything with Windows XP Home Networking

had its own printer. Sharing an Internet connection is also an excellent way to save money. A network that connects computers to each other in a house or office building is known as a *local area network*, or LAN.

In addition to connecting nearby computers to each other, networks have evolved into structures capable of supporting far-flung sales forces, global corporations, and giant networks of game players. These large networks are known as *wide area networks*, or WANs. The Internet is an example of a very large WAN.

What Your Modem (Modulator/Demodulator) Does

Communication with a provider of Internet services is accomplished by a device that modulates data signals into electronic pulses that are able to transit some distance to the provider's Internet facilities. The actual type of modem used will depend on the speed of the service you are connecting to. High-speed Internet services use cable or Digital Subscriber Line (DSL) modems to connect computers and home networks to the Internet. Lower-speed services might use (slower) dial-up modems to provide Internet access.

What the Router (Gateway) Does

Most network designs use a *concentrator* to allow the connection of devices at a central point. A concentrator can be any device that serves this purpose. Examples of concentrators are hubs, switches, and routers (also known as gateways). In Figure 1-1, the function of the concentrator is served by a combination router/switch. This device consolidates the network connections and serves as the connection point to the Internet service. Many manufacturers build gateway devices that are able to manage network addressing, protect against intrusions from the Internet (firewall), and communicate with both wired and wireless networking devices (wireless access point).

The Role of Computers and PDAs

Computers are still the mainstay of network communications. We increasingly use computers to manage our finances, shop, play, work, and even order pizza. Our children are growing up in a world where instant communication is taken for granted. Actions that would have branded us as some sort of computer geek are now commonly performed by five-year-olds.

Computers are the primary data storage and management devices on the network, sharing files with other computers and devices on the network. They also provide the principal means of managing the network. Many of the more complex network devices provide interfaces for managing their settings by using a computer connected to the device with a cable or by connecting to the device over the network.

PDAs have been widely adopted for business and personal use. Calendars, contact lists, messaging, and Internet access can be consolidated in these devices. Having the proper infrastructure available at home enables messaging and applications from work to be available. As more of us telecommute, this becomes an important reason for the home network to support these technologies.

The Network You Don't See

A network relies on more than just the hardware you see when you look around the room. Each computer runs an operating system that manages its communications. Each network device must be assigned a unique address in the network. Networks use protocols to control delivery of information. We'll begin here by describing the role of the operating system, and then we'll speak a little about addresses and protocols. In later chapters, we'll cover each of these items in much more depth.

Computer Operating Systems Are a Vital Part of a Network

The ability to make sense of the devices and addresses in a network depends on the facilities of an operating system. As a computer user, you may be familiar with the role of an operating system in managing files and applications on a computer. Operating systems in general, and Microsoft Windows XP in particular, are also capable of managing communications and resources across a network as well. Referring back to Figure 1-1, Windows XP running on the desktop computer and the notebook computer is able to share the desktop computer's printer with applications running on the notebook computer. This allows the family to share one print device with multiple computers. The resulting cost savings is just one of the advantages of using a network in the home.

Each Device Needs an Address

Devices on networks need unique addresses that allow other devices to direct communications to them when necessary. Some of these addresses are local and can be reached only by devices on the same network, while some reside on other networks around the world and can be reached via the global Internet.

Protocols Define Communications

Network equipment manufacturers belong to groups that control communication standards for the various networking technologies. These standards are known as *protocols*. Some protocols control electrical signaling on the actual cable, while others control more intangible aspects of communication such as data integrity or encryption. The Internet itself uses a suite of communication protocols to control

delivery of data on a global scale. You will learn how to configure these protocols later when you consider the actual installation of your network.

Connect Computers and More with Your Network

Networks transport, organize, and secure data. They carry documents, messages, voice, video, music, and games. Since the creation of the Internet, there have been many changes in the types and amounts of data carried on the cables. It is certain there will continue to be many more changes as more of us get online and use networks in different ways.

In the home, a network can form the backbone for all the home's information-sharing appliances, enabling communication both within the home and outside the home via Internet connections. It can be the conduit for home control systems, home security systems, and audio/video/voice distribution systems.

The Role of the Internet

The global Internet is the largest network in the world. It serves the purpose of connecting millions of networked computers and other devices to each other in a vast mesh of interconnected networks. Those who work and play in this digital expanse use a staggering array of different applications and tools. Among these are web browsers for the World Wide Web, newsreaders for participating in discussion networks referred to as newsgroups, e-mail applications for sending and receiving messages, and various real-time chat clients for those who want to interact spontaneously.

Find Information on Web sites

The global Internet forms a lattice of interconnecting networks dotted with millions of computers. Many of these computers participate in the World Wide Web. *Web servers* serve up information on virtually any topic that one can imagine. Data on these servers is organized into hierarchical directories called *web sites*. Internet search services such as Yahoo! and Google catalog these web sites, allowing those looking for information to search by keyword or phrase (see Figure 1-2). Web clients or *browsers* access this information and present it as a series of hyperlinked documents called *web pages*. The hyperlinks in these web pages contain pointers to other pages creating, in effect, a vast web of interconnected information.

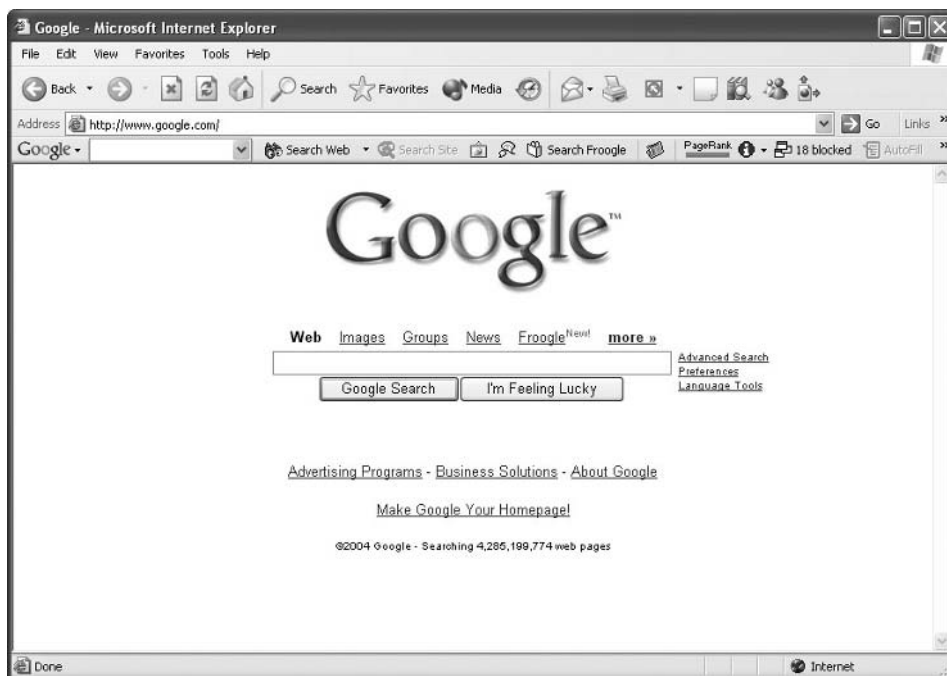


FIGURE 1-2 Google is one of many services used to search the Internet

The explosion of information on the Internet has given rise to a number of industries, many of which we will touch on in this book. Chief among these are the providers of security services designed to protect our computers and networks from those who have a little too much time on their hands.

Discuss Your Interests on Newsgroups and Mailing Lists

Internet *newsgroups* are discussion forums that allow users to maintain public discussions on topics of their choice. These discussions are typically organized into threads (sequences of messages, responses to those messages, and so on) based on their content. This allows users to quickly locate items of interest. Newsreaders are designed to facilitate the use of these forums.

Mailing lists are similar to newsgroups in that they allow threaded discussion, but they are typically hosted by an organization that maintains tighter control over the content of the messages. List servers are configured to allow interested parties to register their e-mail addresses for inclusion in the list's mailings.

Keep in Touch with Text and Instant Messaging

Common messaging applications include e-mail and instant messaging. *E-mail* has become an inexpensive way for businesses and individuals to communicate with each other. The cost of using e-mail services is relatively low when compared to any other communication method that offers similar immediacy.



You probably have heard of MSN Messenger or AOL Instant Messenger (AIM). These are examples of real-time messaging applications that allow their users to *interact* with each other across the Internet. Many instant messaging (IM) applications also support voice communication over the Internet as well.

Join the Crowd with Chat

There are many other ways to interact with others on the Internet in real time. Probably the most familiar to Internet users is *chat*. Chat differs from Instant Messaging mainly in its ability to support many users in organized chat rooms rather than ad hoc sessions. Many chat networks exist, but most are based on Internet Relay Chat (IRC). IRC is a collection of networks that communicate using the IRC protocol. Each network hosts from tens to thousands of chat rooms. Having many servers for each network provides a redundancy that ensures the network is always available and that a nearby connection point exists in most areas to support clients.

IRC clients range from computer applications controlled by the user to web-based applications that use the IRC infrastructure to provide more restrictive access to chat rooms approved by the web site administrator.

Go Multimedia with Voice, Video, Music, and Games

Another popular use of a network involves the transmission of voice, video, or music over the network. These types of transmissions are broadcast in real time as they occur. This type of transmission is called a *stream*. Systems that carry data in this manner are referred to as *streaming media*. Radio stations broadcast their programs across the Internet; businesses conduct videophone calls and product demonstrations; overseas military personnel phone home across the Internet. In fact, the Voice over Internet Protocol (VoIP) is generating a lot of buzz right now as a potential replacement for local and long-distance telephone carriers. Figure 1-3 depicts the web site of a maker of Internet phone equipment.

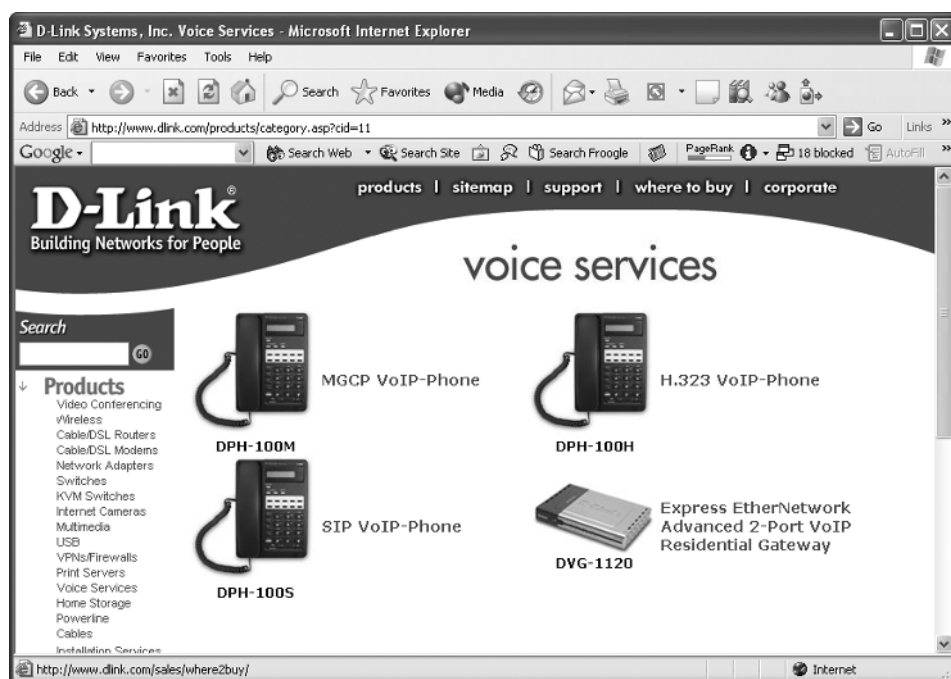


FIGURE 1-3 Web site of VoIP product manufacturer D-Link Systems

Did you
know?

Celebrities Play Bridge Online

Bill Gates, co-founder and Chief Software Architect of Microsoft, is an avid bridge player. He also enjoys playing bridge online and has been known to challenge fellow billionaire Warren Buffet to a regular Saturday online bridge match.

A quick visit recently to MSN Games by Zone.com found over 118,000 active game players online, including over 1,450 bridge players!

Online gaming has also gained a lot of momentum. Neighbors are installing wireless networks to allow the kids to play computer games. Internet-enabled computer games like EverQuest (also known as EQ) allow thousands of players to participate in virtual worlds. Other game portals such as MSN Games by Zone.com provide more familiar games such as backgammon, chess, and bridge.

Other Uses in the Home

Recently, there has been an explosion of network devices for wireless networks. Media-sharing devices for home entertainment, video cameras, data storage devices, game-sharing devices—the list is growing daily. This segment of the market is expanding so rapidly that we have dedicated a section of this book to these emerging technologies. For more information on these devices, see the spotlight section in the center of the book.

Home Networking Challenges

Perhaps the greatest challenges to those implementing home networks are the lack of deep pockets and the complexity of getting a collection of different devices to communicate with each other.

Cutting Network Cost

In the past, networking equipment was too expensive to be cost-effective for home use. Of course there were always those who needed home networks for business purposes, or who had to have the latest and greatest of everything. The rest of us

just made do with a floppy disk or maybe a data link cable connecting your computers to each other via serial, parallel, or USB ports.

Lately, the network equipment that has become a commodity item for corporate buyers is now also within the budget of many homeowners. Depending on how many devices you are connecting, wired networks can be set up for less than \$100U.S., wireless for under \$150. At these prices the savings on shared Internet services or shared peripherals can easily justify the cost.

Reducing Network Complexity

Getting two or more computers to communicate with each other can be an interesting diversion. Prior to Windows XP, it could take hours just to get all the correct device drivers installed and to configure the communication protocols. Only computer enthusiasts or those who absolutely had to have a home network would want to spend the time and effort. There were .ini files to edit, entries to place in the startup files config.sys and autoexec.bat, and command lines to learn. (Oh, and don't forget to configure protocol.ini, win.ini, and system.ini in Windows!) If the planets were aligned and the OS didn't collapse under the weight of all the real-mode drivers, you might get your two computers to talk to each other. Want to connect to the office network to catch up and do a little work from home? Best to just have the IT guy out to the house for that one!

Beginning with Windows 95, this all began to get easier. Microsoft finally began to get the idea that the Internet was going to be the next big thing. Windows 95 drew Internet protocols deep into the operating system. Applications such as America Online appeared to use the new graphical user interface to put a friendly face on online communications. Netscape Navigator and Internet Explorer made it possible to access thousands (yes, only thousands) of web sites. Incremental changes were made to the friendliness and stability of Windows. Windows 95 OSR2 and Windows 98/98SE were better and more stable. Windows 2000 was much more stable (and much more expensive). Windows Millennium (Windows Me) was best forgotten.

Finally, Windows XP arrived to bring together the stability of Windows 2000 and the price and friendliness of Windows 98. Windows XP Home Edition can now scan your hardware, make itself at home, connect you to your home network, and even connect to the Internet with very little direct intervention. If you know your Internet account settings (provided by your Internet provider), you can be online 30 minutes out of the box! If you do not have an Internet provider, one can be selected and configured from the collection of online services that ship with virtually every PC. In that case, you'll need slightly more time, say an hour?

With all this ease of use, you might begin to wonder why you bothered to pick up this book. Rest assured we fully intend to earn our keep here. The ease of configuration experienced by users of Windows XP has not been fully realized in the rest of the networking world. There are still addressing and configuration of network devices to attend to. Security (or the lack thereof) has also received much attention lately due to high-profile attacks on web sites and the explosion of Internet worms and viruses. As we progress with this book, you will learn how to protect your computers and network from these attacks and how to avoid becoming the launch pad for other, even more destructive attacks against corporate and government targets. You will also learn how to protect your financial and personal data from those who would misuse it.

Components of a Network in More Detail

We skimmed over the components of a typical home network just a few pages ago. Now we will spend more time drilling down onto each type of equipment so that you can begin to determine which are more suitable for use in your own network.

The Three Types of Modems You'll Find Today

There are basically three types of modems in widespread use today: cable modems, DSL modems, and dial-up modems. The feature they all have in common is the ability to convert digital data from your computer or network to analog electrical signals suitable for transmission over long distances to your chosen Internet provider.

If You Have Cable Service, Cable Modems Are Fastest

Designed to provide Internet services over the same cable systems that bring you television, cable modems connect your computer or network to similar equipment on the cable television company's "head end." Typical connection speeds for cable Internet subscribers often exceed 2 Megabits/sec (two million bits per second). This is significantly faster than speeds available on DSL services for similar prices. One drawback often cited by DSL providers competing with cable for your business is the sharing of bandwidth by all cable Internet subscribers in a given area. It is possible for users to experience slowdowns during times of peak usage.

Most cable modems are certified to the Data Over Cable Service Interface Specification (DOCSIS). This ensures they will interface to most cable company

equipment. The cost for a typical cable modem runs \$60–100. Most cable Internet providers will also rent modems for a nominal fee.

1



DSL Modems Are Fast Too, but Limited in Range

Digital Subscriber Line services provide high-speed connections over a telephone company's existing copper cable networks. Users of DSL report dramatically faster connections than experienced by dial-up users, all without interfering with voice communication on the same line. There are two “flavors” of DSL. Synchronous DSL (SDSL) offers equal speeds for traffic to and from the Internet. Asynchronous DSL (ADSL) offers faster speeds from the Internet than are available to the Internet. Most home DSL services use ADSL for its higher download speeds. ADSL download speeds vary from a low of 256 Kbps (kilobits per second) up to 7 Mbps (megabits per second). Upload speeds peak at 1 Mbps. These speeds are optimal, of course. DSL services are provisioned by the provider to use their networks most efficiently. It is possible at times to experience somewhat less than the rated speed of the service. Your speed will also depend on your distance from a central office. If you're too far away, you may not even be able to receive DSL service.

Like cable modems, DSL modems must conform to signaling standards. There is no single standard, however, so it is always best to check with your DSL provider before purchasing your own modem. Cost for DSL modems is similarly erratic, ranging from a low of \$30 to a high of over \$500, depending on speed, features, and availability.

Dial-Up Modems, Still There When You Need Them

Ah, dial-up modems, the old standby! With all the high-speed options available to us, you might think dial-up modems would be falling out of favor. Unfortunately,

only about one in five American (and fewer European) households have access to high-speed Internet services. If you are not one of the lucky ones, dial-up is still your best bet. There are wireless services, and even satellite services, but these remain out of reach for many budgets.

Dial-up modems are easy to configure, are easy to use, and can connect to Internet providers from virtually anywhere.

Most computers are delivered with a dial-up modem already installed. Windows XP will already have detected it, have the correct drivers, and be waiting for the phone number and password of your Internet provider.

Network Concentrators: The Heart of a Network

Concentrators allow the connection of network devices at a central point. They orchestrate the communication of all the devices on the network, functioning as an electronic traffic cop, directing devices signaling to prevent excessive collision of data. Network hubs, switches, wireless access points, and Internet gateways all are examples of concentrators. While there are other types of networks available, for simplicity and affordability we will concentrate on Ethernet in our home network. Wired Ethernet hubs are available for less than \$50, and network adapters for Ethernet are available for as little as \$20. In addition, many new computers have an Ethernet adapter already integrated or installed.

Interconnect Your Devices with Hubs

Hubs electrically connect several computers or other network devices to each other. The most basic hubs merely splice the connections into the network, while more advanced hubs are able to sense problems with cables or devices and *partition*, or separate, them from the rest of the network to prevent widespread interference from the faulty device. The most advanced hubs offer features such as switching and crossover detection to facilitate better interconnectivity with the larger network.

Ethernet hubs allow the interconnection of several network devices. Each device can see the others, and they all share a *segment* of the overall network. Ethernet uses a signaling technology known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Briefly, what this means is that each device checks the channel before transmitting (carrier sense). In the unlikely event two devices begin to talk at the exact same instant, they each stop and wait for a random interval (measured in milliseconds) and check the line again. If it is clear, they begin to transmit again.



Limit Network Collisions with Switches

For smaller networks (less than 200 networked devices), hubs are perfectly acceptable. As networks grow, however, the ability for all devices to see each other begins to cause problems. As more devices are added, collisions happen more frequently until the network finally grows to the extent that some computers cannot get a word in edgewise. When this happens, we install a *switch*.

Externally, a switch looks like a hub. It also performs substantially the same task as a hub, with one important difference. Switches are designed to separate their ports from each other, creating—in effect—several small network segments, each with a separate *collision domain*. A computer on a switch port will never sense another computer talking, as it will seem to be alone on the network. The switch acts as a sort of traffic manager, delaying some traffic just long enough for all to transmit without collisions. Many Internet gateway products incorporate switch technology into their wired connection ports.

Wireless Access Points: Hubs Without Wires

Wireless access points (WAPs) connect wireless network devices by radio in much the same way a hub connects wired devices into a network. The access point communicates over a specified radio frequency with other devices using the same frequency and protocol. WAPs currently use one of three communication standards: 802.11b, 802.11g, and 802.11a.



802.11b The most familiar (and least expensive) of the WAP standards is 802.11b. This standard supports data rates of up to 11 Mbps and provides for communication over 11 different radio frequencies or channels in the 2.4 GHz band. However, appliances that operate at the same frequencies, such as microwave ovens and cordless phones, can interfere with 802.11b signals.

Also, as more devices are added to the network and distances between devices and the access point increase, the network steps down data rates to ensure reliable communications. In a busy network it is not uncommon to see data rates as low as 1 Mbps. The 802.11b standard supports connections between devices as far as 300 feet apart.

802.11g Devices based on the 802.11g standard are growing in popularity and dropping in price. Supporting higher, 54 Mbps data rates, this is becoming the new standard for wireless networks. It operates at the same frequency as 802.11b and is therefore subject to some of the same interference issues. It is common to find wireless devices that incorporate both 802.11b and 802.11g technology.

802.11a Capable of operating at a data rate of 54 Mbps, 802.11a uses a federally regulated radio frequency in the 5 GHz band and therefore is more expensive and not as widely used. Using a different frequency range than 802.11b and 802.11g, it suffers less from radio interference. The range of the radio signal is somewhat less due to the weaker penetration capabilities of the higher-frequency signal. The 802.11a standard has found a niche in locations that have significant interference at the 2.4 GHz range.

Internet Gateways Connect Your Network to the Internet

Internet gateways combine the best of switch and/or WAP technology with Internet security features. Principal among these are Network Address Translation (NAT) and firewall functionality. Network Address Translation uses the address of the gateway in all Internet communication, hiding your true address from those on the Internet and affording a measure of protection to your computer. Firewalls block uninvited connections from the Internet, protecting your computers and devices from attempts to access and control them from outside your network.

One device provides your network with Internet connectivity and a built-in concentrator. Some gateways even operate as print servers, which are devices that allow the direct connection and sharing of a printer with computers on your network.

**NOTE**

Occasionally you will hear a gateway referred to as a router. These are perfectly interchangeable terms for this device.

Tie It All Together with Cables and Connectors

As we consider a wired network, we will be describing the Category 5 cable standard. There are other newer standards such as Cat5e and Cat6, but they are incremental improvements to Cat5 and are necessary only when using super-high-speed Ethernet in the Gigabit and 10 Gigabit ranges. These networks are still firmly in the domain of corporate backbone networks and will not have an application in the home for some time to come.

NOTE

For a discussion of Ethernet speeds, see the section titled “When You Feel the Need for Speed” in Chapter 2.

Most Wired Installations Use Category 5 Cable

Supporting transmission distances of up to 100 meters (328 feet), Cat5 cable uses four twisted pairs of copper wire to carry electrical signals from one device to another. This cable is available in precut lengths of 3–100 feet at your local computer store and by the 1000-foot box from online retailers and local home centers.

TIP

Try going to Froogle.com and searching on Cat5 to get a huge list of available cables, connectors, and accessories.

The connectors on the end of each cable are classified as RJ-45 (or Registered Jack type 45) and are of the same family of connectors used for telephones. They are crimped on with a special tool available from the place you bought your cable.

For most uses, however, you should be able to work with cables that are pre-cut to specific lengths with connectors already attached (pre-terminated). This makes it much simpler to get your network up and running.

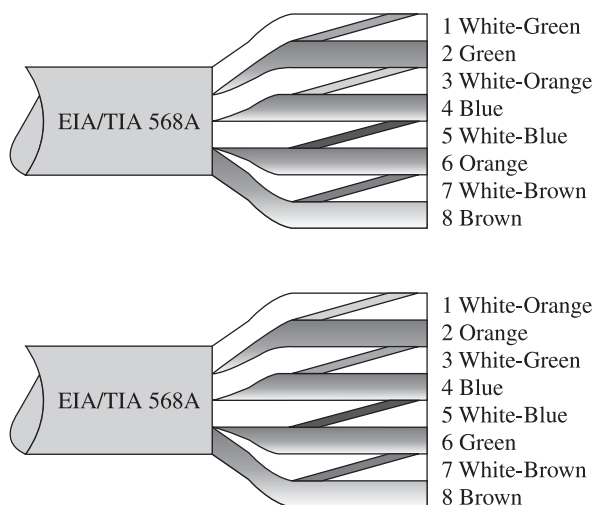
NOTE

If you find it necessary to cut and terminate your own cables (you are pre-wiring your house, or you really hate having an extra two feet of cable to loop up somewhere), read on. If you plan to use pre-terminated cables, you can skip down to the section titled “How to Install Your Category 5 Cabling Without Special Tools” later in this chapter. If you are the type who still wants to know how all this works, stay around; we won’t be long.

The Characteristics of Category 5 Cable Cat5 cables have special characteristics for wire size and number of times each pair is twisted per one inch. These characteristics are designed to not allow the individual wires to run right alongside each other for too great a distance. The twist keeps the wires in different positions relative to each other to keep this from happening. If they are allowed to lie alongside each other for too great a distance, there is an opportunity for signals from one wire to interfere with signals from another. This phenomenon is known as *crosstalk*. If there is too much crosstalk in a cable, there will be degradation of the signal and corresponding loss of data throughput. The Cat5 standard dictates that individual pairs may not run more than 1/2 inch without a twist. It is important to ensure this is maintained even into a connector in a wall jack. Only untwist enough to get the wires into their slots.

When running cable through your home, avoid sharp bends or kinks in the cable. Do not staple the cable tightly to any structure, either. These variations in cable geometry can cause disturbances of the data signal, resulting in degraded performance

Category 5 Color Codes Help Us Connect Cables Properly Category 5 cables are color-coded to indicate pair relationships. The transmit (Tx) lines from one Ethernet device must be connected to the receive (Rx) lines of another. The color codes are used to help sort out the wires on either end. There are two color code standards, EIA/TIA 586A (T568A) and EIA/IA 586B (T568B). Figure 1-4 shows the color layout for each standard. They are identical except for the green and orange wires, which are exactly opposite between the two standards. There doesn’t appear to be anything other than a love of complexity behind the difference; both standards pass the connection straight through to the other end. For consistency, most cabling

**FIGURE 1-4** Category 5 color codes

installers will use the T568A standard for their in-wall connections. You'll find the cables that connect your devices to the wall (patch cables), which you can buy from most stores, use the T568B code. There are no concerns with interconnection of T568A and T568B standards as long as both ends of each individual cable use the same standard.

If you terminate your own connections, be sure to choose wall jacks that have color-coded connectors. You will only need to match the wire colors up with the color map on the jack.

Tips for Installing Category 5 Cable It may be a challenge in a finished house to get cable from one room to another. In this section we will provide a few tips and tricks for getting cable where it needs to be. Keep in mind that we now have many options when networking a home. If it appears too difficult to get cable where you need it, you have power line and phone line network options, as well as wireless network equipment.

NOTE

Chapter 3 will go into much greater depth about installing Category 5 cable systems in your home.

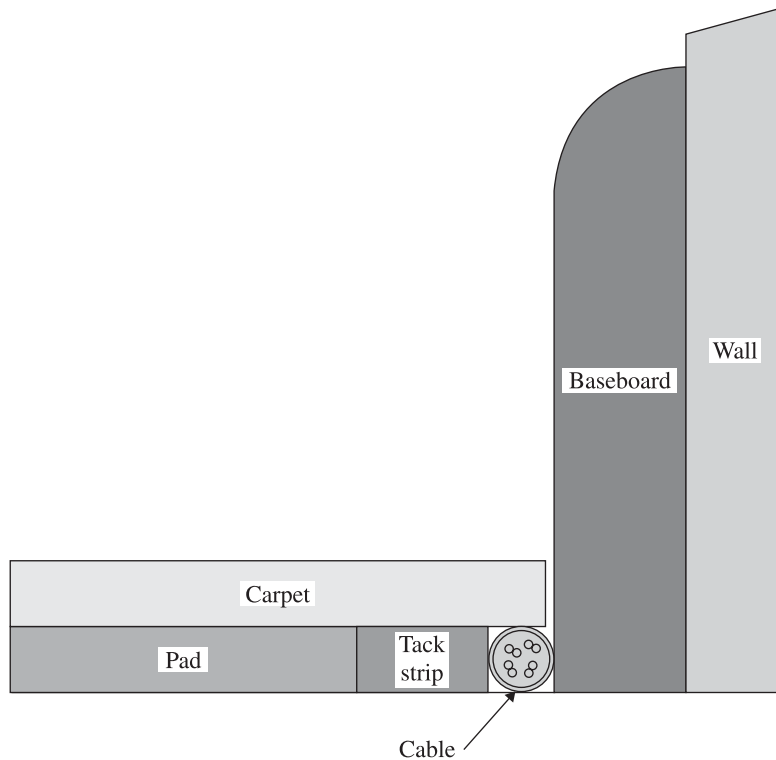


FIGURE 1-5 The cable inserts between the carpet and the baseboard

- **Use the baseboards** If you just need to get to the next room, you may push the cable into the space between the carpet and the baseboard, as shown in Figure 1-5; it can go right through doorways in this space and pop out again where it is needed.
- **Hide the cable behind special molding** Cove molding can hide network cabling as it runs around a room, as shown in Figure 1-6. Check your home center for other molding styles that leave a space behind them that can hide a cable.
- **Wire molding can be used on the wall surface** If you don't mind seeing some evidence of its passage, you can also protect your cable with wire molding from your home center; see Figure 1-7. This product is designed to adhere to the wall and provide a space to run cables.

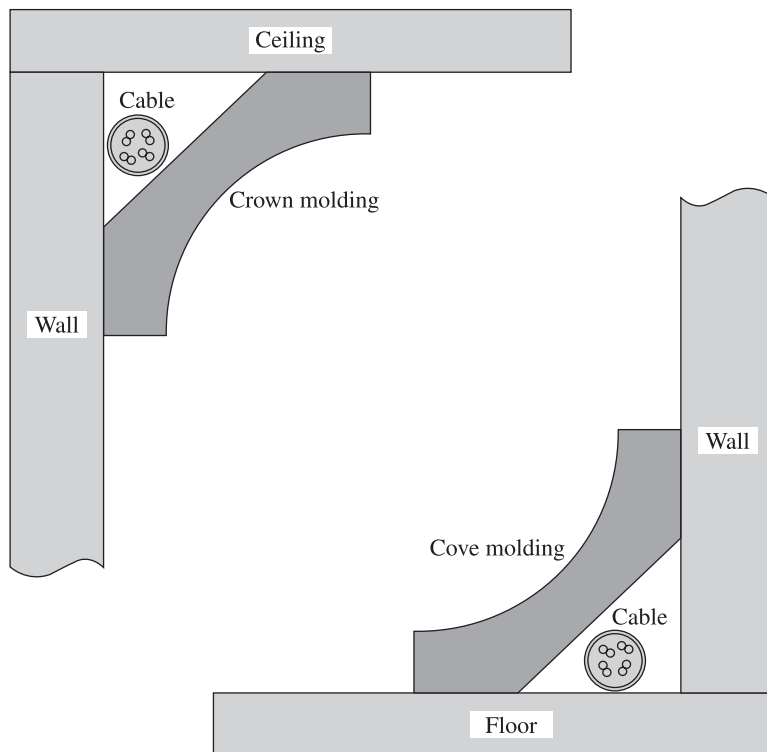


FIGURE 1-6 The cable goes behind special molding

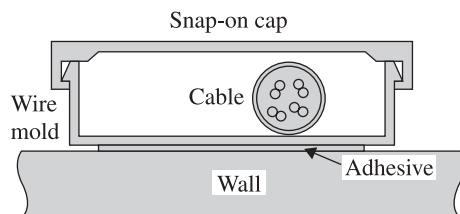


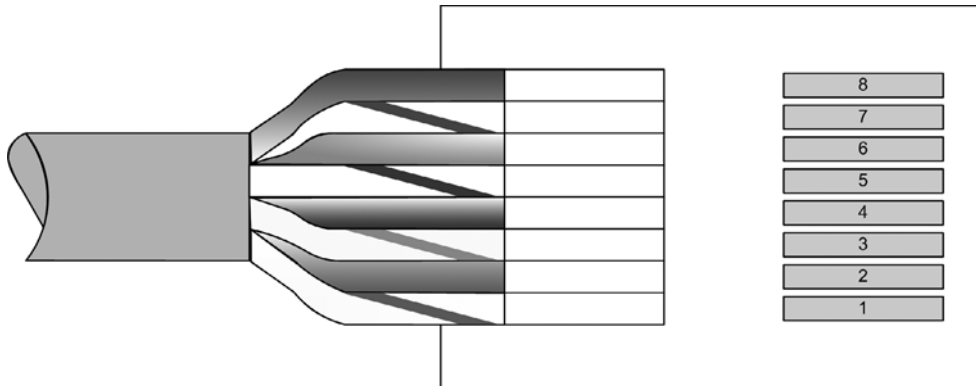
FIGURE 1-7 The cable is hidden by wire molding

- **Use the ventilation system to reach other rooms** If you can't find any other way, you can get cable from room to room in the air ducts. Special cable called *plenum-rated cable* is designed for running in ductwork. This type of cable has a jacket specially formulated so that it will not release noxious fumes when it burns. It is required by most electrical and fire codes when cable is to be run in ventilation spaces. **DO NOT** use standard cable for this purpose, as it releases toxic fumes when it burns.

You Can Use These Category 5 Cable Connectors

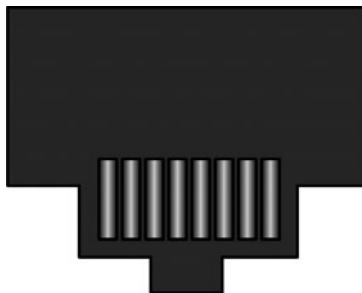
The connectors on the ends of Cat5 cabling resemble phone plugs. In fact, they are of the same class, called RJ (for Registered Jack). The principle difference is the number of wires in the jack. The standard phone cable has a four-wire jack; RJ-45 has eight wires. Because of the extra wires, the RJ-45 plug and jack are necessarily bigger. You cannot plug an R-45 plug into a standard phone jack.

RJ-45 Plug Connectors These connectors are crimped onto the ends of the cable with a special tool. You can usually find this tool at your local home center or your local Radio Shack. When you insert the wire, be sure to arrange it according to the Cat5 color code you are using.

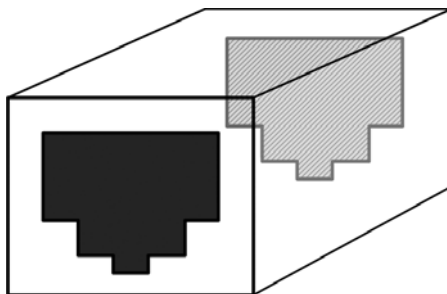


RJ-45 Jacks Cat5 wall jacks have color-coded *punch-down* connectors for terminating your in-wall cable. Most use a Type 110 punch tool, which we will discuss later in the section “Cable Installation Tools.” Some do-it-yourself jacks have tool-less connections or include a small plastic punch tool in the packaging. When the cable is inserted into the jack, the jack can then be mounted in an appropriate faceplate for the location you are installing your jack. Faceplates are

designed to mount in a standard wall box or to surface-mount when a wall box is not available.



Category 5 Inline Couplers An inline coupler is a small box with female connectors on each end. It is designed to connect two Ethernet patch cables end-to-end. It is preferable to use a single length of cable when possible, but if the need arises, you can obtain Cat5-rated inline couplers where you get your Cat5 cables.



Cable Installation Tools There are several types of tools you can use while wiring your home for networking. In this section we will look at RJ-45 termination tools, including crimp tools, cable strippers, cutters, and punch-down tools.

- **RJ-45 crimp tools** The RJ-45 plug is installed on the cable with a special tool designed to *crimp* the plug onto the prepared cable. These tools typically have a slot that looks like an RJ-45 jack that the plug is inserted into. The cable is then inserted into the plug and crimped with a squeeze of the handle. Prices for these tools vary from about \$20 to as much as \$150, depending on the quality of the tool and other features it may have. You may have to

order your crimp tool from an online computer retailer or your local home center store.



- **Cable strippers and cutters** While you can use a very sharp knife to strip the cable before installing plugs and jacks, it is much easier and safer to use a proper stripper. It also helps avoid nicking the conductors, causing performance degradation in the assembled cable. Several manufacturers make strippers for Cat5 cabling. You can buy strippers at Radio Shack, online, or at your local home center.



To cut Cat5 cable, all you need is a good pair of diagonal cutters. You can get these at your local hardware store or home center.



- **Punch-down tools** RJ-45 jacks use Type 110 punch-down terminals to connect the individual wires from the cable to the jack. Some jacks ship with a small plastic tool for punching these wires in, but you'll usually get better results if you use a dedicated Type 110 punch-down tool. These are available from your local home center or online and typically cost between \$10 and \$40.



- **Category 5 cable testers** Professional cable installers can certify their cables for compliance with the electrical specifications of Category 5 cables. Electronic testers send a series of signals over the cable and record the detected interference and crosstalk. If everything tests within specifications, the cable is certified. For most home networks, certification testing of Cat5 cable will not be necessary, but consider it if you have your cable professionally installed. For a few dollars more, you have assurance that it was properly installed and terminated. Some installers will test the cable as a matter of course. Be sure to ask your installer.

Use Your Electrical or Telephone Cabling for Data

As you have no doubt noticed, we just spent several pages discussing the installation of cable for networking. If that all seems a bit too much, you might want to consider alternative networking technologies. We will discuss wireless networks in two other chapters in this book, but right now we will look at two excellent alternatives to dedicated wired Ethernet.

Homeplug: Ethernet over Power Lines

Homeplug is a 14 Mbps standard for transmitting Ethernet signals over power lines. This device transmits Ethernet signals over your home's electrical wiring and plugs into a standard wall outlet. Many manufacturers now sell products using this standard. It is an excellent way to get a network port into a hard-to-wire room. It is also great for temporary networks. The Homeplug signal travels through your power lines from device to device and can be used anywhere in your house. The signal carries out to the nearest power transformer, so it can possibly be detected in your neighbor's house.

How to ...

Install Your Category 5 Cabling Without Special Tools

It is possible to install Cat5 cabling without all the cutters, strippers, punch-down tools, and crimpers. Radio Shack sells an in-line coupler designed to snap into a wall plate also sold by Radio Shack.



Using this coupler, it is possible to construct your home network entirely out of pre-made patch cables:

- Measure the distance of each cable run and buy the appropriate length of pre-made Cat 5 cable.
- Pull the cable into place.
- Connect the snap-in coupler to the end of the cable.
- Snap the coupler into the faceplate and install the faceplate on the wall.

Not to worry, Homeplug incorporates encryption into the product to ensure your neighbors cannot listen in on your conversations.



Ethernet over Telephone Lines

Several manufacturers also sell devices to carry Ethernet over standard phone lines. These devices currently support data rates of 10 Mbps.



This page intentionally left blank

Chapter 2

Design Your Own Home Network



How to...

- Determine your requirements
- Choose between wired and wireless
- Map your physical network
- Map your logical network
- Create a utilization plan

You've read up on the basics of home networking, and now you're no doubt itching to roll up your sleeves and get started putting in the system. In this chapter we will cover the planning of your network and the selection of appropriate equipment for your design.

Mostly what you are going to need are a basic idea of your requirements for your network and a plan of how we are going to satisfy those requirements. We start by creating a list of all the devices you are planning to place on the network. We will determine the best way to connect them and which type of network device to use for the task. We will then map it all out so that you can refer to the plan later when you are installing your network equipment.

Determine Your Requirements

The first thing you need to do is make a list of all the items you are planning to connect to the network. This list is not as short these days as it once was. In addition to a list of your computers and possibly a printer or two, you can now add your home media equipment, cameras for viewing the front door or back yard, the game console, and even network devices such as storage drives or IP telephones. Some of these devices will include their own network connections; some will need optional networking devices to enable them to connect to the network. Take a look at your documentation on the device to see if it includes an Ethernet port or if it supports TCP/IP networking.

List Your Computers

The first devices to list are your computers. They were the first residents of networks and will continue to be the main network devices for some time yet. Create a simple list of computers by name of computer. This list can be done on your computer and

Network Attached Storage

If you require centralized storage for media or document files, you can attach a Network Attached Storage (NAS) device to the network. A NAS unit is simply a server optimized for file sharing. It can have one or more disk drives, providing gigabytes of storage space, and can typically be accessed by most operating systems and web browsers on the network.

printed for ready reference, or it can be kept on note paper if your computer is still in a box. In most cases this will be the computer name that is configured in Windows XP. Figure 2-1 shows the Windows XP System Properties dialog box with the Computer Name tab displayed. If you have not named your computers yet, you can do so now or use a description instead.

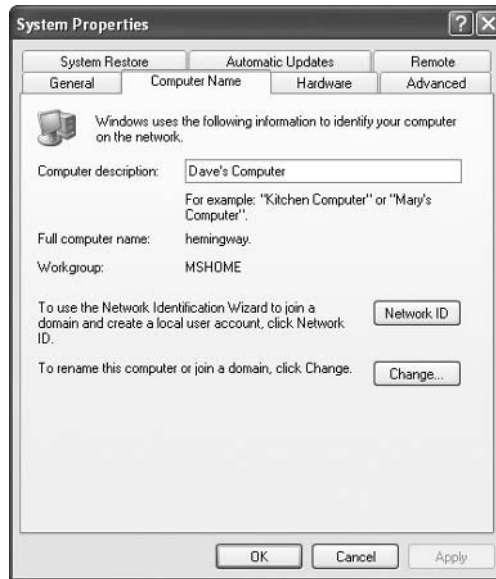


FIGURE 2-1 Computer name displayed in System Properties dialog box

How to ...

Change the Name of Your Computer

If you still have the default computer name given to you by Windows, usually something that looks like YOUR12E2341, now would be a good time to give your computer a descriptive name:

1. Right-click My Computer and select Properties, or open the System applet in the Control Panel.
2. Select the Computer Name tab; click Change to open the Computer Name Changes dialog box.



3. Enter a new computer name in the Computer Name field and click OK.
4. You will be prompted to restart your computer to complete the name change. Click OK to restart your computer.

List each computer name, the operating system version it is running, whether it will be sharing any printers or files, and what type network adapter it has installed (if any). This information will be used when mapping the network and will also help determine if any additional hardware will be required to connect the computer to the network. An excerpt from the author's device list appears in Figure 2-2.

Computers:			
Name	Operating System	Shares	Network
Hemingway	Windows XP Professional	<ul style="list-style-type: none">• HP Laserjet 697C• File sharing	Ethernet
Beauty	Windows XP Home	No shares	None
Beast	Windows XP Professional	<ul style="list-style-type: none">• File sharing	Ethernet
Tampa	Windows Server 2003	No shares	Ethernet
Other Devices:			
Name	Shares		Network
Network Camera	<ul style="list-style-type: none">• Video• Photos		Wireless Ethernet

FIGURE 2-2 The Author's network device list

There may be additional pertinent information about the devices you are listing. Recording this information will be helpful when you are determining how best to construct your network. This may be information such as

- The brand of your Ethernet adapter (if known).
- Any special notes about the device's location in the house, such as wireless signal obstructions.
- Any special cabling concerns, such as having solid walls, and any need for surface-mounted cable raceways.

List Your Other Network Devices

There may be other devices you are planning to connect to your network. An example of an additional device would be your Game Cube or a network camera. Add these devices to the list as well, keeping in mind that you will need to know where and how they will connect to the network.

Plan for Future Expansions

As more network-enabled devices become available, it will be necessary to extend network connections to them as well. Most new network-enabled consumer devices

use wireless Ethernet to enable connectivity. This will make it simpler to get these devices added, but it makes wireless networking a must if you want to future-proof your network. If you plan to include any of these kinds of devices in your network in the future, you will want to plan now for installing wireless Ethernet.

NOTE

For more information on next-generation wireless devices, see the spotlight section in the center of the book.

Select the Best Network Type for Your Home

There are many factors that can work for or against a certain network technology.

- Accessibility to crawl spaces or attics can dictate whether it is possible to get cables from room to room.
- Building materials used in walls, floors, and ceilings may help determine whether radio signals can pass through them without excessive signal loss.
- Security concerns or ease of installation may tip the scale in one direction or the other.
- Speed may be a factor if you regularly transfer large media files from computer to computer or between your computer and your media equipment.

In this section we will present some of these concerns and help you decide which technology is best for your home.

Planning Cable Routes

For wired Ethernet installations, it is necessary to get the cable from one room to another. There are many ways to accomplish this, and each will have to be evaluated to determine whether this type of network is feasible. The effect on the appearance of the home will also be a factor. Many of us will want to hide cables in walls, in floors, or above the ceiling.

Chapter 3 will discuss many ways of getting cables into hard-to-reach places. We will discuss room-to-room cable routing techniques, ways to get cable around a room, and other tricks of the trade. Keep in mind as you read the tricks that extreme measures will be necessary only if you cannot find an effective alternative. Wireless Ethernet should be considered before you go tearing up your house unless you have a security need that prevents your considering it.

Why Building Materials Matter

Building materials matter just as much in your determination of which technology to use as the construction method the builder used. Certain materials can block the radio signals of wireless Ethernet. Other materials will make it very difficult to get cable where you need it.

Signal Attenuation by Metallic Materials

Signal attenuation is the capacity of certain types of building materials to weaken or block radio signals. Materials such as reinforced concrete, aluminum siding, metallic screens, and expanded metal lath can effectively block radio signals in the 2.4 GHz band—the frequency band used by 802.11b and 802.11g wireless Ethernet. Reinforced concrete and metal studs are used extensively in commercial buildings, apartments, and condominiums. Metal lath is used to reinforce plaster walls. If you suspect your home includes these materials, or any other material with a high metallic content, you may want to have a couple of wireless-equipped laptop-toting friends come over and test your walls.

TIP

Think of the radio signal as a powerful flashlight beam that can shine through only a certain amount of material. The more dense the material, the less the beam will penetrate. Shine the beam around your place, focusing it on where the radio signal will need to go. What do you see between you and your target? Is there a concrete floor? A paneled wall? If you visualize your installation in this way, you will begin to see where you will have attenuation problems.

The alternative, of course, to wireless in these circumstances would be wired Ethernet. Buildings using concrete and steel construction should have conduits and plenum spaces you might use to route your cables. Check with the building maintenance manager to see if there are any open conduits you can use. If you own your home, you may need to hire an electrician to locate or install conduits or cable raceways.

Fiberglass Makes You Itchy

Not to be ruled out in your evaluation of which method to use is the fact that you may have to crawl across carpets of fiberglass insulation or try to push cables through insulated wall spaces. Building materials like brick and adobe are definitely going to resist your efforts to run cable. In these environments you may have to opt for cable raceways or other surface-mount techniques.

Unfortunately, some of these materials will attenuate wireless signals as well, so test your area before you invest too much in wireless technology.

Security Implications for Network Selection

In environments where security is a top concern, wireless Ethernet is sometimes shunned by network installers. At the end of the day, you are the one that has to rest easy knowing your data is secure. Wired Ethernet is definitely simpler to secure, as you know with certainty where it comes from and where it goes. You won't have to take extra measures to ensure your data is secure on the network. However, as you will see in Chapter 6, there are excellent ways to secure wireless networks against all but the best-equipped crackers.

Distance Criteria in Network Selection

As you begin to plan for your installation, you will begin to see how far your devices are from your hub or router. Most homes will not pose a problem for distance, but it may be wise to keep in mind the effective distances of each network technology. Table 2-1 shows the transmission distances each common home network technology can achieve. Keep in mind these are for best-case scenarios. Signal attenuation will shorten your effective distance for wireless Ethernet. Cable defects can shorten your effective distance for wired Ethernet.

When You Feel the Need for Speed

The last aspect of network requirements we will consider in this section is speed. Some applications simply require more bandwidth than certain technologies are capable of. At 54 Mbps, 802.11g wireless Ethernet has largely closed the gap with

Network Technology	Maximum Distance ¹	Maximum Speed ²
Category 5 Wired Ethernet	328 feet (100 meters)	100 Mbps
802.11a Wireless Ethernet	50–75 feet	54 Mbps
802.11b Wireless Ethernet	300 feet	11 Mbps
802.11g Wireless Ethernet	250 feet	54 Mbps

¹Wireless network technologies are rated under perfect conditions. Real-world installations will have attenuation factors and radio frequency interference that will shorten the effective distance you can achieve.

²Speed for wireless technologies will decrease as distance approaches maximum. At a maximum distance, it is not uncommon to see speeds as low as 1 Mbps.

TABLE 2-1 Distances for Various Network Types

High-Speed Ethernet

If you find 100 Mbps is not enough (you're designing space shuttles or broadcasting High Definition Video), you may need to investigate higher-speed technologies such as wired Gigabit Ethernet or even 10 Gigabit Ethernet. These technologies are still too expensive for most homeowners and are used only in corporate backbone networks and on high-performance servers and workstations. If you see yourself needing this kind of horsepower, you will probably require the assistance of a professional installer, as your cable runs need to be certified to Cat5E or Cat6 to support these speeds.

100 Mbps wired Ethernet. In fact, some wireless vendors are making 108 Mbps wireless available with proprietary channel-bonding technologies.

CAUTION

Channel bonding leads to incompatibility problems. For more information, see the Did You Know? sidebar about channel bonding in Chapter 6.

Most of the consumer wireless gear, such as cameras and media-sharing devices, uses 11 Mbps 802.11b wireless Ethernet for connectivity. If the device is designed for that speed, it will likely be effective for your needs. Keep in mind that wireless bandwidth is aggregate. This means that each device transmitting at 11 Mbps is using the full resources of your network's access point or router when it is transmitting. When additional devices come on the air, the bandwidth available for all is reduced proportionately. If wireless is still your first choice, using 802.11g access points and routers would be a good choice for this scenario. These devices are downward-compatible with 802.11b and will have speed to spare for other devices.

Create a Physical Map of Your Network

To be able to visualize your network, you need to lay it all out on a map. The technique you use is less important than the planning a map will require. You may not be the type who writes things down, preferring to get out the tools and start pulling cable. I urge you to persevere with this step. It will aid you in estimating your materials, it will point out potential problems you will face, and it may be necessary if your municipality requires prints for any work of this type. Figure 2-3 shows the plan of a home's first floor. You will see this plan again as we discuss other topics in this section.



FIGURE 2-3 First floor plan of a home

Sketch the Outline

For visual appeal, we use computer-generated drawings in our book. You have no such restrictions. If you are comfortable drawing this on the back of an envelope, by all means, go ahead. Be sure to measure and indicate the relative positions of walls and rooms. You will be referring to this plan, as shown in Figure 2-4, when you determine your placement of equipment. Know where your network devices will be placed. If your home will have equipment on two levels, sketch both levels and indicate the relationship between the two. If you will be submitting this to a building official, they will want to know where you will be creating openings between floors.

Add Your Devices to the Map

After you have the general outline of your rooms, you can begin to place your network devices on the map. As you do this, you will begin to see where your networking



FIGURE 2-4 The multi-level floor plan

challenges will be. In the house in these drawings, you can see challenges both for pulling cables and for wireless coverage. Both levels are fully finished, so pulling cable would require special tools such as special drills and fish tapes (metal or fiberglass coils that can be “fished” inside a wall to guide a cable). There is also a mass of closets and stairs in the center of the first floor. This will attenuate the wireless signal quite a bit. Only by placing our devices on the map will we see these challenges and be able to develop strategies for dealing with them. Figure 2-5 shows the plan with placement of potential network devices.

As you can see, this installation calls for some flexibility for movement for a laptop computer. You can see that wireless Ethernet will play some role in this design unless we give the poor soul a 100-foot cord!

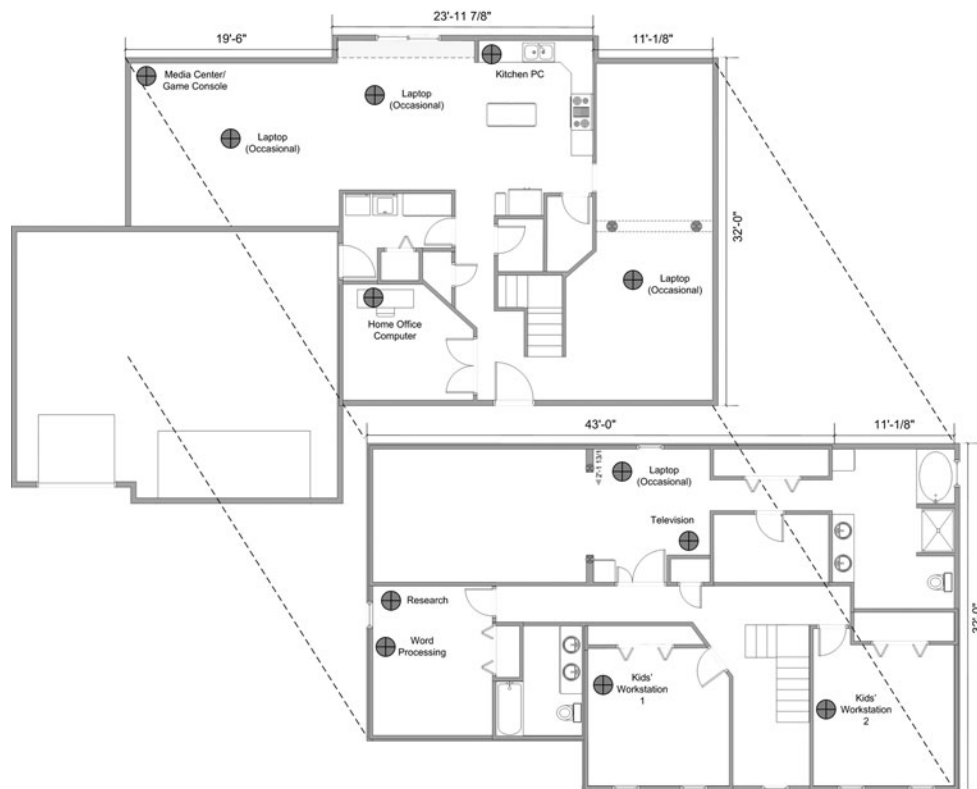


FIGURE 2-5 Placing network devices

Get the Numbers Right

A network map will help you think in terms of distance. You will come to know how many feet your cable has to reach; how many walls your signal must penetrate. You will begin to see relationships between different network devices. You may discover that, for instance, if you move your desk you can take advantage of a wall shared with your media center in the next room.

Take measurements of all your potential cable routes. Keep in mind both the amount of rise (vertical distance) and run (horizontal distance) the cable will have

to travel. The total of the two will be the required length for your cable. When you are done, you can add up all your cable lengths to determine how much cable you will require overall.

Visualize Your Signal

If your plan begins to get a bit too ambitious for wired installation (as ours has), you will probably start to determine how to get the best wireless Ethernet signal to your network devices.

Many people set up a wireless access point in the home office, put wireless adapters in each computer, and wonder why they are only getting 2.5 Mbps in the next room. When you are looking at your plan, try to spot signal blockers. These can be plasterboard walls, concrete floors, large plants, even closets full of outdoor wear.

Did you know?

Microwaves Are Used to Transmit Data

The ability of water molecules to capture microwaves is what makes a microwave oven work. The microwaves are captured by the water molecules in food and transfer their energy to the food. This is why you will be able to remove a glass plate without a hot pad after cooking. The heat was transferred only to the water-containing food. Microwave a dry pretzel sometime. It will barely get warm. But put a moist slice of bread in for a few seconds and it will burn your hand.

Wireless Ethernet uses microwaves to transmit data. Any item in your house that contains water will effectively block these radio waves. This can be a large plant, a closet of wet coats, a laundry basket, even your family members. After all, we are just large bags of water as far as radio waves are concerned!

Commercial installers of wireless Ethernet equipment will tell you that they have to plan for crowds when they install equipment. They will either raise the antennas above the crowd or plan for reduced range when the room fills up.

Look closely at the Home Office in Figure 2-5. Right next door is the laundry. This room will contain damp clothing, large electromagnetic fields from the appliances, water pipes, and a closet for wet coats and boots. Aside from metal, water is probably the best most effective attenuator of microwaves.

If I were to install a wireless access point or router in the Home Office, I would run the risk of intermittent signal loss. In addition, I would always have difficulty reaching the kitchen through what amounts to six or seven walls.

Where else can I put it? Take a look up on the second floor. That is where the Writing Office is. It seems sort of off to one side, but we can play a neat trick here. If I send a Cat5 cable up the inside wall, I can run it a short distance through the attic to the center of the house, as shown in Figure 2-6. Installing a wireless access point there will shower signals down through the entire house from above. At most, each room will be getting its signal through a carpeted floor and one wall. Centering the access point will also shorten the distance any signal would have to travel. Being flexible in your placement will help you get the best coverage possible.

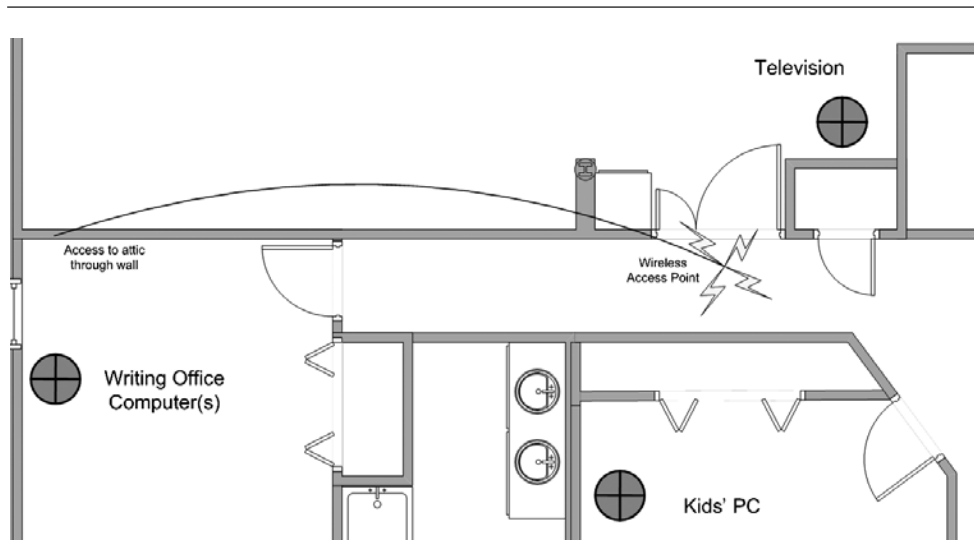


FIGURE 2-6 Centering the wireless access point

How to ...

Install Antennas to Remote Locations

2

You can install wireless networking equipment in places not served by power lines by transmitting the power over the Cat5 Ethernet cable. Power over Ethernet devices are produced by most manufacturers of wireless networking devices and are available from online retailers and select local computer stores. A special device connects to one end of the run and injects electrical current into the same cable that carries your network signal. Another connector on the other end pulls the power off the cable and makes it available to power the network device.

If you find it impossible to route your network cable and power to a remote location, you can also purchase extension cables and remote antennas for your access point. These allow you to place the antenna a short distance away from your wireless device to get better placement.

Create a Logical Map of Your Network

A map of your physical layout and network device placement is intended to help you visualize the scope of your wired or wireless installation. A physical map will deal with actual device placement and cabling, while a logical map will assist you with the setup and configuration of your devices once they have been connected to the network.

Once again, it is not necessary to create a piece of art suitable for framing here. You mainly need a good idea of how the various devices are connected to the network and, by extension, to each other. You also need a way to keep a record of their addresses or other configuration information. An ink sketch of the devices and their connections to each other is sufficient. You can fill in the addresses when you have assigned them.

Determine the Placement of Concentrators

When you have determined which type of network you are going to install, you will place the appropriate concentrators (hubs or switches) at the center of your network. Since this is merely a logical map, it is sufficient to arrange your devices in

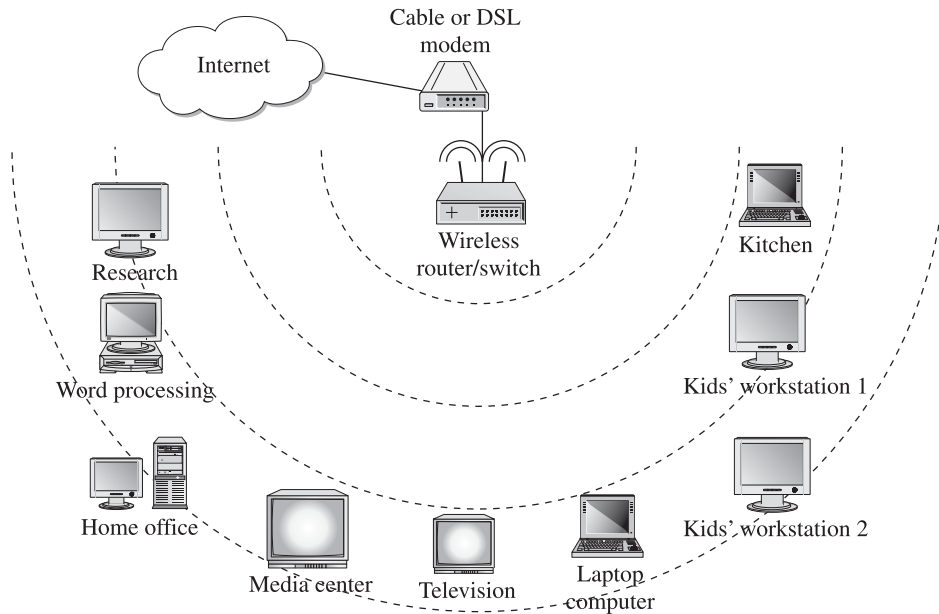


FIGURE 2-7 A diagram of our devices using wireless networking technology

a semicircle around your concentrator. As you develop the logical design, you will fine-tune the placement of your physical devices.

The concentrator will form the focal point of your network. Each device will connect directly to the concentrator, either with cable or via wireless connection. Figure 2-7 shows the network we are designing using wireless Ethernet.

For wired networks, you will need to provide “home runs” for your devices to the central switch or hub. A home run is an unbroken length of cable from a device or its wall plate to the main wiring location. As you begin to see the requirements for cable runs, you may decide to adjust the placement of your concentrator in the home. It does not need to be in the office; it can even be in a closet if that is the most efficient place for it. Feel free to move back and forth between your physical map and your logical map as you see the need to make adjustments.

Figure 2-8 shows our devices connected by cables. Note the laptop and televisions are still using wireless. In this situation, it would be better to choose a hybrid of wired and wireless connectivity, as the laptop would lose its mobility with cabled Ethernet and the media-sharing devices are designed specifically for wireless Ethernet.

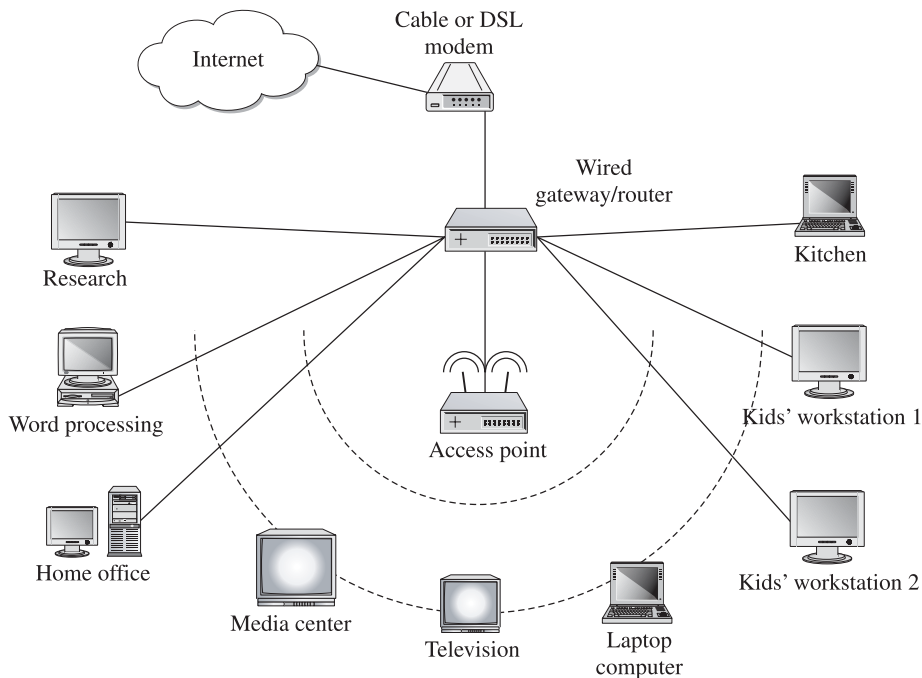


FIGURE 2-8 The same network devices using wired Ethernet

Create a Network Utilization Plan

By now, we have placed all of our equipment except for the cable/DSL modem. The concentrator (router or gateway in this case) or its antenna is planned for the upstairs hallway, each device has its physical location mapped, and we know how we plan to extend connectivity to it. For the actual execution of the cabling plan, we will refer to Chapter 3 for wired Ethernet or Chapter 4 for wireless Ethernet. All that remains for now is to decide how these devices will interact. Do we want kids to store their homework on the Home Office computer? Will any of the PCs be tapping into the media sharing network? Will all computers have Internet access?

As we answer these questions, we will be forming our plan for implementation of the peer-to-peer networking features of Windows XP, and for control of the Internet access settings of the Internet Gateway. When we cover installation of networking features in the next two chapters, we will cover basic setup of these services.

Did you
know?

Most Homes Use Peer-to-Peer Networks

Most home networks will employ a *peer-to-peer* or *workgroup* logical configuration. This type of network allows each computer to control access to its own files and printers. Each computer controls security for its own resources, and there is no central administration.

This is opposite to what you will see in most corporate networks. These larger networks will employ centralized access controls and will be controlled by a central administrator. Networks of this type are known as *domain* or *directory* networks.

Chapter 3

Install a Wired Network



How to...

- Install Network Cabling
- Install Networking Equipment
- Configure Your Computers
- Connect Your Network to the Internet

By this point in the book, you have decided what the network will look like and what types of equipment and cabling you will be using. The fact that you are reading this chapter at all indicates you have decided to wire at least part of your home. In this chapter we will cover installation topics we have previously alluded to in much more depth. We will begin by showing you the tools, tips, and tricks used by professional cabling installers to wire homes and businesses. We will then discuss the installation and configuration of networking equipment and computers on the network. Finally, we will show you how to get your network connected to the Internet.

Install Your Network Cabling

You may have chosen to use wired Ethernet for security reasons, higher communication speed, or simpler network device configuration. In this section we will help you minimize one of the drawbacks of wired Ethernet, namely the cable installation. We will show you how to get into the tight spaces in your home and get the cables where they need to go.

We will show you the special tools installers use, and introduce some of the jargon used in the installer-speak. This should prepare you for the task at hand and help you to understand industry writings you may encounter in equipment instructions and online guides. Next we will demonstrate some of the techniques for pulling (or pushing) cable. Then we will cover how to connect the cable ends into plugs or jacks. Finally we will present some alternatives to Category 5 cable.

Select Your Installation Tools

Cable installation tools fall into two broad categories: tools for installing cable in walls, floors, and ceilings; and tools for connecting the ends of the cable into plugs and jacks. In this section we will provide some illustrations of each and give a brief explanation of their use.

Tools for Pulling Cable

This category of tools includes tools for operating in crevices and inside walls to push or pull cable where it needs to go.

Fish Tapes and Rods “Fish tapes” are any of a large family of tools resembling a coil of steel or fiberglass. They are used to “fish” inside a wall and pull a cable back out with them. They are excellent for getting cable across suspended ceilings without dropping all the tiles or pulling cable between floors in a multistory dwelling.



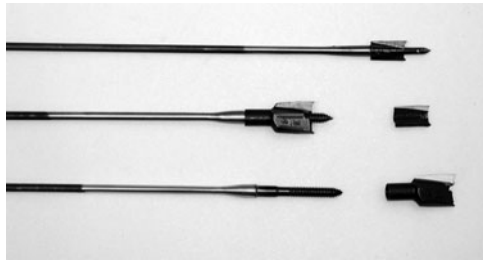
“Fish rods” are similar in construction to fish tapes but come in shorter lengths that can be attached end-to-end to reach some distance in a wall or ceiling space. Deciding whether to use a fish tape or a fish rod is typically a matter of personal preference among installers, and one is not necessarily better than the other for all uses. That being said, the fish tape is typically better for long cable runs, while the fish rod is easier to maneuver in tight spaces.



As you determine your need for this type of tool, consider the distance you will be pulling cables. If you just need to get a few feet inside a wall to reach a jack or to pull a cable up from the level below, you can use a rod. Pulling cable through many feet of conduit will generally require a tape. While both tools can push and pull cable, often a rod is better for pushing cable because of its extra stiffness.

Fish tapes can often be found at rental centers and can be obtained for between \$30 and \$40 at electrical supply stores and hardware stores. Fish rods are usually available to order at electrical supply stores, hardware stores, or online from outlets such as hometech.com or smarthome.com.

Fish Bits and Other Special Drill Bits “Fish bits” are special drill bits designed to drill through studs or wall plates deep within a wall cavity, often flexing around a corner to do so, to penetrate an area where cable needs to go. Often the cable is actually attached to the drill bit when the hole is completed and pulled back through the wall with it. Directional guides are often used to aim the bit within the wall space. Bits are available for drilling through wood, steel, and masonry. For a graphic of a fish bit in action, look at Figure 3-2 later in the chapter.



Wood-boring bits are often used in new construction to speed drilling through the many vertical wooden wall studs that must be bored to make way for the cabling. Equipped with a powerful right-angle drill, a single person can bore all the required holes to wire a home in half a day.

Fish bits and boring bits are available at local electrical supply stores and hardware stores.

Tools for Connecting Cables

Tools for connecting cable were introduced in Chapter 1, but in case you are doing a surgical strike with this chapter, we will briefly describe each tool again. After the cables are in place, they must be connected (“terminated” in installer-speak). For this we need tools to *strip* the insulation back from the wire ends, *crimp* on jacks, or *punch* the ends into wall jack connectors.

Strippers Most hardware stores will have strippers designed to strip only the outer jacket from the cable. We do not need to strip the actual wires themselves, as connectors of the type we use will actually penetrate or displace the insulation as

they are installed. Ask for a *cable jacket stripper* at your local hardware store or electrical supply store.



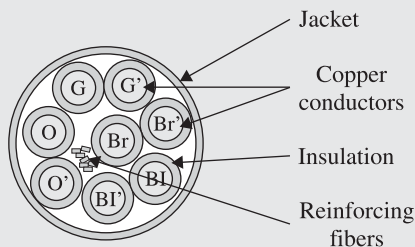
3

How to ...

Prepare the End of a Category 5 Cable for Termination

To prep the end of a cable for termination, you must perform two steps:

1. Strip back 3/4" of the outer jacket. The outer jacket forms a layer that protects the inner wires and holds them in the proper position relative to one another. It must be stripped back to expose the inner wires. Here's a cross-section of the cable:



2. Untwist the inner wires and arrange them in the proper orientation for the connector. An RJ-45 connector will require them to lie flat for insertion into the connector. A jack will just need them to be inserted into the appropriate slots in the jack.

Crimpers RJ-45 plugs are *crimped* (or pressed) onto the cable end using a tool called a crimper. This tool is designed to hold the plug in place while the wires are inserted and then to crimp the connector down onto the wires. The crimping action displaces the insulation on the wire, making contact with the copper conductor inside.



Punch-Down Tools *Punch-down tools*, also called *punch tools*, are used to insert wires into the type 110 punch-down connectors within a cable jack. The act of inserting the cable into the connector displaces the insulation, allowing the wire to make contact with the jack's circuits.



Cable Pulling Techniques

In this section we will expand on some of the tricks we introduced in Chapter 1. Using the tools presented in the previous section, we will use diagrams to show how cables are routed through wall, floor, and ceiling spaces to reach the location where they are required.

New Construction Cabling

New construction cabling is perhaps the simplest to manage. The biggest challenge here is finding the proper time to run the cables. Many builders allow time for electricians to perform “rough-in” (or basic cable routing) work, and then allow time later on for “finish” work. We will tell you which tasks to perform at each

juncture, and what to look for with your contractor. We are describing the procedures to use for wood frame houses, as they are most common. If your builder is building with a different technique, please refer to the section “Pull Cable in a Completed House” for ideas.

Rough In Your Cables Ask your builder when the electricians will be roughing in the electrical wiring. Often the electricians will be working during the daytime. If there is a chance you might be getting in their way, wait for evening.

Look at the way the electricians route their cabling through the house. Runs between floors will follow a stud to the ceiling level and then pass through a hole in the wall top plate into the space above. They will then pass up through the floor above and the bottom plate of the wall above.

NOTE

Avoid the temptation to follow the electrical cabling. Electrical cabling generates sizable electromagnetic fields during operation that will disrupt signals in your cable. Maintain a minimum of six inches between your cables and electrical cabling when run parallel, and ensure any cables that cross electrical cables cross at a right angle. Crossing at a right angle will minimize the interference picked up by your cabling.

Figure 3-1 illustrates cable routing in a frame wall. It shows three cables entering a wall box. This is typical of the box you may use near your hub or switch. The other cable runs go to different rooms in the house. Note the staples used to hold vertical portions of the installation. Be careful to staple cables lightly using staples designed for coaxial or Category 5 cable. Arrow makes the T59 staple gun for installing insulated staples designed specifically for installing rounded data cabling. You should be able to order it at your local hardware store or online. Pinching or kinking cable can damage it, resulting in poor signal carrying capability and reduced transmission speed. This is not what you want happening in a wall where it is not easy to repair.

Also in Figure 3-1, note the staple just above the wall box. Staple your cables just above the box and before crossing through the stud or over to the opposing stud. This keeps them in place when workers are moving wallboards around and may bump your cables. Be sure to staple cables in the center of the stud to keep them away from the face of the wall. A stray drywall screw (it happens) will ruin a cable. In addition, when you are boring holes through studs, keep to the center of the stud to avoid penetration by screws coming from the stud face. If you can't get to the middle of the stud for some reason, you can find steel protector plates at the hardware store to prevent a screw from hitting your cables.

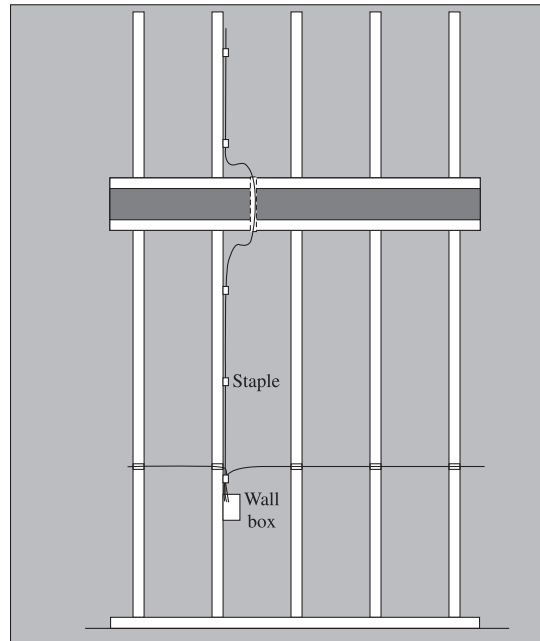


FIGURE 3-1 Cable routing in frame wall construction

Finally, be sure to coil several inches of extra cable in the box (to have slack to work with during termination) and shove it well back into the box to allow the drywall installers to provide a cutout for the box during drywall installation.

Keeping Your Cable from Getting Twisted

When you are running long lengths of cable, it may try to come off the spool in coils. If you pass a broom handle or dowel through the center of the spool and support it on both ends so that the spool can spin as the cable is removed, the cable will then come off the spool without a tendency to coil. An alternative is to purchase Category 5 cable in boxes. Boxes for cabling are designed to prevent the cable from coiling as it is removed. This makes it much easier to handle when pulling it through the wall spaces.

Finish Cabling After the rooms are finished, you can pull your coiled cables from the wall boxes and terminate them. We will cover this procedure in depth later in the chapter. This is also the time to do any last-minute routing along outside surfaces. If you were unable to reach an area where the cable run would be exposed due to solid wall construction, use a raceway (surface-mounted wiring conduit), as we will describe in the next section.

Pull Cable in a Completed House

Okay. Maybe you are not actually building a house at this time. You will need some pointers on finding ways to get your cables in place. In this section we will describe ways to duplicate the results of new construction installations and tricks to get cable to the most difficult locations.

Fish Cable Through the Walls If you did not read the preceding section, please do so now. The best way to install cable with a finished appearance is to attempt to duplicate the results of new construction. This can be accomplished with a little extra effort by using the fish rods and fish drills described earlier.

Fish rods are available in kits with several lengths designed to be attached end-to-end to get the appropriate length for the job. Drills are available in lengths up to 72" to reach into the top or bottom of the hollow portion of the wall between the studs to drill into the next level. The fish rod can then be used to push the cable into the next area. Figure 3-2 shows a drill-and-fish operation being used to push a cable to the level above.

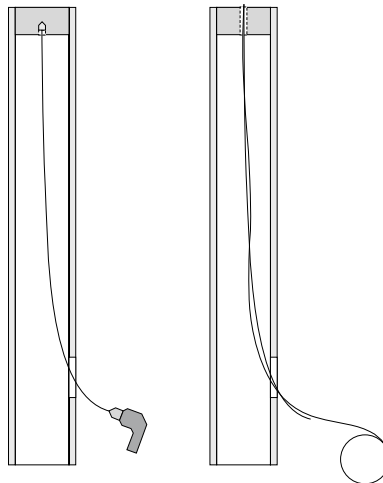
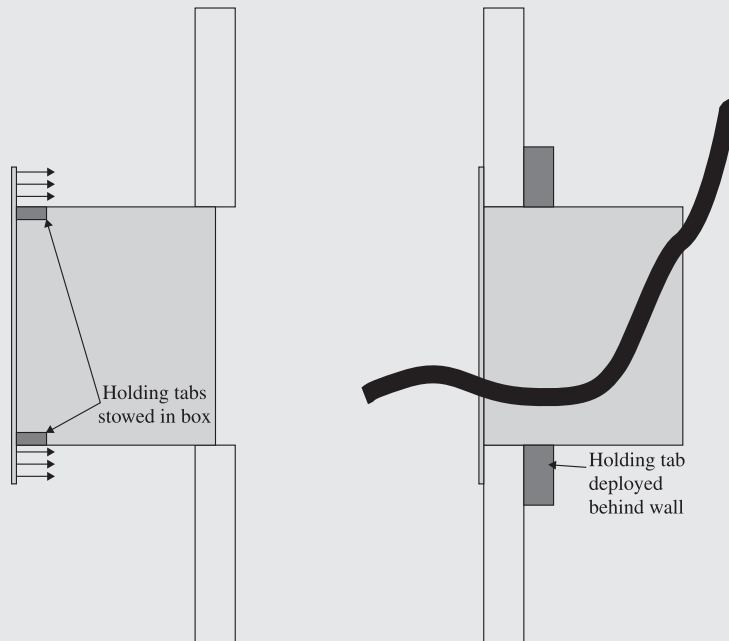


FIGURE 3-2 Using a fish drill and a fish rod to install cabling in an existing wall

How to ...

Use “Old Work” Boxes for Existing Walls

When installing cable into existing walls, you can use what is known to the industry as an “old work” box. This is a box with two or more levers or ears that open behind the wall when the box is inserted to hold the box tight to the wall face. Shown next is the process of installing an old work box.



To install an old work box:

1. Using the box as a template, or using a template supplied with the box, mark the outline of the recessed portion of the box on the wall.
2. Cut out the opening with a saw or utility knife. Take care not to cut any cables that may be inside the wall.
3. Install cabling into the opening from above or below and insert it into the back of the box.

4. Making sure the mounting tabs are folded within the box, push the box into the opening, pressing it tight to the wall face.
5. Depending on box design, tabs may snap out behind the wallboard upon insertion, or you may have to spread the tabs by twisting their screws clockwise with a screwdriver.
6. Tighten the tabs against the wallboard to hold the box snugly in place.
7. Terminate the cable and install the appropriate faceplate.

You can also drill and fish cables horizontally through a wall space. You will drill each stud in the series until you reach the stud bay where you plan to install the wall box. Again, use an old work box for this task. Take care not to drill any electrical cables that may exist in the wall. Your hardware store or electrical supply store should have stud finders that can electronically locate studs and cabling behind the wallboard. These tools usually emit an ultrasonic or magnetic signal through the wall as they pass over its surface and display an indicator when a stud or cable is sensed in the space behind the wallboard.

Use Baseboards and Raceways If drilling and fishing sounds like just too much work, you can choose to hide your cables in baseboard molding, the space between carpeting and the wall, or surface-mounted cable raceways. We outlined this process in Chapter 1.

You can make this job easier by using a fish rod. Fasten the cable to the rod and push it through the space where you are routing it. When you get to the destination, pull the cable end out from the space and route it to your equipment. This is not as neat and tidy as routing it through the wall, but after your desks and other furniture are installed, it will be virtually undetectable.

Use Air Ducts or Suspended Ceilings If you do not have carpet, or it is not practical to use the previous methods, you may choose to run your cable above a suspended ceiling or through the ventilation ductwork. If you do this, be sure to use plenum-rated cable, as the jackets of non-plenum-rated cables emit noxious fumes when burned; such cables are banned by most fire and electrical codes.

Use a fish tape to pull the cable from room to room and extract it from the duct into a cable raceway to route it to your equipment. This should be viewed as a method of last resort, as the cable will be exposed to any equipment that is used to clean or maintain the ductwork. It will also act as a snag to capture dust and lint inside the air duct. Still, when it is the only method available and wireless is not feasible, it is a perfectly acceptable way to get the job done.

Connect the Cable Ends

After the cable ends are sticking out in the proper places, it is time to connect them into the plugs or jacks you will use to connect your devices. Remember to leave some slack to give you some extra cable to work with when you terminate it. In this section, we will discuss termination of Category 5 cable. We will show you how to install it into wall jacks and RJ-45 plugs.

Connect Your Wall Jacks

Most wall jacks use color-coded “punch-down” style connectors. All that is typically required is to insert the correct color wires into the correct slot and press (or “punch”) them into the slot with a punch tool or the plastic tool supplied with the jack. The most important requirement to consider when installing a jack is the amount of wire left untwisted inside the jack. It is best to try to untwist no more than 1/4"–1/2" of wire on each color pair. This practice helps avoid *near-end crosstalk* (NEXT, the X being shorthand for cross, cute, eh?), the interference introduced in neighboring wires by electromagnetic waves generated by each wire.

Avoiding Near-End Crosstalk (NEXT)

Near-end crosstalk (NEXT) is the interference introduced in signal wires when they lie near one another for too great a distance. Electromagnetic fields generated by a signal in one wire induce a signal in the other that may interfere with data transmission in that wire. At the frequencies used by modern networking cables, it is only necessary for the wires to lie side by side for a fraction of an inch to induce this phenomenon.

Category 5 cable uses a prescribed twist ratio to prevent crosstalk, but when it is placed into plugs or jacks it must be untwisted. Untwisting too great a length will cause it to become susceptible to NEXT, which can significantly affect higher-bandwidth networks. Professional installers can use test devices to test for the existence of NEXT and remedy the condition by reterminating affected cables. In the home, this is not feasible, so extra care should be taken to minimize the amount of untwisted wire you leave in a connector.

When inserting wires into a jack, attempt to see that the twist is maintained to the last possible instant, untwisting only enough wire to lay it into the punch slot. Likewise for plugs, untwist only enough to reach the bottom of the channel in the plug where you insert the wires for crimping.

Terminate RJ-45 Plugs

You probably will not have much reason to install RJ-45 plugs. Most installations use wall jacks and then use ready-made patch cables purchased from the store to connect the devices to the jacks.

If you do need to terminate plugs:

1. Refer to Figure 1-4 in Chapter 1 for the proper color codes for each pin of the plug.
2. Untwist enough wire to reach the bottom of the plug's insert channel, and arrange the wires according to the color code.
3. Place the plug into the tool and insert the wires into the plug.
4. Crimp the plug onto the wires and release the tool. Many tools have a ratcheting action designed to apply the proper amount of force to the plug to get a good crimp.

When You Just Can't Get a Cable There

Sometimes, after your best effort, you still cannot get the cables where they need to go. Maybe you hate drilling and getting all itchy from fishing around inside your walls. Whatever your reason, there are reasonable alternatives to Category 5 Ethernet. In this section we will discuss transmission of your Ethernet signal over house electrical wiring or telephone wiring.

Ethernet over Power Wiring

Ethernet over Power Lines, aka HomePlug, provides a connectivity option for networking your home without pulling a single cable. It uses your home's existing electrical wiring to transmit data from one device to another. HomePlug can clock 14 Mbps in the laboratory, but in practice most networks using HomePlug devices achieve about 7.5 Mbps, which is more than adequate for most web surfing and file sharing uses. The standard is still being improved, with the stated intent of someday providing a single plug to power and network your computer and your entire home's media equipment.

NOTE

HomePlug now has a big brother! Broadband over Power Line (BPL) is being tested by electrical utilities as a means of transmitting broadband Internet connectivity over the same power lines that feed your home. It is seen as the best hope for rural residents to gain affordable access to broadband Internet connections. There are still several hurdles to clear with the Federal Communications Commission (FCC), but it looks promising.



Ethernet over Telephone Wiring

If 10 Megabit connectivity is fast enough for you, you can choose Phoneline networking. Cisco/Linksys has a complete line of HomeLink Phoneline networking products for networking PCs, notebook computers, and other Ethernet devices. They even provide a Phoneline-equipped Internet gateway that allows both Phoneline and Category 5 Ethernet connectivity in one device.



Connect Your Networking Equipment

After completing the cable installation, it is time to connect your network devices. With wired Ethernet, this task is relatively simple. We will just discuss here how to verify you have a good connection. We will discuss assigning addresses to your network devices after you have configured your computers.

How to ...

Verify Ethernet Device Connectivity

When you plug your cables into your Ethernet devices, they establish a link with the network. Most devices offer some sort of link status verification. Often this takes the form of a link status light that may change color depending on the speed of the link or blink to indicate network activity. If you are using a device that does not have a link status light, you can verify connectivity by looking for a link status light at the device on the other end of the connection. If this device is a hub, switch, or Internet gateway device, you can check the link status light for the port you have connected the device to.

If you do not receive link status verification, check that the devices at both ends are powered up. If they are, and you still do not have a status light, you may have to recheck your cable connections or terminations. Usually you will find a wire out of place according to the color code you are using. It is rare to find a defect in the cable unless you had to exert excessive force when pulling it and snapped one or more wires inside.

Windows XP can also indicate connectivity when you plug in a network cable. A notification area icon will announce the arrival (or departure) of connectivity for a few seconds each time a cable is plugged or unplugged.

3

Configure Your Computers for Home Networking

Since computers were the original network citizens and probably still are the most important, we will spend some time now discussing how to configure your computers for home networking. After we have configured your computers, we will then discuss giving the remaining pieces of your networked equipment their own network addresses.

Manage TCP/IP Addressing

Each device on a Transmission Control Protocol (TCP/IP) network requires a unique address. We will now discuss how to select your addresses and how to manage them.

What Is an IP Address?

IP addresses consist of four groups of numbers (called octets) separated by periods (called dots). Converting each octet into binary numbers will provide eight digits of zeros and ones (hence the name octet).

An example of an IP address would be

122.168.100.235

which would be spoken, “one-twenty-two <dot> one-sixty-eight <dot> one-hundred <dot> two-thirty-five.”

By experimenting with all zeros or all ones (you can use Windows Calculator to do the binary to decimal conversions), you can see that when converting eight binary digits to decimal, only numbers of 0 to 255 are possible. That is why you will never see an address like 192.888.999.180.

These addresses are consolidated into network groups according to their left-to-right octet order. The address begins with the network address and progresses to the host digits toward the end. For this reason you would most likely find 122.168.100.235 on the same physical network as 122.168.100.234. Internet routers maintain lists of addresses (called routing tables) that they use to direct data to the appropriate network for each device. When the data arrives at the final router in its travels, that router (the Internet gateway) knows which physical device to send the data to.

When you configure a device to connect directly to the Internet, you will be assigned an address that Internet routers will use to find you. This is typically handled automatically by your Internet service provider and does not require any manual addressing on your part.

Select Your Network's Address Range

To communicate effectively, each device on a network requires a unique address. This allows other devices to direct data to it without fear that the data will arrive at the wrong location. On the global Internet, each connected device has an address—called an Internet Protocol (or IP) address—that belongs to no other device in the world. Obviously, it takes some level of management to ensure that no two devices

use the same address. This task is shouldered by the Internet Assigned Numbers Authority (IANA) and your Internet service provider (ISP). When you connect a computer or network to the Internet, you are assigned an address by your ISP from a block given them by the IANA.

Connecting multiple devices to the Internet would require you to be assigned an address for each device. Your ISP would want to charge you for each individual connection, and you would use a large number of global IP addresses for your devices. If each household did this, we would run out of addresses very quickly. For this reason, we can choose to have a “private” range of addresses that we can use inside our home that nobody on the Internet will care about. These address ranges are already set aside by the IANA for private use and will never be routed over the global Internet.

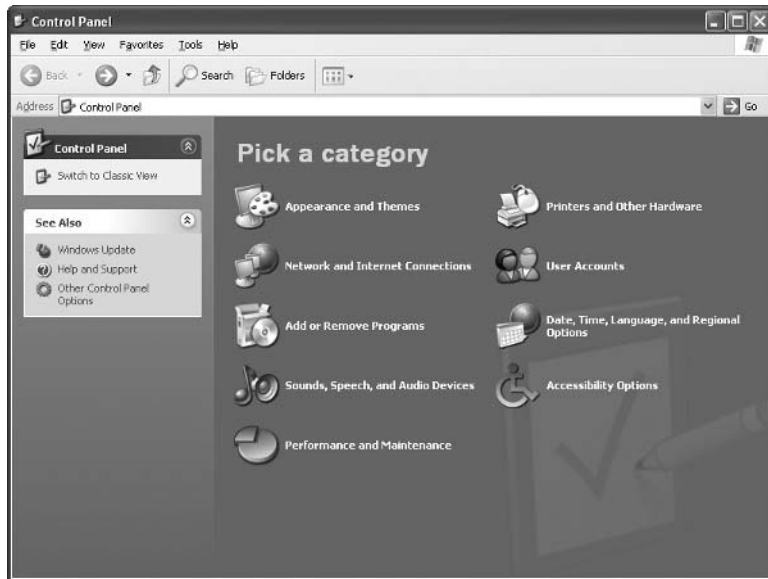
While three private address ranges are set aside for different-sized organizations, we will concentrate on one specific range. This private address range is a collection of small network groups using the first two octets 192 and 168. Addresses 192.168.0.1–192.168.255.254 are possible using this range, but each network will usually stick to the same third octet number, yielding an address range such as 192.168.100.1–192.168.100.254. Of these addresses, 192.168.100.0 is set aside to denote the network ID, and 192.168.100.255 is set aside for communications that are destined for all devices on the network (called broadcasts).

You can safely select an address range using 192.168 and any third octet number from 0 to 255. Each resulting network can support up to 254 devices. You will find when you configure your Internet gateway that it may already use a group of addresses from one of these ranges. Begin by addressing your gateway device with <dot> one, for example 192.168.0.1, and continue with the next number until all your devices are addressed.

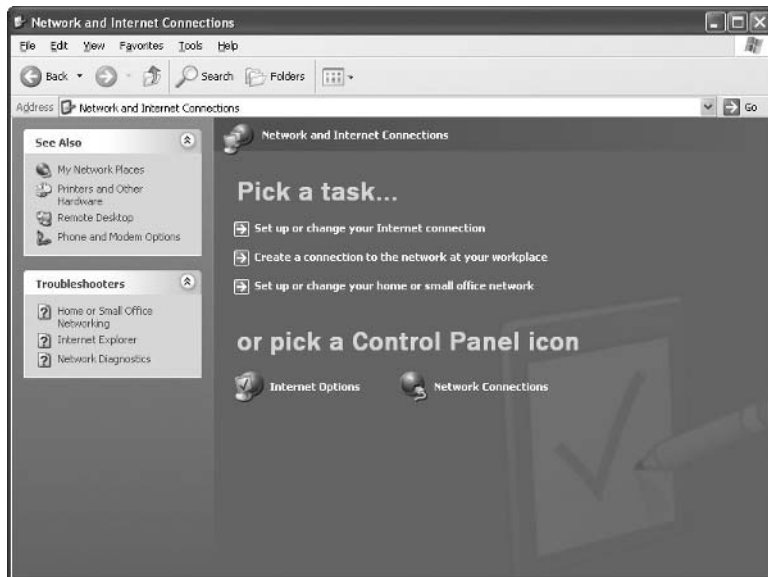
Use Static Addresses

If you are not using an Internet gateway device that includes the ability to dynamically assign addresses, that is to automatically give each device connected to it an address, or if you just like to control things like that yourself, you will use static IP addresses. Using the address range you have selected in the preceding section, configure each device with a unique address. In Windows XP, this is managed in the TCP/IP Properties for the network connection you are using to access the network.

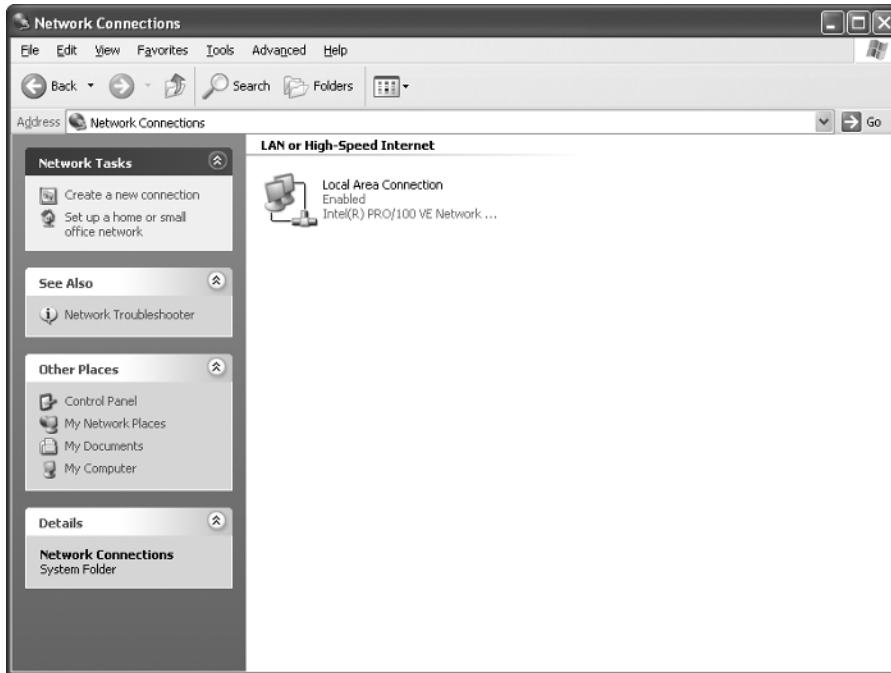
1. From the desktop, click Start and select Control Panel.



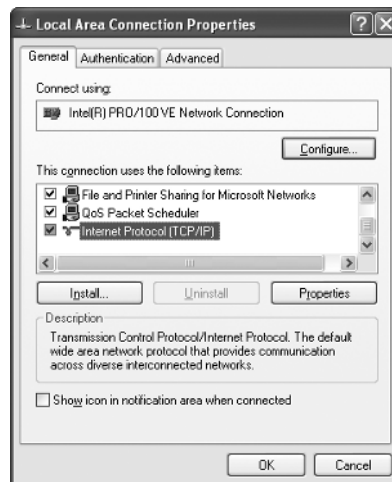
2. Choose Network And Internet Connections to open the Network And Internet Connections area of the Control Panel.



3. Select the Network Connections Control Panel icon at the bottom of the screen. You will see your Local Area Connection icon.



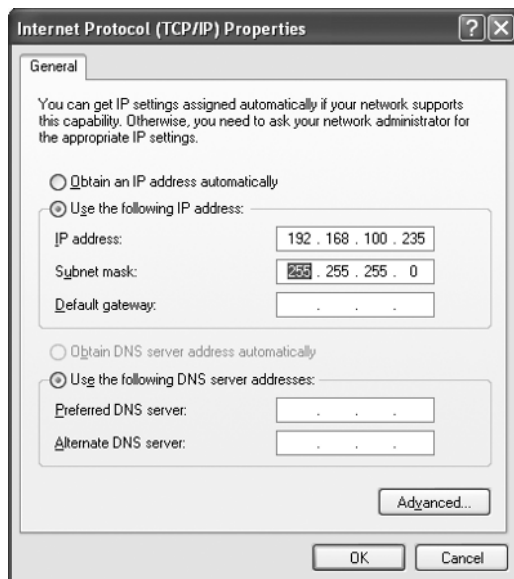
4. Right-click Local Area Connection and select Properties.



5. Select the Internet Protocol (TCP/IP) and click Properties.
6. You will be presented with the following dialog box:



7. Select the Use The Following IP Address option and configure the IP address you have been assigned or have chosen.



8. Use the default subnet mask.
9. Click OK to save this configuration.

You have given your computer a unique address that will allow it to communicate on your network.

How to ...

Use Dynamic Host Configuration Protocol (DHCP) to Assign Network Addresses

By default, Windows XP and most network-attached devices will be configured to get their addresses from a Dynamic Host Configuration Protocol (DHCP) server. Such a server on a corporate network is usually run on one of the network's server computers. In a home network, however, it is usually possible to have the device that provides Internet connectivity (the Internet gateway) function as a DHCP server.

When a gateway device is installed, it will usually default to providing a group of addresses from a range of addresses configured by the manufacturer. This range is usually derived from the 192.168.0.0 private range set aside by the IANA. Computers and other network devices receive an address when they start up and go right to work communicating with each other.

Read the installation instructions provided with your Internet gateway to see which range of addresses is used for this purpose. You can generally also discover these in a table using the gateway's configuration utility. Quite often this is an HTML application accessible by typing the address of your gateway into your web browser's address bar. You will probably find your other network devices using addresses in this range. Most of these devices, such as printers and media devices, will also make your computer aware of them, either by broadcasting their addresses to your computer's My Network Places application or by responding to the setup program included with the device.

Use Dynamic Addresses

If your Internet gateway dynamically assigns addresses, you should be able to connect to it by following the manufacturer's instructions; if that is true, you do not have to configure anything else in Windows XP to enable networking. If you have to manually configure Windows XP for using a dynamically assigned address, follow the preceding instructions, except select Obtain An IP Address Automatically.

Set Up Workgroup Networking

After all your computers and other network devices are communicating on the network, it is time to let your family share files and printers. Using Windows XP to share files and printers is known as *peer-to-peer*, *P2P*, or *workgroup* networking. Windows XP computers are assigned a workgroup during the setup process, or after setup in the System Properties dialog box (see Figure 3-3). Naming the workgroup provides a structure in My Network Places to collect the computers when browsing. Windows XP automatically collects the computers with the same workgroup name into one group in My Network Places. This can make it simpler to find computers near you on a large network. On a home network we are only concerned with workgroups to ensure you do not have any difficulty finding your other computers. You may have more than one workgroup, but a computer may only belong to one workgroup at a time. That said, the workgroup designation merely allows for grouping of computers; it does not prevent a user with proper credentials from accessing resources on a computer in another workgroup.

Name Your Workgroup

Workgroup names may be up to 15 characters long and may contain any alphanumeric (a–z and 0–9) characters, as well as special characters except for ; : " < > * + = \ | ?.

Name Your Computers

Computer names can be up to 15 characters long and have the same naming restrictions as workgroups. In addition, the computer name cannot be the same as the workgroup name.

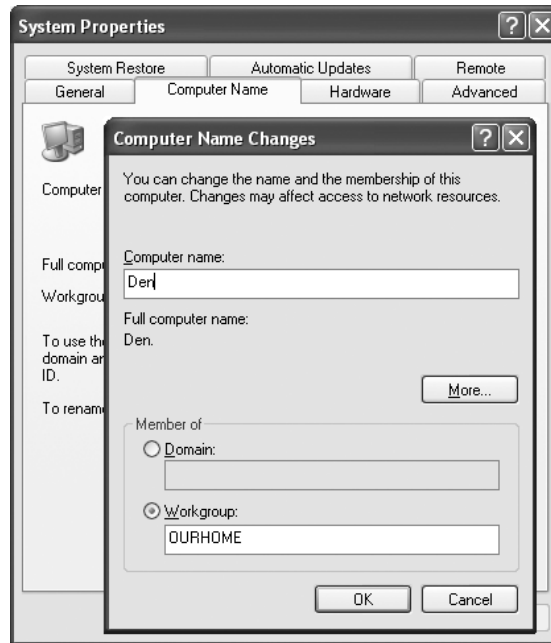


FIGURE 3-3 Naming your workgroups and computers

Share Your Files and Printers

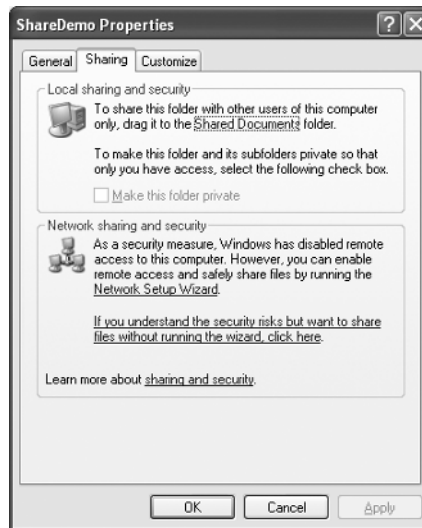
Windows XP uses a method of sharing files called Simple File Sharing. If you use Windows XP Home Edition, you will always use Simple File Sharing, but if you have Windows XP Professional, you have the option to turn it off and use passwords to further restrict access to shared files and folders.

Enable Windows XP Simple File Sharing

Since Windows XP Home Edition always uses Simple File Sharing, and Windows XP Professional Edition uses it by default, we will stick with it in all our descriptions. If for some reason you are using Windows XP Professional Edition and it is turned off, you may enable it by going to the Tools menu in Windows Explorer and selecting Folder Options. Select the View tab and scroll to the bottom of the options. Check the box next to Use Simple File Sharing (Recommended).

To share files with Windows XP with Simple File Sharing enabled, follow these steps:

1. Right-click the folder you wish to share and select Sharing And Security. You will see the following dialog box:

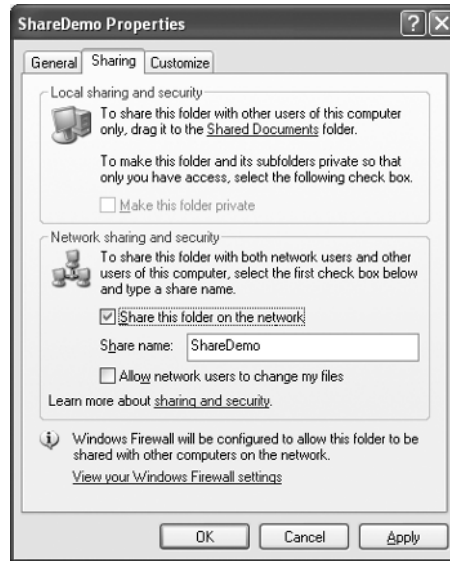
**NOTE**

If the folder dialog does not look this way, network file sharing may already be enabled. Attempt to continue the procedure with the next step.

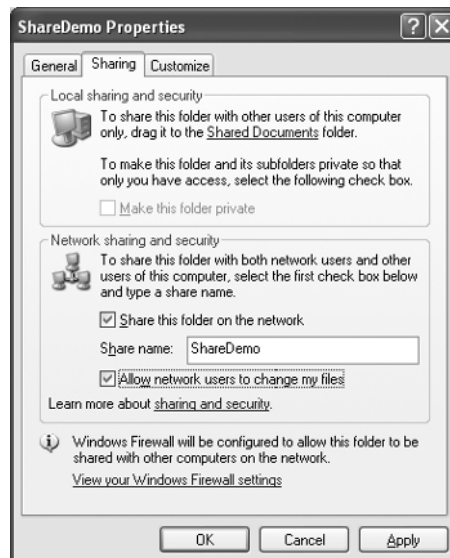
2. Click "If you understand the security risks but want to share files without running the wizard, click here." This will activate file and printer sharing on this computer. You might choose to run the Network Setup Wizard, but most of the steps the wizard accomplishes, such as enabling file sharing are already done, and it is too easy to have it change something for the worse. The Network Setup Wizard can establish configurations that are not compatible with file sharing (or home networking, for that matter). After clicking the preceding message, you will see the following dialog box:



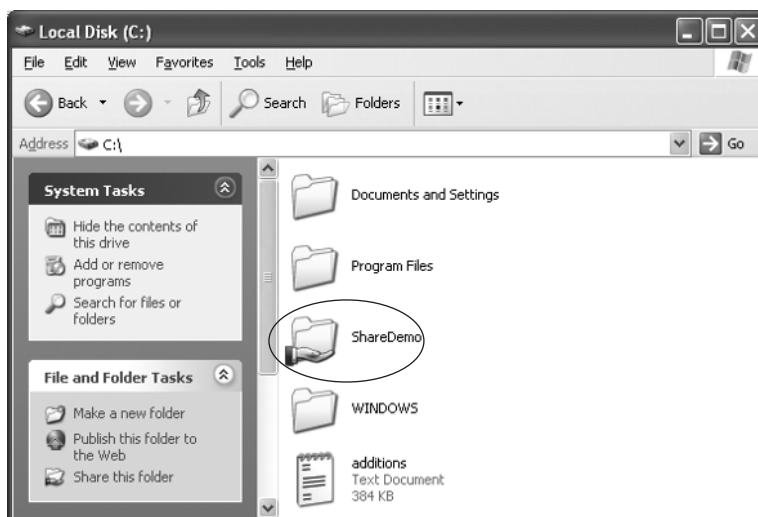
3. Choose Just Enable File Sharing. You will then see the following change to the folder's Properties dialog box:



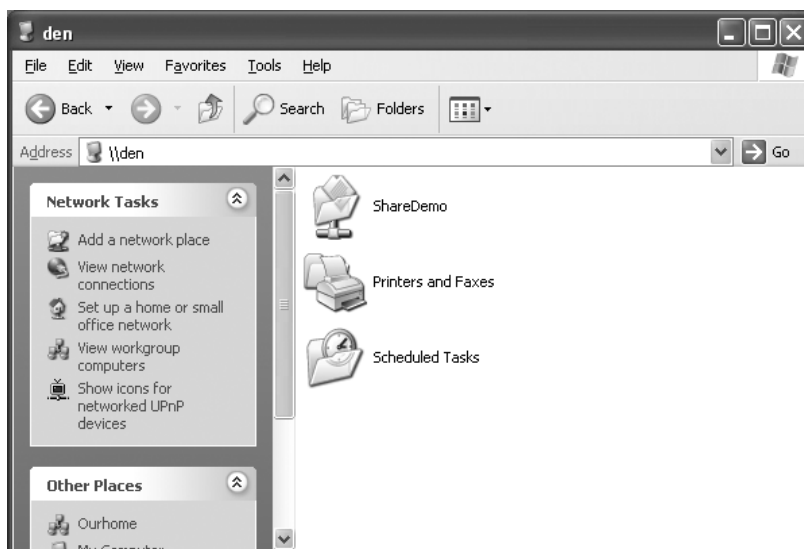
4. This folder is now set to share files with “read only” security. Users can read them but not change them. If you wish to allow users to change files, click the check box next to Allow Network Users To Change My Files.



5. After clicking OK, you will see a “sharing hand” under the folder.



Network users will see the following when they browse to your computer in My Network Places:



Share Your Printer

Sharing a printer is very similar to sharing your folder.

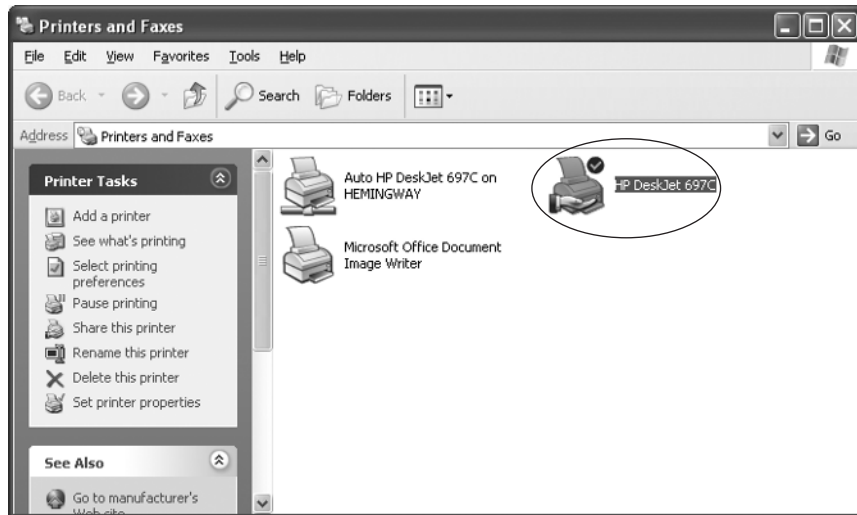
1. Right-click the printer you wish to share and select Sharing. You will see the following dialog box:



2. Select Share This Printer. Provide a name for the shared printer.



3. Click OK, and the “sharing hand” will appear under your printer.



Connect Your Network to the Internet

Connecting your network to the Internet is the next logical step in getting everybody online. If you have installed an Internet gateway, chances are that you are already online. The instructions that come with the gateway are all you need to get the job done. If you need assistance with this setup, the manufacturer of the gateway and the technicians at your ISP are able to get you set up right. Due to the variations in settings and connection options, we cannot cover all the possible combinations here.

In this section we will show you how to share an Internet connection when you do not have an Internet gateway device. Windows XP Internet Connection Sharing allows your computer to function as an Internet gateway.

Configure and Share a Direct Internet Connection

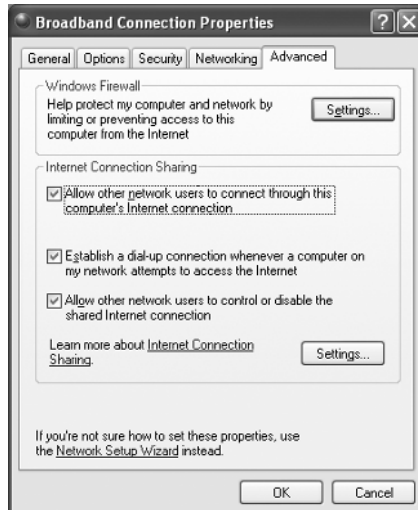
If you do not have a gateway, connect directly to broadband, or have a dial-up connection to the Internet, you can still have all your computers access the Internet. We will show you how to share this connection with all the computers on your home network.

1. Begin by finding your connection on the Network Connections folder. You can locate this by navigating to Start, clicking All Programs, moving to Accessories and then Communications, and selecting Network Connections.
2. Right-click your Internet connection and select Properties. Click the Advanced tab and you will see the following dialog box:

3



3. Click “Allow other network users to connect through this computer’s Internet connection.”



If you are curious about how Internet Connection Sharing works, you can read the help link provided by [Learn More About Internet Connection Sharing](#), but you are essentially done. If you try to connect to the Internet from another (client) computer, you will see the computer on which you just enabled sharing (the server) dial your Internet connection, and then the client computer will begin to display web pages.

NOTE

Enabling Internet Connection Sharing will change your IP address to 192.168.0.1 and enable a simple DHCP server on your computer. If you have already chosen another IP address range, you will have to reconfigure any Static IP addresses you may have configured. Your devices and computers with dynamically set IP addresses will change next time you start them, and they will then be able to access the Internet.

Chapter 4

Install a Wireless Network



How to...

- Select Wireless Network Devices
- Determine Placement of Wireless Network Devices
- Configure Wireless Network Devices
- Connect Your Wireless Network to the Internet
- Share Files and Printers on Your Wireless Home Network

If wired Ethernet or the other wired alternatives do not work for your home network, or you crave the mobility only wireless networking can give, you will be found wandering the aisles of wireless network equipment at your local big-box computer retailer. In this chapter we will discuss what you should bring home from the store and what to do with it once you have it home. We will determine placement of your devices and how to get them all to work together. Finally, we will connect the whole network to the Internet.

Select the Proper Wireless Ethernet Equipment

We discussed wireless network devices in Chapter 2. In this section we will elaborate on some of the decisions you might make and how they will affect the layout of your network.

Choose the Device Types for Your Home Network

Many types of wireless Ethernet devices are now available for a variety of uses. In this section we concentrate on infrastructure devices such as adapters, bridges, and access points. We will help you decide which of the equipment in the wireless aisle to bring home.

Internal vs. External Wireless Adapters

If you are the type who really doesn't want to know what the inside of your computer looks like, you will definitely want to choose an external wireless Ethernet adapter. These connect to your computer's USB port and can be placed on or near your computer. If you have signal strength issues, an external adapter affords you greater flexibility in device placement for optimum signal strength.



If you don't mind seeing your computer's innards, need to conserve USB ports, or like everything nice and neat with fewer cables, you will most likely choose an internal wireless Ethernet adapter. You will have less flexibility in device placement (your computer will not appreciate sitting on a bookshelf), but you will also not have to deal with an extra cable in the nest behind your computer.



Finally, if your computer is a notebook or tablet PC, you will probably opt for a PC Card adapter. It's not really internal, not really external.



Bridges

One last option, for wirelessly connecting a computer (or other network device) that has a wired Ethernet port, is a wireless Ethernet bridge. This device converts (or bridges) the wired Ethernet signal to an 802.11 wireless signal for use with your wireless network.



Access Points vs. Gateways

If you already have an Internet-sharing device such as a wired Ethernet gateway, you can give wireless network devices access to it by adding a wireless Ethernet access point to your network.



If you do not already have the Internet access issues solved, there are many excellent gateway devices that provide wireless Ethernet, wired Ethernet, even Phoneline network access as well as security features such as firewalls.



Choose Your Wireless Ethernet Protocol

Wireless Ethernet for consumer applications currently supports three different wireless standards: 802.11a, 802.11b, and 802.11g. In this section we will evaluate the differences and help you choose the one that best fits your needs.

802.11a: Less Interference

The 802.11a standard is the black sheep of the 802.11 standards. It operates on a totally different frequency range (5 GHz versus 2.4 GHz) and is not forward or backward compatible with any other protocol. There will be fewer devices competing for the same airwaves with your wireless devices. On the down side, its higher frequency penetrates less and therefore suffers from higher signal loss due to attenuation. Distances of over 60 feet will be a challenge. Bandwidths of up to 54 megabits per second (Mbps) are possible with this standard.

802.11b: Better Compatibility

The 802.11b standard is most widely used for wireless Ethernet, and most specialty wireless equipment uses it. Its 2.4 GHz signal penetrates better than 802.11a, but it has more competition for the frequency range, competing with cordless phones, wireless remote controls, and some security systems. Its speed, up to 11 Mbps, is slower, but fine for web browsing and most home network uses. Its lower frequency allows for better penetration of materials, giving up to 300 feet of coverage.

802.11g: Speed and Compatibility

The 802.11g standard is a second-generation 2.4 GHz standard. It supports speeds of up to 54 Mbps and is backward compatible with devices using 802.11b. It suffers from the interference concerns of 802.11b but offers greater penetration (up to 300 feet) than 802.11a with equal speed.

Standard	Frequency Band	Range ¹	Speed ²
802.11a	5 GHz	Up to 75 feet	Up to 54 Mbps
802.11b	2.4 GHz	Up to 300 feet	Up to 11 Mbps
802.11g	2.4 GHz	Up to 300 feet	Up to 54 Mbps

¹Range subject to attenuation and interference.

²Speed subject to distance, attenuation, and interference.

The Advantages of Multiprotocol Devices

You can find 802.11a/g and 802.11a/b devices that allow you to use the two protocols interchangeably. These devices are more expensive to buy but also support the greatest range of possible uses. An 802.11a/g device will actually support all three standards, due to the backward 802.11b compatibility of 802.11g. Devices supporting 802.11g may also be marketed as 802.11b/g devices for the same reason.

Breaking the Speed Limit

Beginning with 802.11b, some manufacturers have included proprietary channel-bonding techniques to effectively double the throughput of their devices. What this means for the consumer is that *if* you buy only that manufacturer's devices, you can enable the speed-doubling technology. This function goes by different names:

- Xtreme G (108 Mbps 802.11g)
- Super G (108 Mbps 802.11g)
- Turbo (22 Mbps 802.11b)

The common denominator here is that there is no common denominator between manufacturers. If you plan to use channel bonding, use devices all from one manufacturer.

CAUTION

Channel bonding may cause interference with other networks close by, so you might want to just check with the neighbors when you enable Super G to make sure they are still online!

Place Your Wireless Network Devices for Best Reception

Radio waves are affected differently by materials through which they pass. Cloth and wood block them very little (unless these materials are wet), while concrete, stone, and metal can absorb or even reflect the signal. Wireless Ethernet in the 2.4 GHz band, for instance, is readily absorbed by materials containing water, effectively blocking the signal.

Sources of Radio Interference

Cordless phones, radio frequency wireless remotes, and even some security systems can interfere with the 2.4 GHz signals used by wireless Ethernet devices using the 802.11b and g standards. Cordless phones are beginning to appear in the 5.8 GHz bands (the upper end of 802.11a's range) as well, so interference is beginning to build there, too.

For best range, limit the number of devices that use the same frequency band. For instance, choose a 5.8 GHz cordless phone if you are using 2.4 GHz 802.11b or 802.11g devices.

Causes of Signal Attenuation

As mentioned previously, many materials absorb and reflect radio waves. The loss of signal strength in this manner is referred to as *attenuation*. The higher a radio frequency is, the more easily it is attenuated by materials.

Some big attenuators are

- Water (found in wet clothing, plants, aquariums, and people)
- Metal (found in large appliances, stucco, and reinforced concrete)
- Stone (many rocks have high metallic and/or water content).

To minimize signal attenuation, try to position devices to minimize the amount of attenuating material between them. Use the flashlight trick mentioned in Chapter 2. Shine a pretend flashlight around and visualize what the beam would have to pass through to reach your wireless network devices. Rearrange devices that would experience high attenuation, or consider possible strategies for extending your range.

Strategies for Extending Signal Range

You can extend the range of your wireless network in two ways. You can increase your wireless device's range with an antenna, or you can add additional access points to increase your coverage zone.

Extend Your Range with Antennas

Antennas are available for many wireless Ethernet devices to increase effective range, sometimes dramatically. Antennas are available in two basic types: omnidirectional antennas that boost signals coming from all directions, and unidirectional antennas that boost signals from a single direction only. In general, unidirectional antennas offer the greatest improvement, as they also serve to limit interference by pointing directly at a single source.

NOTE

Some folks have built their own “cantenna” for wireless Ethernet. Starting with a cashew can and a potato chip can, you can build a unidirectional antenna. Instructions are found on the Internet by searching for cantenna. Will it be better than “store-bought”? Probably not. But it is a fun experiment in radio, and if done right it can inexpensively extend the range of your network.

Use Repeaters to Extend Your Coverage

Another way to increase your network's footprint is by adding repeaters. A *repeater* is a device that listens for signals from a wireless access point or client and then amplifies and retransmits them. Adding repeaters can allow you to extend your network into areas with poorer signals, increasing the signal strength and speed of communications in those areas.

Configure Your Wireless Network Devices

The specifics of configuring wireless Ethernet devices vary by device type and manufacturer. In this section we will cover some of the configuration options you should keep an eye out for so that you know if you are missing anything. Some of this information will be presented again in much more depth in Chapter 6. We present it here to get your network up and running, but *do not rest* until you have taken care of the security. An unprotected wireless network is like going to bed with your garage door open. You never know what you will find in there in the morning.

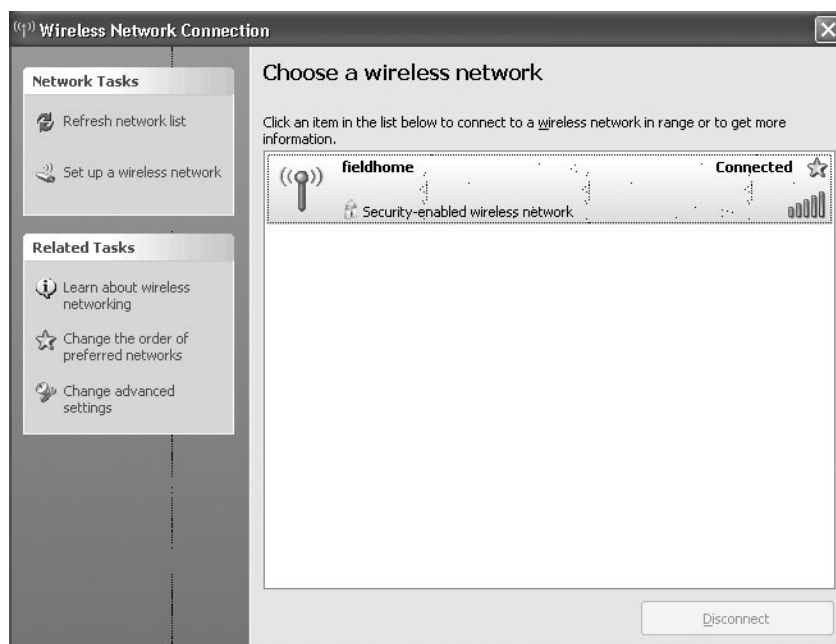
Find a Clear Channel

Begin your wireless configuration by finding an open channel. Nearby wireless networks can be using default channels and would cause interference with your own. Finding a clear channel can be accomplished with the equipment you bring home.

Perform a Site Survey

Site surveys are performed by professional installers to determine where to place access points and repeaters. They walk around the installation site recording signal strength with a notebook or Pocket PC equipped with a wireless Ethernet card and wireless scanning software. They then identify weak spots and add repeaters or additional access points where they are required.

You can approximate this by using your wireless laptop. Fire up Windows XP and open the Network Connections Control Panel applet. Right-click your wireless adapter and select View Available Wireless Networks. If you don't have a laptop, a survey can still be accomplished by using your desktop computer. Watch your available networks for a while and see how strong the signals are from nearby networks.

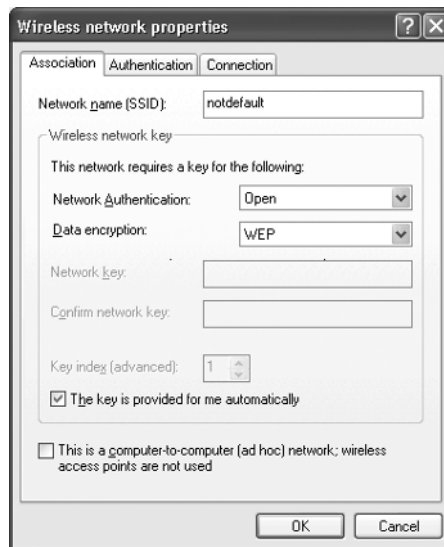


If you see other networks, note which channels they are using. When you configure your wireless access points or gateway, choose a channel that is not in use nearby. This will reduce interference from the neighboring networks.

Configuring a Service Set ID (SSID)

Your wireless networking devices come with a default Service Set Identifier (SSID) that is set in the factory. These are well known to those who might want to penetrate your network and will be used along with popular encryption keys to attempt to get in.

Choose a new SSID and configure your equipment with it. Each device will include instructions for configuring the SSID. You can even turn off SSID broadcast, lowering your network's profile to casual observers. It will not completely hide your network from someone who is looking for it, but it is a good start.



NOTE

Disabling SSID broadcast in your access points and gateways can make earlier versions of Windows XP wireless auto-configuration malfunction. If you experience this, obtain and install the latest Windows XP service pack.

Enabling Encryption

Wireless Ethernet devices now available support encrypted communications. Encrypting your data makes it harder for crackers to penetrate your defenses. In this section we will discuss Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

Wired Equivalent Protection (WEP)

Wired Equivalent Privacy (WEP) is the most widely used encryption standard now available for wireless networks. It is accomplished by configuring each device with an encryption key. These keys are available in 40-bit, 128-bit, and even 256-bit key lengths. The numbers of bits just indicate the relative length (complexity) and therefore strength of the key. The device uses that key to encrypt data it sends on the network and decrypt data received from the network. WEP has had some high-profile deficiencies exposed recently, but it remains the only choice for many until its apparent successor, WPA, is available on all devices.

To enable WEP, use the configuration tools provided with your wireless devices to create a key. Enter the key in the configuration of each device on the network to enable encrypted communications.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is an extension to WEP that adds the ability to authenticate the initial connection and assign the initial key automatically. After that, the key is changed periodically by the Temporal Key Integrity Protocol (TKIP), which is part of the WPA standard.

WPA is designed to use a server-based authentication scheme called RADIUS (Remote Authentication Dial-In User Service) to authenticate users to the network. If they are accepted, their network adapter receives the initial encryption key, and the TKIP is initialized. After that, the keys are changed periodically by the TKIP. This prevents penetration by changing keys faster than they can possibly be broken.

Users without RADIUS servers can still make use of WPA. WPA includes the ability to manually designate an initial key for devices using WPA. This is similar to the static WEP key. It is used only until TKIP is initialized and begins rotating keys.

NOTE

For much more on wireless Ethernet security, please refer to Chapter 6.

Connect Your Wireless Network to the Internet

If you are using a wireless Internet gateway, chances are you have already established your Internet connection. If not, you can work with your Internet service provider (ISP) to configure your Internet connection to support your gateway.

Be up front about what you are doing. Most ISPs will cheerfully help you get your network online. Some ISPs will not be happy about your connecting an entire network to their relatively inexpensive connection. If you get too much flak, just find a more cheerful ISP.

Configure Your Internet Gateway

Your Internet gateway will be configured with default settings to enable multiple computers to receive IP addresses and communicate with the Internet. If you plan to enable encryption, rename your default SSID, or disable SSID broadcast, consult the device manufacturer's instructions on how to accomplish this. Figure 4-1 shows a Linksys configuration screen to give you an idea of what you will see.

Enable DHCP to Control IP Addresses

By default your gateway should provide IP addresses to connected clients using the Dynamic Host Configuration Protocol (DHCP). If this is not the case, consult the manufacturer's instructions to determine how to enable this.

Configure Clients for Dynamic IP Address Allocation

You might have to configure your Windows XP computers to receive dynamically allocated IP addresses. To configure Windows XP to receive an IP address automatically,

LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: 1.00.10

Setup Wireless B Broadband Router HW1W154

Setup Wireless Security Applications & Gaming Administration Status

Basic Setup Advanced Routing

Internet Setup

Internet Connection Type: PPPoE

User Name: snabuddy

Password: [REDACTED]

☒ Connect on Demand: Max Idle Time 0 Min

☐ Keep Alive: Redial Period 30 Sec

Host Name: [REDACTED]

Domain Name: [REDACTED]

MTU: ☒ Enable ☐ Disable Size: 1492

Network Setup

Router IP

Local IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Local DHCP Server: ☒ Enable ☐ Disable

Start IP Address: 192.168.2.100

Number of Address: 50

DHCP Address Range: 192.168.2.100 - 140

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0.0.0.0

Static DNS 2: 0.0.0.0

Static DNS 3: 0.0.0.0

WINS: 0.0.0.0

Basic Setup

The Basic Setup screen is where basic configuration is performed. Some ISPs (Internet Service Providers) will require that you enter the DNS information. These settings can be obtained from your ISP. After you have configured these settings, you should set a router password from the Administration > Management screen.

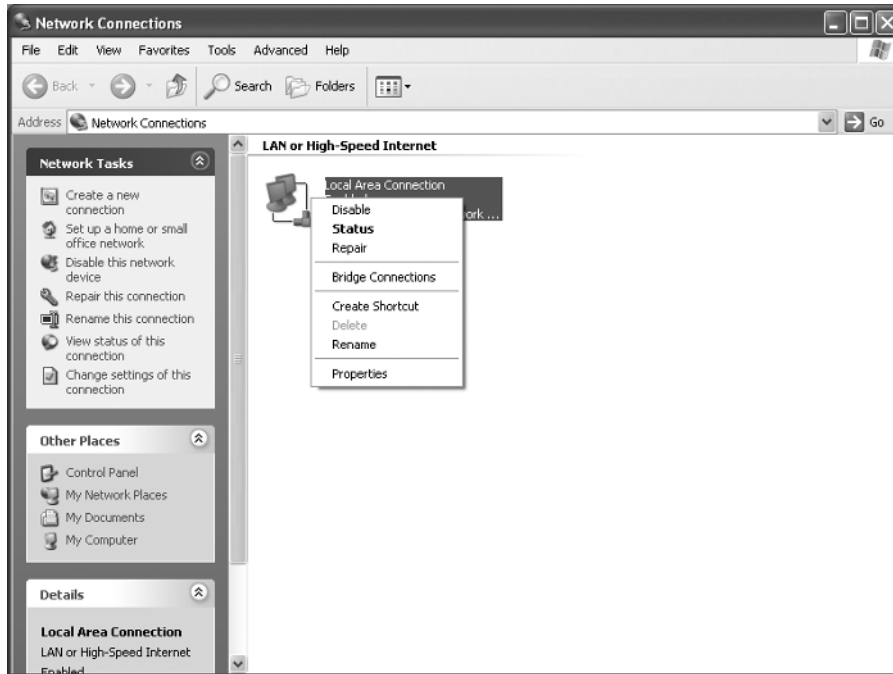
Completing the Internet Setup section is all that is required to set up for your specific ISP. Please look at the table below to configure the Router for your Internet connection.

More...

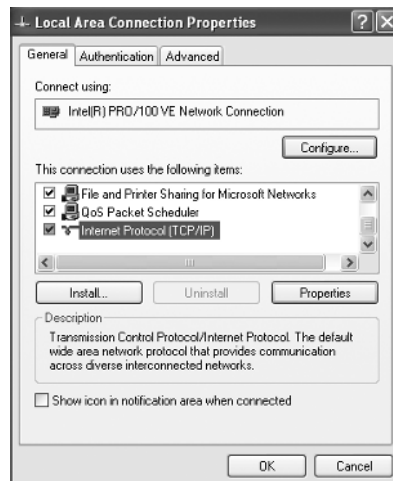
Save Settings Cancel Changes

FIGURE 4-1 Configuring a Linksys Internet gateway

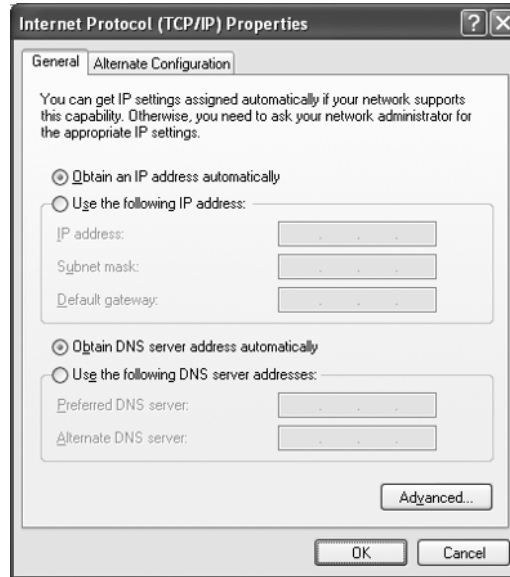
1. Open the network adapter's Properties dialog box by right-clicking the appropriate network connection icon in Network Connections and selecting Properties.



2. Find and select Internet Protocol (TCP/IP) and click Properties.



3. Select both the Obtain An IP Address Automatically and Obtain DNS Server Address Automatically options and click OK.



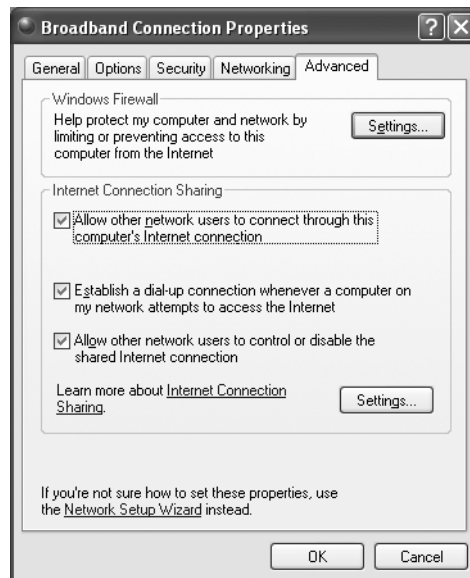
Going Online Without a Gateway

Just as with a wired Ethernet Network, you can use the Internet Connection Sharing capabilities built into Windows XP to share your Internet connection. Begin by finding your connection on the Network Connections folder. You can locate this by navigating to Start, clicking All Programs, moving to Accessories and then Communications, and selecting Network Connections.

1. Right-click your Internet connection and select Properties. Click the Advanced tab and you will see the following dialog box:



2. Click “Allow other network users to connect through this computer’s Internet connection.”



If you are curious about how Internet Connection Sharing works, you can read the help link provided by Learn More About Internet Connection Sharing, but you

are essentially done. If you try to connect to the Internet from another computer, you will see your computer dial your Internet connection, and then the other computer will begin to see web pages.

NOTE

Enabling Internet Connection Sharing will change your IP address to 192.168.0.1 and enable a simple DHCP server on your computer. If you have already chosen another IP address range, you will have to reconfigure any static IP addresses you may have configured. Your devices and computers with dynamically set IP addresses will change next time you start them and will then be able to access the Internet.

Configure Your Computers for Home Networking

This section is discussed in detail in Chapter 3, but we will reprise it here with a wireless angle.

Manage TCP/IP Addressing

If you are using an Internet gateway or have enabled Internet Connection Sharing, you will not need to manually assign IP addresses to your devices. If you do not want to use dynamic address assignment, you will have to configure your devices' addresses manually.

Select Your Network's Address Range

To communicate effectively, each device on a network requires a unique address. This allows other devices to direct data to it without fear that the data will arrive at the wrong location. On the global Internet, each connected device has an address—called an Internet Protocol (or IP) address—that belongs to no other device in the world. Obviously, it takes some level of management to ensure that no two devices use the same address. This task is shouldered by the Internet Assigned Numbers Authority (IANA) and your Internet service provider (ISP). When you connect a computer or network to the Internet, you are assigned an address by your ISP from a block given them by the IANA.

Connecting multiple devices to the Internet would require you to be assigned an address for each device. Your ISP would want to charge you for each individual connection, and you would use a large number of global IP addresses for your devices. If each household did this, we would run out of addresses very quickly. For this reason, we can choose to have a “private” range of addresses that we can use inside our home that nobody on the Internet will care about. These address ranges are already set aside by the IANA for private use and will never be routed over the global Internet.

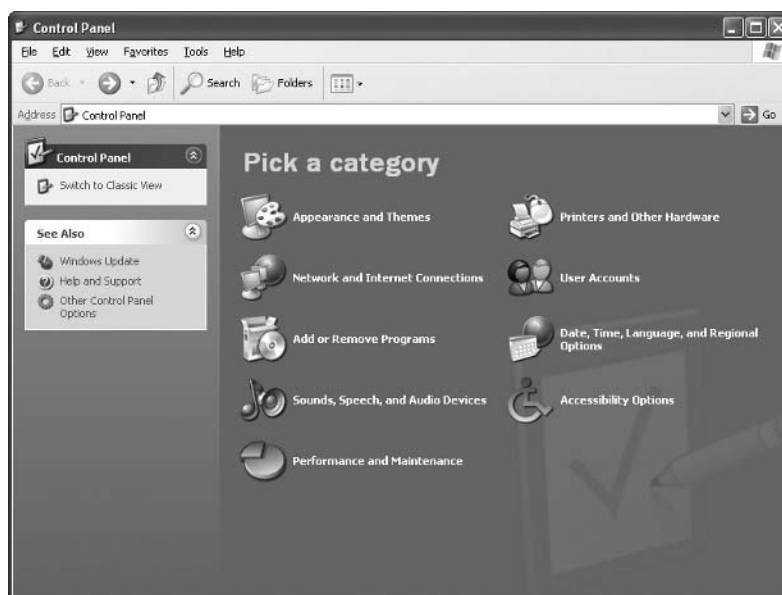
While there are three ranges set aside for different-sized organizations, we will concentrate on one specific range. This range is a collection of small network groups using the first two octets (so-called because they're 8-bit numbers) 192 and 168. Addresses 192.168.0.1–192.168.255.254 are possible using these ranges, but each network will usually stick to the same third octet number, yielding an address range such as 192.168.100.1–192.168.100.254. The address 192.168.100.0 is set aside to denote the network ID, and 192.168.100.255 is set aside for communications that are destined for all devices on the network (called a broadcast).

You can safely select an address range using 192.168 and any third octet number from 0 to 255. Each resulting network can support up to 254 devices. You will find when you configure your Internet gateway that it may already use a group of addresses from one of these ranges. Begin by addressing your gateway device with <dot> one, and continue with the next number until all your devices are addressed.

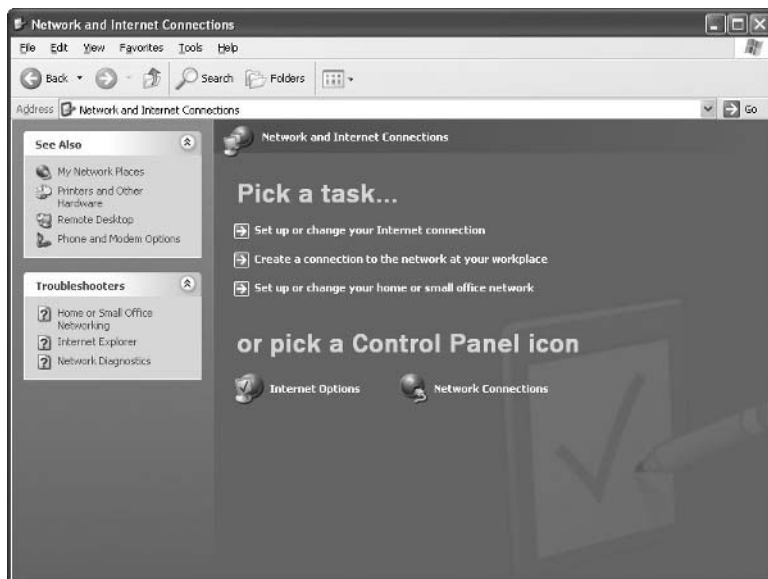
Use Static Addresses

If you are not using an Internet gateway device that includes the ability to dynamically assign addresses, or you just like to control things like that yourself, you will use static IP addresses. Using the address range you have selected in the preceding section, configure each device with a unique address. In Windows XP, this is managed in the TCP/IP Properties for the network connection you are using to access the network:

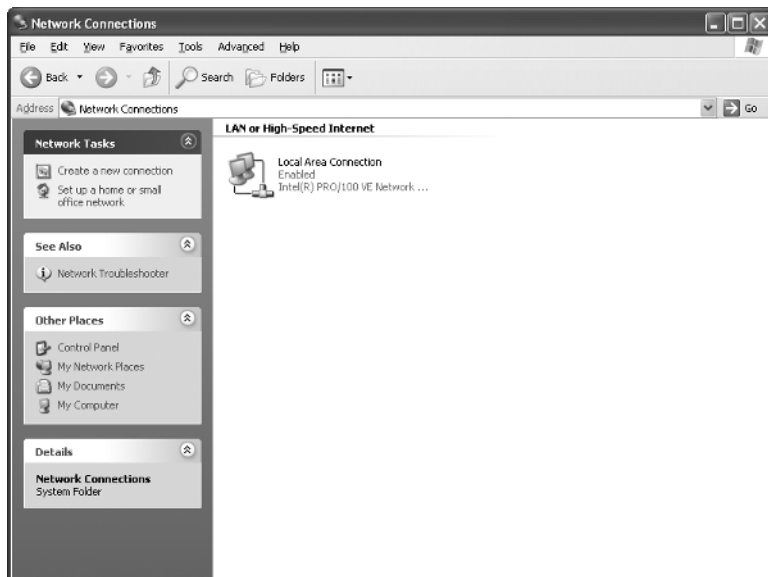
1. From the desktop, Click Start and select Control Panel.



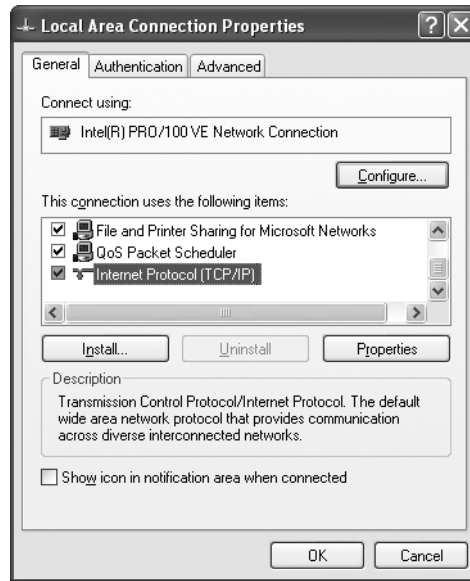
2. Choose Network and Internet Connections to open the Network And Internet Connections area of the Control Panel.



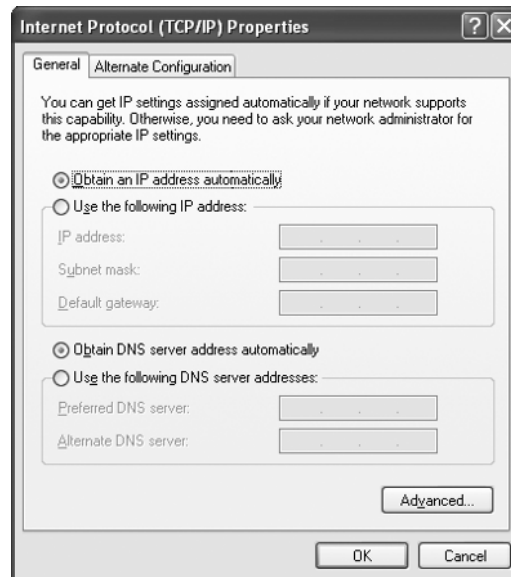
3. Select the Network Connections Control Panel icon at the bottom of the screen. You will see your Local Area Connection icon.



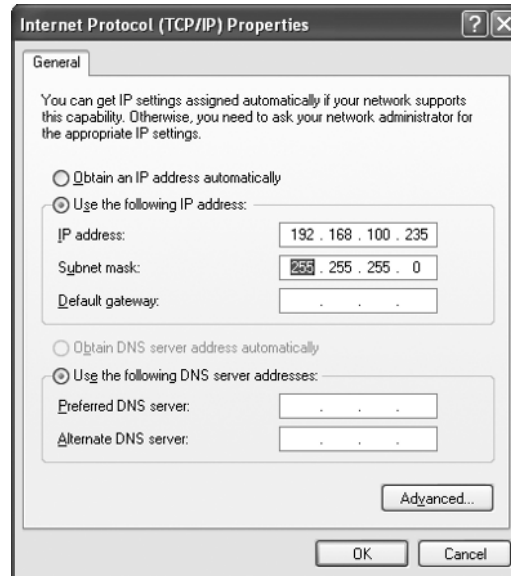
4. Right-click Local Area Connection and select Properties.



5. Select the Internet Protocol (TCP/IP) and click Properties. You will be presented with the following dialog box:



6. Select the Use The Following IP Address option and configure the IP address you have chosen.



7. Use the default Subnet mask.
8. Click OK to save this configuration.

You have addressed your computer to be able to communicate on your network. As you configure more devices, and when you configure your computer or network to communicate on the Internet, you will want to modify these settings. We will discuss any necessary modifications later, when you connect to the Internet.

Use Dynamic Addresses

If your Internet gateway dynamically assigns addresses, you should be able to connect to it by following the manufacturer's instructions; if that is true, you do not have to configure anything else in Windows XP to enable networking. If you have to manually configure Windows XP for using a dynamically assigned address, follow the preceding instructions, except select Obtain An IP Address Automatically.

Set Up Workgroup Networking

After all your computers and other network devices are communicating on the network, it is time to let your family share files and printers. Using Windows XP computers to share files and printers is known as peer-to-peer, P2P, or workgroup networking. Windows XP computers are assigned a workgroup during setup, or after setup in the System Properties dialog box. Naming the workgroup provides a structure in My Network Places to collect the computers when browsing. You may have more than one workgroup, but a computer may belong to only one workgroup at a time. That said, the workgroup designation merely allows for grouping of computers; it does not prevent a user with proper credentials from accessing resources on a computer in another workgroup.

In this section we will discuss the configuration of the built-in file and printer sharing capabilities of Windows XP. This information is very similar to that found in the preceding chapter. It has been verified for wireless networks.

Name Your Workgroup

Workgroup names may be up to 15 characters long and may contain any alphanumeric (a–z and 0–9) characters, along with special characters except for ; : " < > * + = \ | ?.



Name Your Computers

Computer names can be up to 15 characters long and have the same naming restrictions as workgroups. In addition, the computer name cannot be the same as the workgroup name.

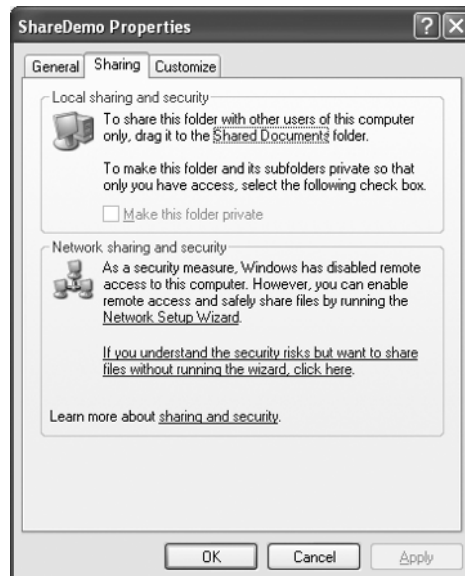
Share Your Files and Printers

Windows XP uses a method of sharing files called Simple File Sharing. If you use Windows XP Home Edition, you will always use Simple File Sharing; if you have Windows XP Professional, you have the option to turn it off and use passwords to further restrict access to shared files and folders.

Enable Windows XP Simple File Sharing

Since Windows XP Home Edition always uses Simple File Sharing, and Windows XP Professional Edition uses it by default, we will stick with it in all our descriptions. If for some reason you are using Windows XP Professional Edition and it is turned off, you may enable it by going to the Tools menu in Windows Explorer and selecting Folder Options. Select the View tab and scroll to the bottom of the options. Check the box next to Use Simple File Sharing (Recommended).

To share files with Windows XP with Simple File Sharing enabled, right-click the folder you wish to share and select Sharing And Security. You will see the following dialog box:

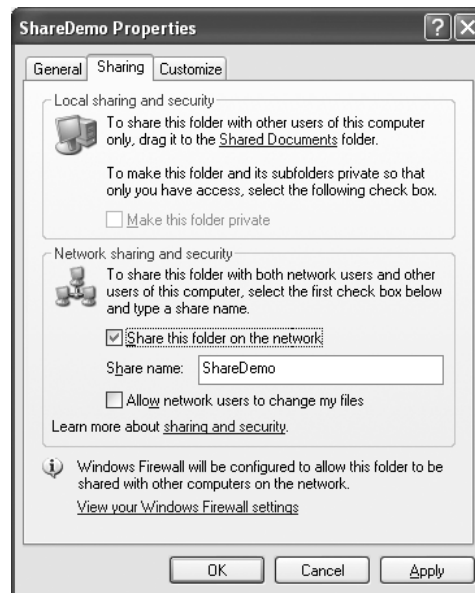


Click “If you understand the security risks but want to share files without running the wizard, click here.” This will activate file and printer sharing on this computer. You might choose to run the Network Setup Wizard, but most of the steps the wizard accomplishes are already done, and it is too easy to have it change something for the worse.

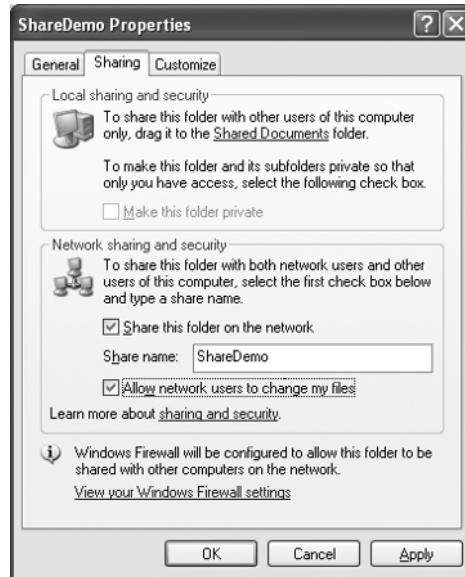
1. After clicking the preceding message, you will see the following dialog box:



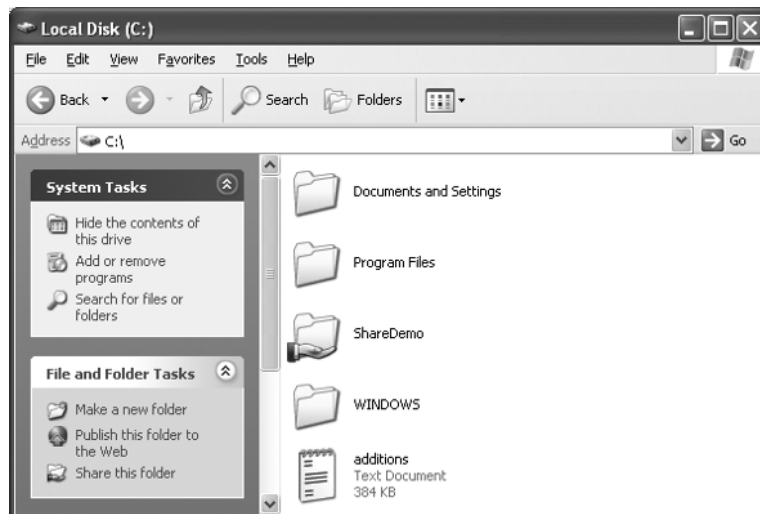
2. Choose Just Enable File Sharing. You will then see the following change to the folder's Properties dialog box:



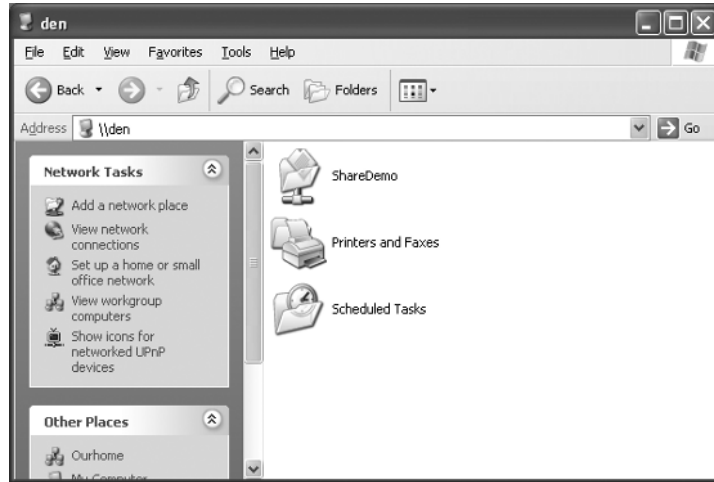
3. This folder is now set to share files with “read only” security. Users can read them but not change them. If you wish to allow users to change files, click the check box next to Allow Network Users To Change My Files.



4. After clicking OK, you will see a “sharing hand” under the folder.



5. Network users will see the following when they browse to your computer in My Network Places:



4

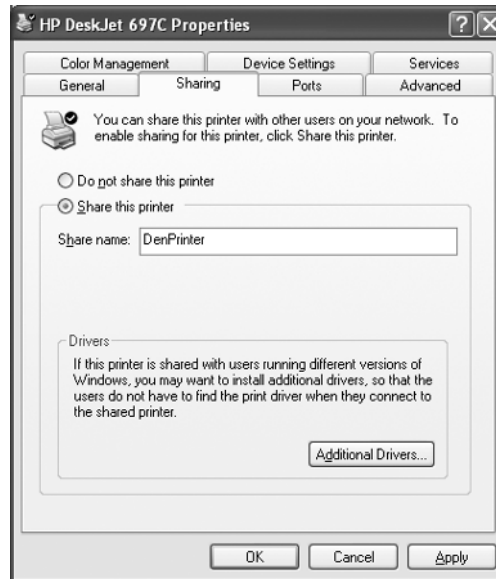
Share Your Printer

Sharing a printer is very similar to sharing your folder. Right-click the printer you wish to share and select Sharing.

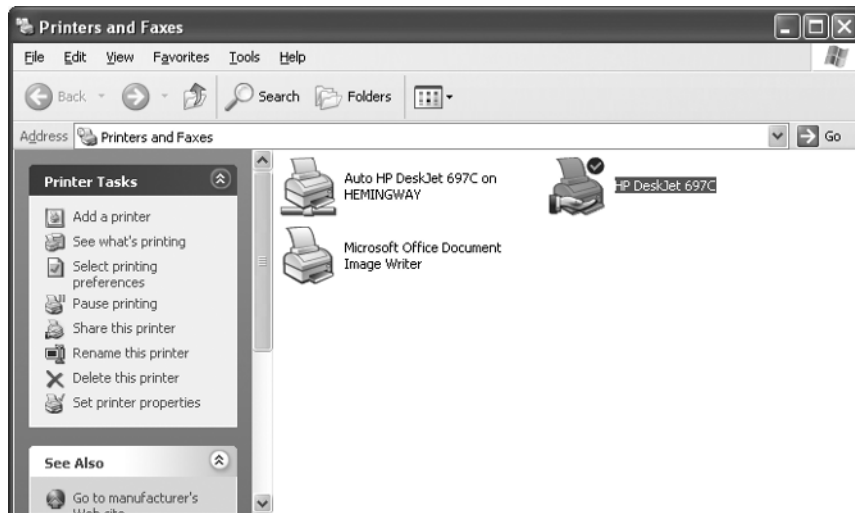
1. You will see the following dialog box:



2. Select Share This Printer. Provide a name for the shared printer.



3. Click OK, and the “sharing hand” will appear under your printer.



Part II

Shut the Door on Hackers



This page intentionally left blank

Chapter 5

Keep Your Internet Connections Secure



How to...

- Define your exposure to Internet security risks
- Use native security tools in Windows XP to protect your network
- Use third-party security tools to protect your network
- Provide “defense in depth” for your home network

If you have successfully configured an Internet connection for your network, great! Now, *shut it down until you have read this chapter*. We are going to show you what you risk by using the Internet, and how to protect your network from hackers, thieves, and other online predators. We will explore the threats they pose and the tools they use. We will then show you how to counter each threat and sleep at night knowing your network is protected.

Internet Security Risks for Home Networks

Corporate Information Technology departments face risks from online attacks daily and use a wide variety of security tools and practices to protect their information assets. Many home users see the effort that goes into protecting a corporate network and shy away from it, either leaving their networks completely unprotected or staying offline and missing out on many of the benefits available by using the power of the Internet.

Home networks are very different from corporate networks. For one thing, they seldom have to support the array of services such as e-commerce store fronts, database applications, and enterprise resource planning (ERP) systems that corporate networks do. This dramatically lowers their threat profile (the relative risk to attack they face). The fewer services and application interfaces you support, the smaller the target you provide for attackers.

Many home networks will access the Internet only as a client. This greatly simplifies security, as they have no reason to ever allow inbound traffic they did not expressly invite. Users who do accept some inbound connections can control access with inexpensive tools and common-sense security practices.

We will now explore the types of Internet security risks your network might face.

Attacks by Viruses, Worms, Spies, and Zombies

After reading this chapter, you may feel like taking a bath. The names of some of these pathogens do not sound savory at all. Attacks from these malicious bits of software, often referred to as *malware*, can leave your network and computers reeling from the effects of overloaded network connections and erratic operation. It is not uncommon to begin to have your Internet browser open of its own accord, taking you to sites you had no intention of ever visiting. You might see activity on your Internet connection even when you are not using it. Your friends and family will begin to warn you they have received viruses from you via e-mail. You may even be shut down by your Internet service provider for abuse until you can have your systems cleaned of these bugs.

Viruses

The most familiar type of computer bug, the *virus*, has received a lot of attention from the media in recent years. You may remember names like Michelangelo, I Love You, and SoBig. You may not know this, but over 80,000 different viruses are known to virus researchers, and about 2,000 of them actually have spread on real-world computers. The rest were research viruses or were not effective at propagation and were never detected in large numbers. A “WildList” maintained by several virus researchers tracks active virus outbreaks and is used to test antivirus software for effectiveness. If you are curious about current threats, you can view the WildList at www.wildlist.org. On average, there are about 200 viruses known to be “in the wild,” that is active, at any one time.

Worms

Worms are a subset of viruses that spread by infecting systems they seek out all by themselves. Often this infection occurs by exploitation of defects in the computer’s operating system or installed applications. The worm is programmed to seek out vulnerable systems and infect them with a copy of itself. The newly infected system then goes to work finding and infecting other systems. Some of the more recent newsmaker viruses (Code Red, Blaster, Nimda, and others) have been worms.

Trojan Horses

More an attack method than a type of malware, *Trojan horses* use the classic method employed by the Achaeans under Odysseus to defeat ancient Troy. Masquerading as links to helpful web sites or free computer programs, they go to work to open back doors into the systems for attackers to exploit, send themselves to other intended

victims, or search the local network for additional computers to infect with other types of attacks.

Often a Trojan horse is part of a *blended threat attack*. This type of attack “blends” some of the attributes of viruses, worms, and Trojan horses to get the greatest infection power possible.

Spyware

Defended as applications to help marketers capture demographic data from Internet browsers, *spyware* at its worst employs all known attack techniques for propagating itself to unsuspecting systems. Many spyware payloads also include viruses and worms to infiltrate systems and send unsolicited e-mail messages to additional targets using the victim’s address book.

Zombies and Bots

Zombies are computers infected by worms, by Trojan horses, or directly by attackers. They come under control of an individual called a zombie master (usually the one who released the infection agent). They are then used to orchestrate massive attacks against the subject of the zombie master’s ire. Often this is a high-profile Internet site or the site of a perceived threat to the zombie master.

Direct Attacks from Internet Sources

Beside the many types of automated attacks we have discussed, your network may come under direct attack by someone who is attempting to take control of your systems to turn them into zombies, steal private data, or simply “see if they can.”

Somehow more personal because they signify someone is attacking *your* system specifically, they are in all likelihood very impersonal. Someone just needs another zombie to add to the fleet.

These attacks take on many forms, exploiting known defects in your operating system or in applications that use the Internet to communicate. We will not present an exhaustive list, as it would be too, well, exhausting. We will outline some of the more prevalent methods used to attack your systems. In the next part of this chapter, we will begin to show you how to protect your systems from these attacks.

Port Scans

Often the first step in an attack is a *port scan*. This is a rapid scan of all the commonly used Internet Protocol (IP) ports on your computer. Ports that respond to the scan are logged as possible targets for attack. The scanning application may then launch an attack, or the user of the program can use another tool against the port.

NOTE

A port is a logical address in the Internet Protocol that defines a connecting point or socket that an application can use to communicate with other applications. When combined with the computer's IP address, a port defines one of 65,535 connecting points (or sockets) available to the Transmission Control Protocol (TCP). Commonly used Internet services use well-known ports to advertise their existence. For instance, when you connect to a web server, you always try to connect first to port 80 unless you have been told otherwise by the server's owner. Other well-known ports include: 25 (Simple Mail Transport Protocol), 137–139 (Windows File Sharing), and 443 (Secure Sockets Layer for secure web sites). See the Internet Assigned Numbers Authority's web site at www.iana.org/assignments/port-numbers for a complete list of the well-known ports. Concerned about running out of ports? Well, the User Datagram Protocol (UDP), a relative of TCP, has 65,535 of its own!

Buffer Overflow Attacks

Poorly written applications do not know what to do when they are given too much data or poorly formatted data. Sometimes the program simply fails; sometimes the result is that the program fails in such a way as to leave an opening through which a properly written exploit program can insert commands or small programs into the host operating system. These commands or programs can then perform actions such as opening a back door into the system, allowing the user of the command to completely control it. They can then install software that logs keystrokes to capture passwords, e-mail addresses, credit card numbers, or other sensitive information. They can use the victim system as a zombie to launch attacks against other systems. They can also use the compromised system as a gateway into the network on which the victim's system lives, potentially gaining access to additional sensitive data.

Logon Attacks

If you have ever forgotten your password to a system at work or to a web site on the Internet, you know you get another chance to get it right. Some systems will lock you out after too many unsuccessful attempts, but some will let you keep right on going until you finally guess the right password or try every password you have ever used. Programs have been written to crack passwords. They will use known or commonly used user account names and run hundreds or thousands of common passwords against them to see if one works. When they find the right one, they gain access to the target system with the privileges of the user account they have used. Sometimes these attacks are called *dictionary attacks* because the list of potential

passwords looks sort of like the dictionary (and uses many of the words in it!). *Brute force* attacks actually attempt to guess passwords by using all possible keystroke combinations against the password until it is finally cracked.

Man-in-the-Middle Attacks

A *man-in-the-middle* attack is accomplished by intercepting traffic between two computers and mimicking each to the other, capturing all the data they transmit in the process. Most modern security and encryption protocols include features designed

Did you
know?

The Term *Hacker* Originated at MIT

The term *hacker* is used to refer to those who are fascinated by finding out how things work. Hackers like to use every feature of an operating system or application, looking to see if they can find any bugs or other issues. The prize of locating an undocumented feature or bug is respect of vendors and notoriety among your peers, and no actual harm is done, as bugs are reported to the manufacturer. Hackers actually *help* software manufacturers write better code and are often invited to help test applications. Many current and former hackers are the security researchers who still find and report bugs and vulnerabilities today.

Crackers use what they learn from their investigation or from the work of ethical hackers to break into systems, harass other users, and even steal identities and money. The media has been unable to find a distinction between the two actions and now applies the term hacking to the actions of the cracker as well.

The first “hackers” were students at MIT. MIT jargon used the term hack to denote any deceptively simple solution to a problem. Hackers were those who were skillful at writing software, solving complex problems easily, or using everyday objects in new and different ways. There are references in MIT student publications to hackers taking control of telephone systems with a computer program and making free long-distance calls.

Hackers have recently tried to create a new distinction between themselves and the crackers, so you may see sites refer to “white hat” and “black hat” hackers. Look back to the days of the Lone Ranger if you need to know the difference between the two.

to defeat these attacks, but the arms race continues, with defects being found and fixed in these protocols with some regularity. Protocol vendors will release fixes for these deficiencies, but it is the users' responsibility to be sure their systems are kept up-to-date.

Denial of Service Attacks (DoS)

When an attacker directs a stream of malformed Internet packets at one specific system with the intent of causing it to become unstable or overloaded, this activity is referred to as a *denial of service (DoS)* attack. The number of packets need not be large; in some cases just a few carefully crafted packets will drop a server or application to its digital knees. To combat these attacks, large corporations have installed systems designed to detect malicious activity and block it.

5

Distributed Denial of Service (DDoS) Attacks

When the denial of service defenses get too good, it is time to simply overwhelm the victim with a deluge of valid packets. Since there is nothing wrong with the data being received, it cannot be distinguished from the valid client traffic. Fleets of zombie computers are commanded to begin sending traffic to the same site, not only overloading the site, but in some cases, their Internet service provider as well. This massive flood of traffic is called a distributed denial of service (DDoS) attack.

Use Windows XP Security Tools to Protect Your Network

Now that we have delivered all the bad news, let's show you how you can protect your home network against some of these attacks. We will begin by demonstrating the security tools Microsoft includes with their Windows XP operating system. We will explore the features of Windows Security Center, Windows Firewall, and Internet Connection Sharing (ICS). Then we will show you how to evaluate your security by using the Microsoft Baseline Security Analyzer.

Manage Your System's Protection with Windows XP Security Center (New in SP2)

A common complaint about Microsoft operating system security was that it was too hard to tell when everything is correctly configured for security. Beginning with Windows XP Service Pack 2, available on all new PCs sold today and for free

download from the Microsoft web site for older machines, we have at our disposal the Windows XP Security Center. This tool allows you to monitor the built-in Windows XP security tools and get more information on security topics.

Use Security Center to Audit Your System's Security

The Security Center is a console-style application designed to give at-a-glance information about a computer's security readiness. It will advise when the Windows Firewall or Automatic Updates have not been configured and enabled. It will also check for antivirus applications and recommend a few if one is not found. You can see in Figure 5-1 a case in which the Security Center cannot locate a virus protection application on a system. By selecting the Recommendations button, you can get



FIGURE 5-1 Windows XP Security Center showing default view



FIGURE 5-2 Expanding the Security Services for more information

information on how to locate and acquire a virus protection package. Also in Figure 5-1, we see that both Windows Firewall and Automatic Updates have been enabled.

Expanding each section of the Security Center display (Figure 5-2) shows the current reported status and additional information about each service. You can then manage settings for these services by using the icons at the bottom of the page. Windows Firewall is self-evident; Automatic Updates is managed in System settings.

Configure Security Center Alerts and Warnings

You can configure Security Center to pop up alerts in the Windows XP Notification Area when it discovers a problem with the configuration of important security tools.

To do so, you click the Change The way Security Center Alerts Me link under Resources.



You can choose to set alerts for Firewall settings, Automatic Updates settings, or Virus Protection.

Keep Patched with Updates

Operating system updates and application updates are so important we are giving them an entire chapter in this book. We mention them here simply to help underline their relative importance in the spectrum of security tools you must make use of to protect your systems.

Operating System Updates

Microsoft makes the Windows Update and Automatic Updates tools available to help you keep up with critical operating system updates. Using these tools properly is an important way to ensure attackers cannot use well-known operating system flaws to break into your system or network.

NOTE

Many of the recent outbreaks of viruses and worms could have been prevented by proper patching of known system flaws.

Application Updates

Microsoft applications can be updated in much the same way as the operating system. Office Update is a tool very similar to Windows Update for finding and downloading application updates. A future version of the Windows Update site will also automate the download of critical application fixes as well.

Protect Your Addresses with Internet Connection Sharing

Another way you can protect your network from intrusion is by using the features of Windows XP's Internet Connection Sharing (ICS). This service connects your network to the Internet through one Windows XP computer. By using a private range of Internet protocol addresses (192.168.0.1–192.168.0.254) and dynamically translating these to a single public address (using Network Address Translation), ICS effectively hides your network's size and structure from the Internet. You are still able to browse the web and use any Internet service you wish, but attackers see only one machine doing all the talking. If you protect that machine, you protect the network.

NOTE

Internet Connection Sharing serves the same purpose as the hardware Internet Gateways we have discussed, offering the same address translation functions as they do. Its main advantage is its price: free. It will require a dedicated system with two network connections (one Internet, one local) that must be powered on as long as any clients in the home might require it.

How Network Address Translation (NAT) Protects Your Network

Let's assume for a moment you are playing Everquest online. Your computer inside your network connects to your Internet Connection Sharing (ICS) computer, and ICS connects to patch.everquest.com port 7000 on your behalf. Your own internal IP address is 192.168.0.5, but patch.everquest.com sees 10.213.255.254 (for instance). Any attacker attempting to exploit your Everquest session cannot see that you are not actually live on the Internet, and any attempts to exploit any known flaws in your Everquest client will fall off, as the machine on the Internet is not actually even running it.

Another benefit of using NAT is conservation of public IP addresses. Connecting a half dozen devices to the Internet via only one address is a great way to conserve IP addresses. This lowers your costs as well as ensuring there are enough addresses to go around.

Changes Internet Connection Sharing Makes to Your Network

When you enable ICS on a Windows XP computer, changes are made to the system:

- Your system becomes a simple Dynamic Host Configuration Protocol (DHCP) server. This allows it to provide other computers and devices on your home network with IP addresses compatible with the Network Address Translation feature of ICS.
- Your system also is configured to act as a proxy for all Domain Naming System (DNS) address resolution queries your clients may issue to locate Internet hosts.
- Network Address Translation routing is enabled on your system, and if necessary, Windows Firewall (up next) is reconfigured to support your computer's new role.

These changes require your Internet Connection Sharing system to be restarted, and any other device or computer on the network will need to be restarted as well to get everyone on the same page, address-wise. You will notice all your systems getting addresses in the 192.168.0.x address range just mentioned.

NOTE

If you have any systems that are using static, or fixed, IP addresses, you will have to manually reconfigure them to participate in the new address range. Give them an address of 192.168.0.x, where the x is an address not used on any other system. Set the subnet mask to 255.255.255.0 and the default gateway to 192.168.0.1 (the address of the ICS system).

Block Hackers with Windows Firewall

With functionality and management improved in Service Pack 2, the Windows Firewall (formerly known as Internet Connection Firewall) gives you inexpensive protection from malicious intent on the Internet. It may not have all the features

of the more expensive third-party firewalls, but it serves as an excellent startup firewall, is priced right (it is free), and is adequate protection for a majority of systems.

How a Firewall Protects Your Network

A firewall protects your network by inspecting traffic that is attempting to enter. If it is not sent as a response to some internal client's request, it is usually dropped. Most firewalls, by default, will act in this manner. It is called "off by default." You can configure a firewall to allow certain traffic, such as web browsing (port 80), to enter your network, but this would be done only when you have a system inside prepared (and protected) to handle the traffic. Some firewalls even allow you to place these internal systems on a separate connection that can be used as a small semiprotected network, known as a demilitarized zone or DMZ, separated from the fully protected network.

Configure Windows Firewall to Protect Your Network

By default, Windows Firewall is enabled on all network connections. Its predecessor, the Internet Connection Firewall, had to be enabled before it began protecting your systems. Microsoft decided it was better to err on the side of protection with Windows Firewall. As a consequence, there may be times when you see Windows Firewall get in the way of your communications. For this reason, you can enable exceptions to the default firewall rule that blocks all unsolicited inbound traffic.

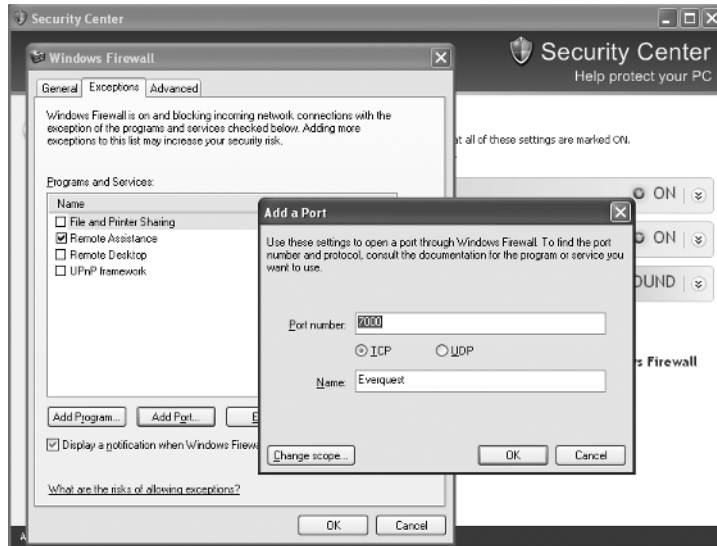
Configure Windows Firewall Exceptions to Allow Inbound Traffic Some firewall rules are taken care of for you when you configure services such as file and printer sharing. Windows XP sees this action and will enable the appropriate exception in Windows Firewall. Others, such as Internet Hearts, will require you to enable the exception manually.

To enable a manual exception, you have two options. You can enable an exception based on a defined port number, or you can enable an exception by choosing the program that needs the exception from a list of available programs.

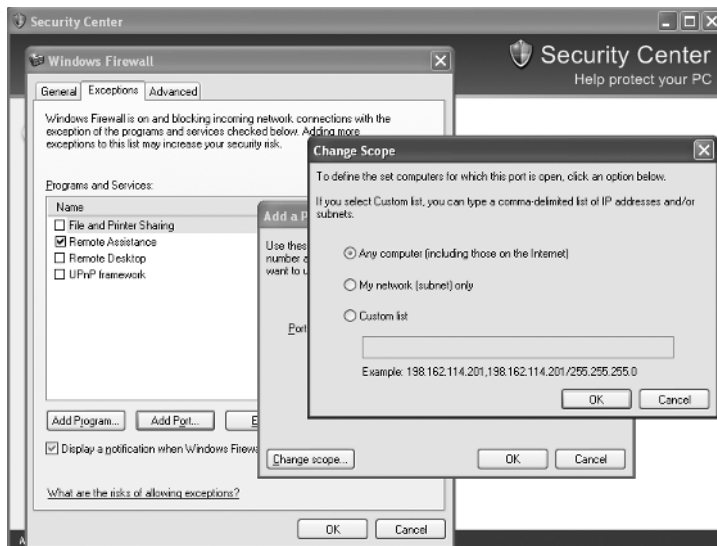
To enable a port exception,

1. From the Security Center, select Windows Firewall under the Manage Security Settings For heading and select the Exceptions tab in the Windows Firewall dialog box.
2. Click the Add Port button.

3. In the Add A Port dialog box, enter the port required by your application and provide a descriptive name for the exception you are adding.



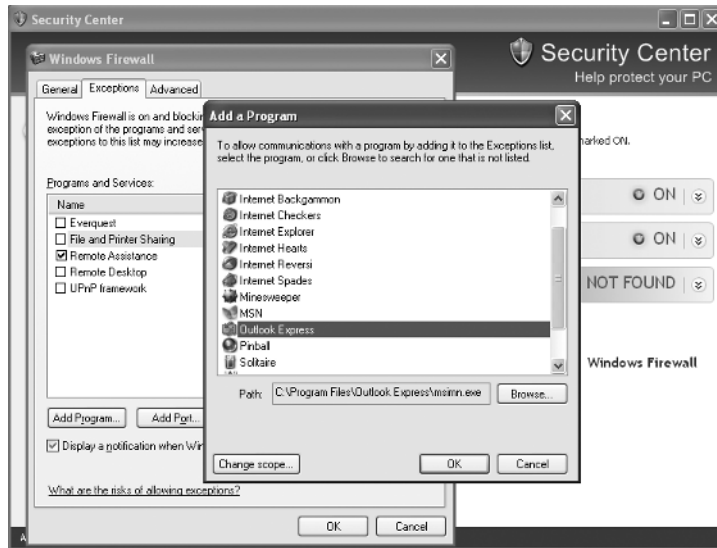
4. If you have more than one network connection or you wish to allow the exception to be effective only for your local network, you can modify the *scope* of the exception. Click the Change Scope button to open the Change Scope dialog box.



5. Select whether the exception applies to all computers, affects your local network (subnet) only, or is more specific (such as a specific computer or range of addresses).

To enable an application exception,

1. On the Exceptions tab just mentioned, click the Add Program button.



2. Select the program you wish to add an exception for or browse for the program executable by clicking the Browse button.
3. Change scope if necessary to achieve the level of control your program requires.

NOTE

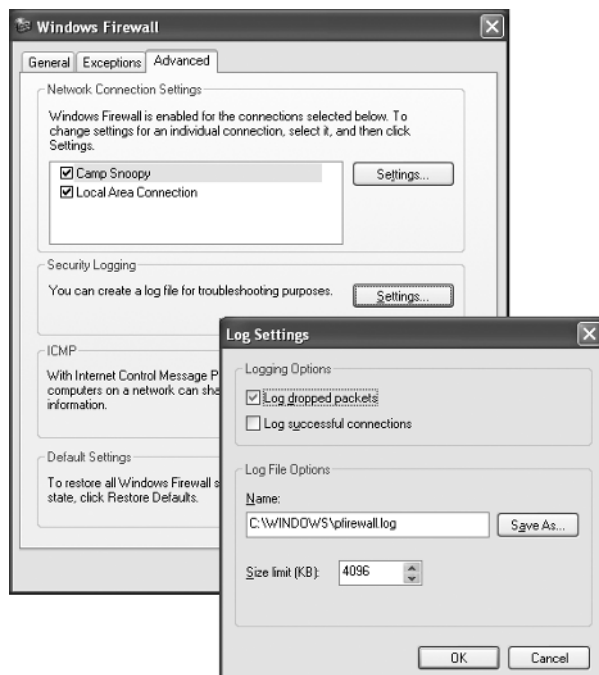
Using the local subnet scope allows your applications to work on the local network but keeps protection from Internet sources in place. This is very helpful for programs you will use locally. If you investigate the scope settings for File and Printer Sharing, you will find it's already set to allow only local addresses to connect to these ports. (Cool, huh?)

Monitor Your Firewall for Suspicious Activity

After you have configured Windows Firewall to your liking, you might begin to wonder if it is really blocking any bad guys/grrlz. You can find out by watching your firewall logs.

To enable Windows Firewall logging,

1. On the Advanced tab in the Windows Firewall dialog box, click the Settings button in the Security Logging section.



2. Choose whether to log only dropped packets or also log successful connections. Logging dropped packets is usually sufficient unless you are investigating an intrusion attempt.

To decipher your firewall logs,

1. Locate the log file. By default, this is pfirewall.log in your Windows folder.
2. Open the file in Notepad.
3. You will see entries similar to those shown in Figure 5-3.

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port

2004-06-23 23:40:48 DROP UDP 192.168.2.102 192.168.2.255
2004-06-23 23:42:13 DROP UDP 192.168.2.102 192.168.2.255
2004-06-23 23:43:32 DROP UDP 192.168.2.101 192.168.2.255
2004-06-23 23:44:42 DROP UDP 192.168.2.102 192.168.2.255
2004-06-23 23:44:42 DROP UDP 192.168.2.102 192.168.2.255
2004-06-23 23:44:42 DROP UDP 192.168.2.101 192.168.2.255
```

FIGURE 5-3 Excerpt from a Windows Firewall log

4. Use the field names listed in the #Fields line to decipher the columns in the text below.
5. After some time you will begin to spot trends of activity and soon will be able to tell what is out of the ordinary.

NOTE

If you wish to participate in efforts to locate and stop malicious activity on the Internet, you can enroll your logs in the DShield.org Distributed Intrusion Detection System. Program information and instructions on submitting your personal firewall logs can be found at www.dshield.org.

Analyze Your Security with the Microsoft Baseline Security Analyzer

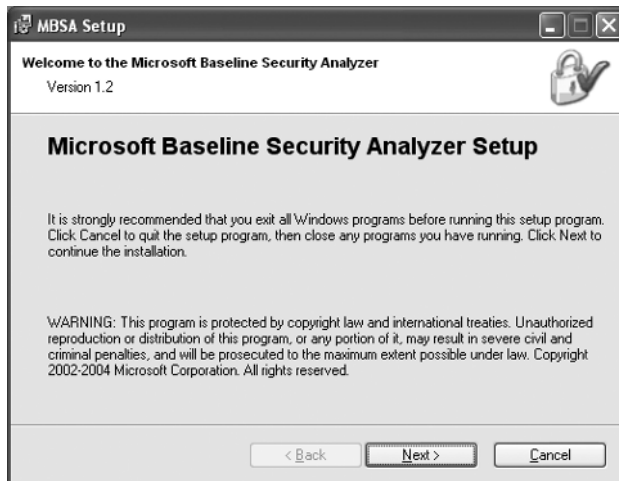
Microsoft provides a tool for auditing your system's security called the Microsoft Baseline Security Analyzer (MBSA). It was originally part of a security toolkit provided to IT professionals, but it can be downloaded here:

<http://www.microsoft.com/technet/security/tools/mbsahome.msp>

Install the Microsoft Baseline Security Analyzer

To install the MBSA,

1. Once you have downloaded MBSA, locate the downloaded installation file and execute it.



2. Verify the installation destination folder.



3. Accept the License Agreement.



4. Choose the default installation options.

How to ...

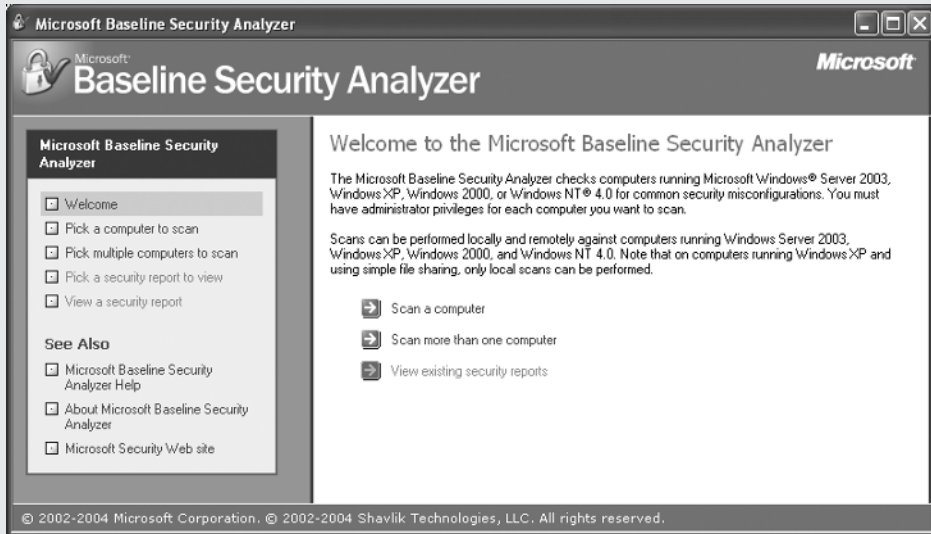
Use Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) is used to scan your system and report on its findings. It will scan for the following security deficiencies:

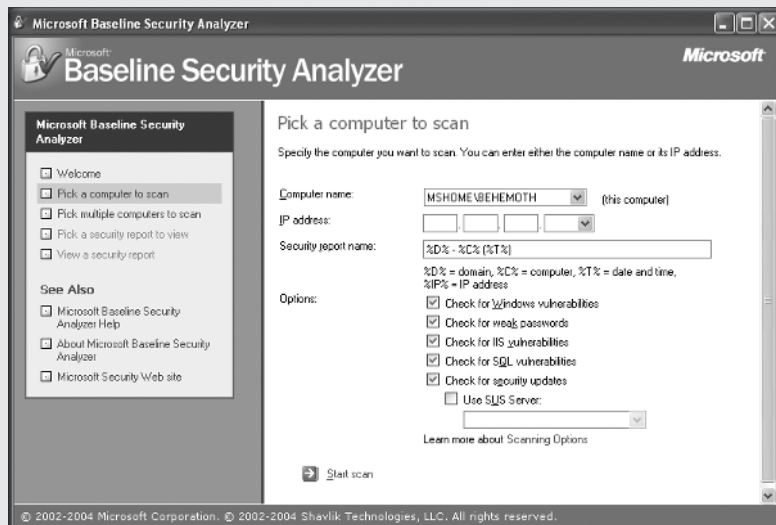
- Missed patches and updates in the operating system and Microsoft Office applications
- Improperly configured Windows Firewall settings
- Configuration of Automatic Updates
- Internet Explorer security settings
- User account security risks such as blank or weak passwords
- Unnecessary services

To scan your computer,

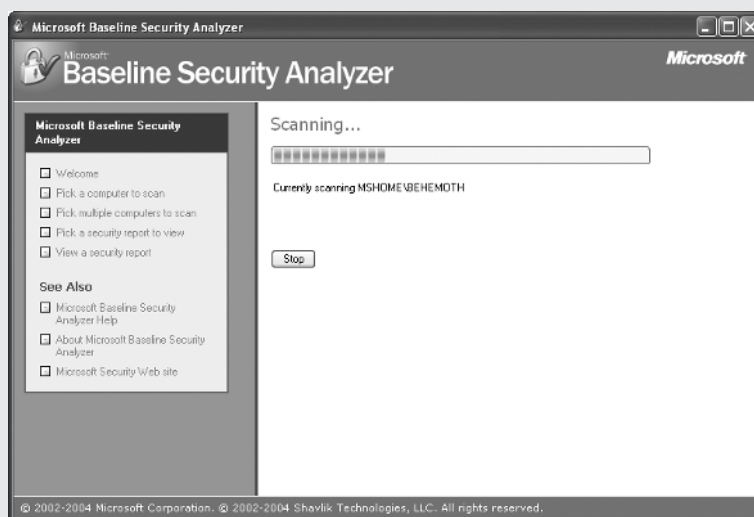
1. Execute MBSA and select Scan A Computer.



2. Ensure your computer name is selected and select the appropriate options.
It does not hurt to leave inapplicable options selected, because you may be surprised to find that you are unknowingly running IIS.

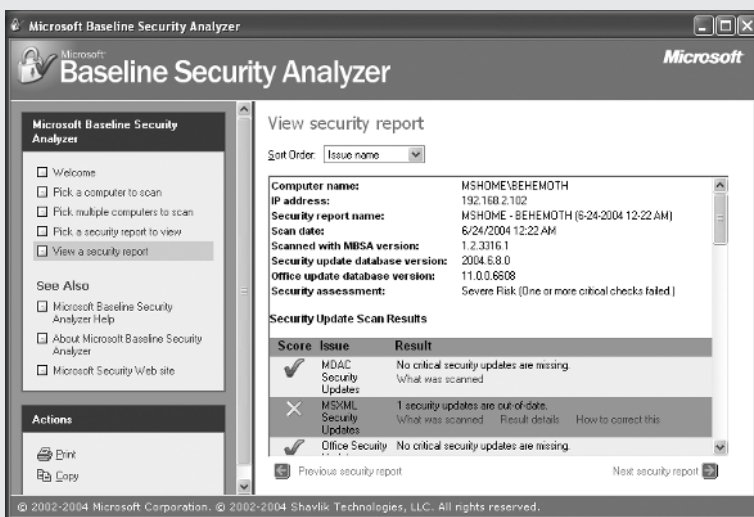


3. Click Start Scan. MBSA will download up-to-date information from Microsoft and begin scanning your system.



5

4. MBSA will complete the scan and display a report of its findings. Each finding will be supplied with additional information and tips on how to correct it.



5. You may print or copy and paste the report to refer to later.

Use Third-Party Security Tools to Protect Your Network

Up to now, we have presented you with the *all Microsoft* solution. There are certain advantages to keeping it under one roof—all the elements of your defenses are designed and tested to work together—but there are equally valid reasons to use third-party products. Many talented individuals who do not work for Microsoft have developed very powerful and simple-to-use applications that give you an added measure of security. There are also applications that offer features Microsoft has not delivered in any of its products. Among these are antivirus and antispyware applications. In this section we will explore third-party products that can increase your security with minimal expense.

Use Antivirus Applications to Stop Viruses

Antivirus applications excel at detecting viruses, worms, and Trojan horses that are on or entering your systems. We devote an entire chapter to installing and configuring antivirus software in this book, so we will just quickly introduce you now and then let you get better acquainted in Chapter 8.

How Antivirus Protects Your Computer

Antivirus applications are armed with extensive databases of malicious software attributes and behavior information. When one of these nasties enters your system, the antivirus application recognizes its mug shot and stops it, either deleting it or placing it in quarantine (your choice). Most antivirus applications can also detect suspicious behavior, using a technology called heuristics, and flag the offending code as a potential virus.

Types of Antivirus Applications and Services

Antivirus applications may differ slightly in their ways of doing business, but all are essentially the same. What really distinguishes them is where they might be found.

Desktop Antivirus Most antivirus vendors have desktop antivirus applications and suites that offer excellent protection against viruses. Each computer you own gets a copy and is maintained separately. This works well for a limited number of computers. When the number of computers rises above ten (not likely at home), it becomes tedious to maintain updates separately.

Network Antivirus When the number of protected systems rises above 10, many organizations opt for network antivirus applications. These applications differ from the desktop versions in that there is usually a server program that maintains settings and updates for all the units. These settings and updates are downloaded into each system over the network.

Antivirus Services Some e-mail services offer antivirus scanning as a feature of their service. Web mail providers such as Hotmail and Yahoo! scan user's e-mail for viruses and spam, helping ensure their users get clean e-mail.

5

Use Antispyware Applications to Terminate Spyware

Privacy gurus have made much of the spyware revolution in recent months. There is now an arms race of sorts going on between “online marketers” and privacy advocates. Software, bordering on malicious, has been spread around the Internet, and software to protect your systems has sprung up to meet it.

What Spyware Does to Your Computer

These programs range from simple tracking files called *cookies* to virus-like applications that spread copies of themselves to other computers and take control of your system, directing you to web sites you never intended. Some even partner with viruses and worms to further propagate themselves.

NOTE

Many sites use cookies to keep track of your preferences for formats and colors or your name and address data. Blocking all cookies might result in the site not being usable, or at the least hamper its ability to retain your preferences. You will most likely need to find a balance between privacy and usability.

Determine Your Spyware Risk Level

If you regularly browse mainstream sites like those of the major news outlets and periodicals, you will probably not be exposed to more than third-party cookies designed to record your *clickstream*.

NOTE

A clickstream is the path you take as you surf the web. Third-party cookies can keep track of your path through a web site and record where you went as you left. If the same marketer has a deal with the next site, they see you arrive and can track your patterns.

If you go to the more out-of-the-way places, however, you run the risk of more insidious contacts. Some spyware authors use advanced hacking techniques to implant spybots in your system that take control of your browsing (Browser “Helper” Objects) and send you where *they* want or capture your keystrokes and passwords.

NOTE

A Browser Helper Object (BHO) is an application embedded into the Internet Explorer environment that “helps” you use Internet Explorer. These can actually be helpful (Spybot Search & Destroy installs a protective BHO to block spyware), or they can be malicious. Many malicious BHOs will watch your keystrokes and open additional windows to search sites with your keywords already entered. The result is an annoyance to you and a few pennies to the BHO author who gets paid per click by the site they just sent you to.

Select an Antispyware Application

Antispyware comes in several flavors. Some applications include all the features we will discuss; some specialize in only one or two.

Pop-Up Blockers Pop-up blockers block the pop-up and pop-under ads you see when you enter web sites. The extra windows these sites open simply never appear when the blocker is running. Some tools that do this are the free Google toolbar; later versions of the Mozilla, Firefox, and Opera browsers; and Internet Explorer (with Windows XP Service Pack 2).



Cookie Management Most antispyware applications will allow you to block or manage cookies. This can range from blocking third-party cookies to blocking or warning about all cookies offered to your browser.

Registry Protection Some spyware removal applications will inoculate your Registry and alert you to any attempted changes to it. Spybot Search and Destroy is especially good at this.



5

Configure Antispyware

When using antispyware, it is important to configure it to accommodate your usage patterns and preferences. If you love getting offers for “free stuff,” you probably won’t mind seeing the pop-ups. If, however, you want few distractions, you might severely restrict the ability of spyware to see into your lifestyle.

Did you
know?

There Are Alternatives to Internet Explorer

In this book we concentrate on securing Internet Explorer, as it is the browser built into Windows XP. There are some other very good web browsers available on the Internet for free download. Mozilla and Mozilla Firefox, Opera, and the text-based Lynx browser all offer alternatives to Internet Explorer. By not offering direct support for ActiveX controls, they can be more secure from malicious controls embedded in web sites. Some even include pop-up blockers, password managers, and cookie management features.

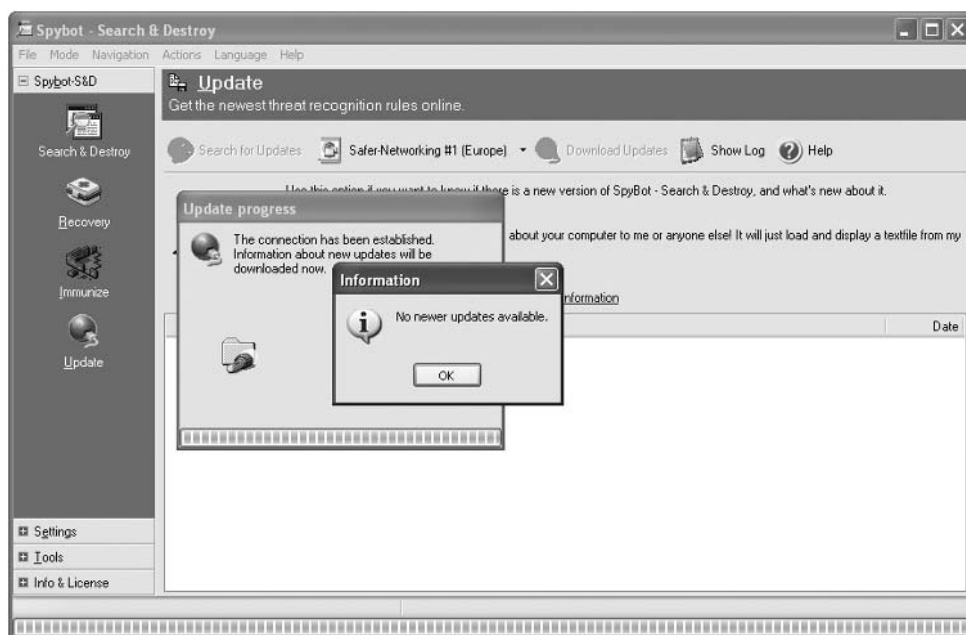
Be warned, however, that Internet Explorer remains on your system and must be kept patched. Even if it is not used for web browsing, any vulnerabilities discovered may still affect your system.

If you choose to install an alternative browser, which we recommend, be sure to choose the option to make it your default browser when asked by the application.

Look for settings that block third-party cookies and pop-ups. Enable Registry protection if available and configure the application to automatically update its detection patterns if possible.

Maintain Antispyware with Application Updates

Antispyware software is only as good as the author's ability to keep up with the latest spyware tactics. Most applications offer the ability to download new detection patterns and program updates. You should always update your detection patterns before a scan. New spyware appears almost every day and would go undetected without these updates.



Use Third-Party Internet Firewalls to Block Hackers

While Windows XP with Service Pack 2 offers a very comprehensive firewall, there are also inexpensive third-party firewalls worth evaluating. They excel in detecting attacks and may be simpler to configure.

How Third-Party Firewalls Differ from Windows Firewall

Third-party firewalls work in ways similar to Windows Firewall but may differ in key areas. Manageability is probably the most apparent. Personal firewalls like ZoneAlarm offer full intrusion detection and the ability to interactively configure application filters (the equivalent of Windows Firewalls “exceptions”) to suit your needs. Another differentiator is performance. A hardware firewall such as those built into Internet gateway devices offers faster filtering performance than those that must wait for CPU cycles from your computer.

Hardware Firewalls

Whether you select a firewall built into an Internet gateway device or a stand-alone firewall, it will most likely sit at the border between your network and the Internet. This location offers a choke point for Internet traffic, allowing the device to monitor all traffic going into and out of the network. Hardware firewalls are typically more difficult to configure when you need something other than the default settings, but they offer better performance and physical separation from your systems. Manufacturers of firewalls for home networks also have configuration wizards that will assist you with initial configuration.

Software Firewalls

Software firewalls install on your systems and protect each one individually. They are typically simpler to install and configure, having their own setup wizards and the ability to obtain information from your network applications and create settings based on the application’s requirements. Even when you choose a hardware firewall, it may be a good idea to install software firewalls on each system on the network. This helps to implement a practice called “defense in depth,” which we will discuss toward the end of this chapter.

Select a Third-Party Firewall

You may select your firewall because it is bundled into an Internet security suite, or you may choose based on price. Your best bet is to compare currently available firewalls (another moving target) and choose the one that best supports your usage patterns and budget. Magazines such as *PC World* regularly publish reviews and comparisons of firewalls, and you can also obtain information on firewall performance comparisons from other online sources. Do a search for “firewall” on CNet.com. You will receive a listing of firewalls they have reviewed in order of rating.

Install a Third-Party Firewall

Each firewall device or application will differ slightly in its method of installation. Read the installation instructions carefully and follow them to the letter. It is very easy to leave a step out of the installation that leaves a nice big hole in your defenses. You can be assured the attacker that finds it will leave you a nice, big thank-you note!

Configure a Third-Party Firewall

Most firewalls will install a good baseline protection configuration. You can then customize it to suit your requirements. As you configure your firewall, you will train it to recognize your traffic. You will want to block any ports that you would not normally use and set up logging so that you know when the hackers are at the door.

Some things to look for:

- All inbound traffic must be blocked by the firewall unless it is in response to a connection being initiated from the inside. There may be exceptions to this when you host games or your own web site. Try to have these ports open only when absolutely necessary and close them as soon as they are not needed.
- Ports for commonly exploited applications should be blocked for outbound traffic. For instance, there is no need to allow ports 135 and 137 outside the firewall. They are used for Windows File Sharing and would only invite attack if they were seen outside your network. Blocking these outbound ports, known as “egress filtering,” can do much to protect your systems. Other ports to block include 20 and 21 (FTP), 23 (telnet), and 445 (Windows Directory Service). In addition, if you hear of a worm or zombie that attacks a certain port, just do a quick check to see you are blocking it. You’ll be considered a good “netizen” if your systems never harm others, even when you may have inadvertently picked up a bug.
- Set up firewall logs and arrange to submit them to DShield.org. You’ll know who and what you are blocking, and you’ll be participating in important efforts to get these hooligans shut down.

Maintain a Third-Party Firewall

To avoid a false sense of security, keep up-to-date with any patches from your firewall vendor. Most firewalls receive regular updates to protect against new attacks or fix vulnerabilities discovered in the firewall itself. Be sure you take the time to ensure the update functions are properly configured. Monitor the update process. If you do not see an update within a month's time, you should begin to be concerned. Check your update program to ensure it is connecting to the proper address and is giving you a message indicating success. This message will be a notification either that there are new updates or that no new updates are available. If the update program cannot connect to its update server on the Internet, it will usually tell you so. Your firewall vendor can work with you to get updates running to keep your systems safe.

Evaluate Your Security with Third-Party Auditing Tools

After you have raised up all manner of defenses, it is time to see how good they are. It is better to be tested on your schedule than at 2 A.M. when Eurasia comes online. The goal of complete stealth (the state of being a hole in the Internet) is possible with the correct settings. After all, they cannot infect what they cannot find!

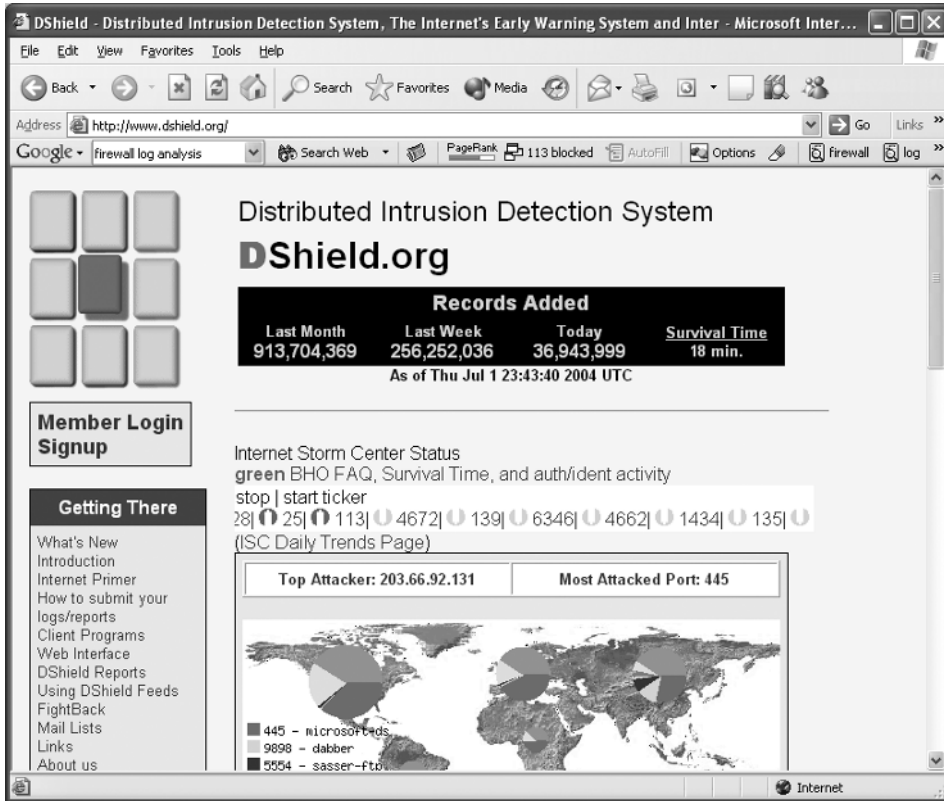
Test Your Defenses with Penetration Testing Tools

Several vendors make tools to test your defenses. These tools range from simple port scanners to full vulnerability testers. Free web-based testers such as grc.com's ShieldsUP! provide a quick check on your firewall's effectiveness. Free or inexpensive vulnerability scanners such as NeWT from tenablesecurity.com (a Windows version of the popular Linux-based Nessus vulnerability scanner) can scan your systems for a large number of known vulnerabilities.

Audit Your Log Files with Log Analysis Tools

Your firewall logs are probably readable as is, but there are also free and low-cost log analyzer tools available online. Users of ZoneAlarm can use ZoneLog Analyser (that's the British spelling) to slice and dice their logs. Many firewall logs can be sent to DShield.org using the tools provided free-of-charge by DShield. When they have been processed, you can obtain some statistics about your logs from DShield's web site. DShield also has an automated abuse monitoring system called "FightBack"

that will alert an attacker's Internet service provider to their activities and sometimes get them kicked off.



NOTE

Notice the “Survival Time” statistic on DShield’s web page. That statistic is the average time between exploit attempts for all logs submitted. It is an estimate of how long you can be online without protection before your system will be infected.

Raise the Alarm with Intrusion Detection Systems

Intrusion detection systems (IDSs) scan your logs and watch your systems for signs of malicious activity. When an attack is discovered, the IDS can sound a tone, send you e-mail, or take your system offline for its own protection. As with other security tools we have discussed, money is no excuse for not having an IDS. There are many free or low-cost IDS applications available. A quick Google for “IDS” nets thousands of hits, including products from Symantec, free tools such as Snort, and enterprise-level products such as Computer Associates’ eTrust Intrusion Detection.

Use Defense in Depth to Protect Your Systems

A secure military installation does not just lock the doors and go home every night. There will be fences topped with razor wire, motion detector floodlights, armed patrols, dogs, and alarmed doors and windows to protect whatever is inside the compound. This is a classic example of defense in depth. A penetration of any single layer will leave any attacker with a long way to go.

Establish a Layered Defense

You can establish your own layered defenses to protect your systems. Starting with each individual system and working our way out, we have the following layers:

- Operating system patches and updates
- Up-to-date antivirus application
- Personal firewall software and IDS with logging enabled
- Firewall at the network's border with the Internet with logging enabled
- DShield.org for log submission and analysis
- Security advisories and alerts from security authorities (take your pick)

As you can see, there are many layers an attacker must face before getting to your data. With all the computer users out there who are not taking security seriously, the odds are great that the attacker will tire of your systems and move on to other, less challenging, targets.

Keep All Systems Up to Date

As noted in the bullets in the preceding section, operating system patches and updates are one of the most critical steps you can take to protect your systems. Simply keeping up with patches would protect you against 80 percent of the attacks out there with *no other action*. Obviously, we want to do all we can to protect ourselves, but do not be tempted to skip this all-important step. With all the firewalls and IDSs in the world, all it takes is one malicious ActiveX control or e-mail to drop your whole system. Web pages and e-mails come right through the firewall at your invitation, and unpatched systems can leave your system as vulnerable as any other.

Voices from the Community

Why Do I Need a Firewall at Home?

Bob Hillery, CISSP, NSA-IAM, GIAC-CFET, is a Senior Security Analyst with IntelGuardians, LLC, and an instructor with the SANS Institute, an information security research and training organization. We asked Hillery to tell us why he thought firewalls are important:

“If you ask a neighbor, ‘Do you have a computer?’ you probably get a, ‘Sure I do. The rest of the family uses it, too. We send e-mail to Granny and friends, the kids do homework, and we do online shopping all the time.’

“Then ask about security. You may get questions like, ‘Why would anyone want my files?’ and ‘Besides, securing a computer is too hard.’

“They’re mistaken on both these counts.

“Let me explain. I live in a rural area of New England. A lot of people commute to the nearby business parks, tech corridors, and universities. That’s a hint about what sort of networking might be happening at home.

“The local library uses the same regional provider that most of the homes and businesses use. All anyone would need is a connection to the Internet and they might be able to see traffic from a thousand other systems. Once someone starts seeing this traffic, it’s pretty easy to find weak systems with many of the vulnerabilities we read about in the papers.

“Ideally, you wouldn’t have any of these vulnerabilities. But let’s say you didn’t have time this week to take care of it. Has the hacker won?

“Not if you have a firewall. Many of the hackers’ probes will be malformed traffic. A firewall drops those. Some will be known ‘signatures’ or bit patterns that are recognized as common attack code. A firewall drops those, too. Some of the traffic may look normal, but be responses to questions you *didn’t ask*—that traffic is dropped.

“Bottom line: Firewalls can prevent attackers from gaining access to your network. They will stop most automated (scripted) probes and most of the annoying script-kiddies that are looking for access.”

Chapter 6

Secure Your Wireless Networks



How to...

- Realize that your wireless network is at risk
- Configure security settings on gateways
- Keep your data secure over wireless connections

Anybody can set up a wireless (or WiFi) network, but it's much more complicated to set up a *secure* wireless network. Many people who try end up frustrated, and many others don't even bother to enable the built-in security provided by virtually all wireless gateway companies in their products. A June study of more than 228,000 wireless networks across the U.S. (published at <http://wigle.net>) found that nearly two-thirds of the networks used no protection whatsoever, and more than a quarter of networks were running with insecure, factory-default settings.

If your WiFi network isn't secure, a thief could steal data as you use the Internet: the password sent by your e-mail client when you check mail, the contents of any e-mail or instant messages you download or upload, or anything you type into a chat room, search engine, or post to a message board—and that's just for starters. The effort involved for the cyber-thief is trivial; software that can listen in on wireless networks is as easy to use as it is freely available.

While not yet widespread, data theft over wireless networks is on the verge of booming. Taking half an hour now to protect yourself may save you a lot of time later. Victims of identity theft crimes often spend dozens or even hundreds of hours to clear their names and straighten out their credit records.

Securing your network is a fairly straightforward process, though the steps aren't always intuitive. This chapter will help you understand the steps involved in securing your wireless network, including surveying your network environment, turning on encryption, enabling MAC address filtering, and preventing your WiFi-enabled laptop from connecting to someone else's wireless network. All of these simple steps can inhibit a dedicated data thief, as well as prevent others from connecting to your wireless network, accidentally or deliberately.

NOTE

In this chapter, we'll use the terms "gateway" and "access point" interchangeably to refer to the box that transmits and receives a WiFi radio signal. Technically, these are slightly different pieces of hardware, but the distinction isn't important when it comes to network security; they are both just building blocks of wireless networks.

Cap That Data Gusher You Call a Gateway

Wireless networks make all kinds of activities a lot more convenient for us, the people who run them. It also makes stealing data or snooping on your activities a whole lot more convenient for people who do those sorts of things. If you're still on the fence about whether wireless security is worth the effort, consider the following:

- **There really, truly are people out there who steal data over WiFi** Denial's a wonderful thing, but that doesn't mean you should wait until you become a victim of identity theft to protect yourself.
- **WiFi radio waves can travel farther than you realize** The typical range of most gateways is around 60 to 80 feet, but other, less intuitive factors (the orientation or mounting height of the gateway, the construction of the building in which the gateway is installed, whether you live at the top of a hill) can boost that range considerably, sometimes for blocks and blocks.
- **Insecure wireless gateways are like data gushers** Anyone within range of your wireless network can listen in and record everything—passwords, the content of messages, the URLs you visit—as you check or send e-mail, send instant messages, or surf the Web. Cap that sucker!
- **You might connect to the wrong gateway** If you accidentally associate (that is, connect) with a neighbor's gateway, your data will then flow through his or her connection, instead of your own. Do you really want your neighbors to know everything you do online, in detail? I didn't think so.
- **Your microwave oven is conspiring against you** Well, not *literally*, but some kinds of home appliances emit radio waves—microwaves, cordless phones, and baby monitors are just a few—that can make a mess of your wireless network and might cause your PC to associate with that nosy neighbor's network, again. Encryption will help keep you connected to the right gateway.
- **Wireless security is really easy** Most people simply don't bother to enable the security settings in their network devices, despite the fact that a trained monkey could do it blindfolded. Unless you have a trained monkey on call, you've got no more excuses.

Configure Your Wireless Network for Security

There are a few important principles to remember when setting up wireless networking hardware. Wireless networks can “bleed” into spaces where you might not want the network to extend. Wireless networks, by their very nature, are less secure than wired networks; you cannot, for example, keep a wireless network secret from war drivers—folks who drive around with laptops in their cars, looking for WiFi networks—and even encrypted networks are not totally protected from intruders.

What can you do? For a start, you can enable one or more of the many security features present in all wireless network devices, change default passwords and other settings on your gateway, and keep track of what goes on, invisibly, around you on your wireless network. If you do even one of these things, you’re way ahead of more than 60 percent of people who run wireless networks with no security enabled at all.

Did you
know?

The New WiFi Standard Improves Wireless Network Security

In June 2004, the Internet standards body IEEE created a new standard for wireless Internet access. Companies will begin introducing new gateways and network cards based on 802.11i (the fourth WiFi standard, following 802.11b, 802.11a, and 802.11g), possibly as soon as December 2004.

One key aspect of the new standard is that it calls for the encryption of the radio signal to be handled by the gateway and wireless network card hardware itself—a feature that allows legacy programs (Outlook Express, anyone?) to take advantage of the new security without having to be patched or otherwise modified. But this feature also requires specialized hardware, which means existing gateways and network cards won’t be able to adopt the new standard with just a firmware upgrade; you’ll have to buy new equipment—both gateways and wireless cards—to take advantage of the security features.

The 11i standard also introduces a new encryption scheme, called WiFi Protected Access 2 (WPA2), that improves upon the existing WPA encryption. WPA2 supports the use of 128-bit Advanced Encryption Standard (AES) encryption, a government-approved, high-security standard, but its real benefit will come for those who use paid wireless hotspots. WPA2 will introduce a feature called *pre-authentication*, which will let your PC hop from access point to access point within a wireless network (almost like a cell phone does, as it

picks up the strongest signal from a radio tower when you're moving), without a big pause as the PC switches to a different access point. This feature, if it works well, may lead to better Voice-over-Internet Protocol WiFi phones you could use to make free or cheap phone calls from anywhere.

But all that encryption and protection comes at a performance price. Laptops will almost certainly see a greater power drain with an 11i connection than they would if they networked with 11b or 11g. That's because all the constant math being done to encrypt data will force the CPU to run at full throttle anytime it's connected to an 11i network. Nobody knows how much of a drain this will cause, but it's guaranteed to be more than zero.

Install Your Wireless Hardware with Security in Mind

Like wired networks, wireless networks are a way to connect a computer to other computers over the Internet. The only difference? The lack of wires, of course. The connection between your laptop's wireless card and the WiFi gateway is the weakest link in any wireless network. When setting up a secure wireless network, you need to think about how you plan to use it, the distance between your wireless gateway and where you want to use your laptop, and how you plan to secure the connection between your wireless card and the gateway.

Where Do You Want to Work?

Software that came with your wireless card or WiFi-enabled laptop should be able to give you a precise reading of the radio signal strength anywhere that the laptop is getting a signal from the gateway. You can use this signal strength information—it usually resembles some sort of meter or thermometer bar—to find dead spots in your own wireless network, and avoid accidentally connecting to another gateway. With your gateway turned on, boot up your laptop, and carry it around with you to all the places you want to do work. But don't just carry the laptop into the dining room, for example, and read the meter; sit down at the dining room table, in the seat where you'll want to work, and then check the signal strength.

In Windows XP, you can check the radio signal strength in several ways: using Windows' own wireless networking properties page, as shown in Figure 6-1; running the software utility that came with your network card (or the laptop, if the wireless card is built inside); or by firing up third-party tools such as NetStumbler, which you'll learn to do later in this chapter.

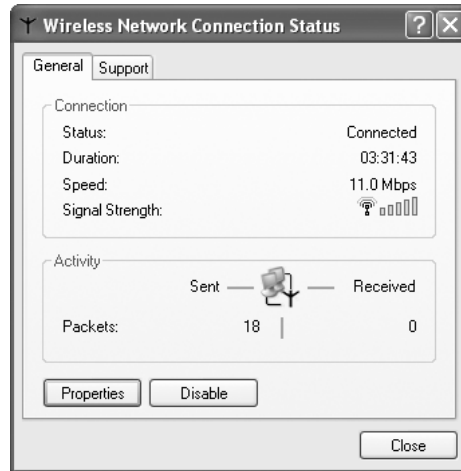


FIGURE 6-1 Windows XP's pre-Service Pack 2 cell phone-like signal strength meter can only tell you roughly how strong the radio signal is being received.

Most wireless network cards include software you can use to connect to a wireless network if you don't want to use Windows' own wireless tools. These utilities are often more sophisticated than Windows XP's built-in WiFi tools and can give you more precise information about radio signal strength. Some will also perform a "site survey," where the software finds all the access points in range and lists them, so you can tell which one will give you the best signal.

If you've installed Windows XP Service Pack 2 (SP2), you'll notice that the wireless network tool has changed quite a bit (see Figure 6-2). With this update, you'll be able to scan the local area for networks, judge their relative signal strength better, and determine whether the network(s) are secure. WiFi setup is so much simpler after you install SP2, you'll wonder how you lived without it. (Head to <http://find.pcworld.com/43292> to download this important update.)

Windows XP displays a bar chart and gives a verbal "signal quality" score to any wireless network it detects. The utility software that comes with your wireless card may give you more detailed signal strength information, such as a combination of bars and numbers (see Figure 6-3 for an example), where a higher number often indicates a stronger signal. No matter which tool you use, shoot for a signal strength of 50 percent or higher. If the signal is any weaker than that, you might find that you will disconnect from the Internet or disassociate frequently from the access point. But solving a weak signal problem may be as easy as just turning your body slightly, or reorienting the antennas on your gateway.

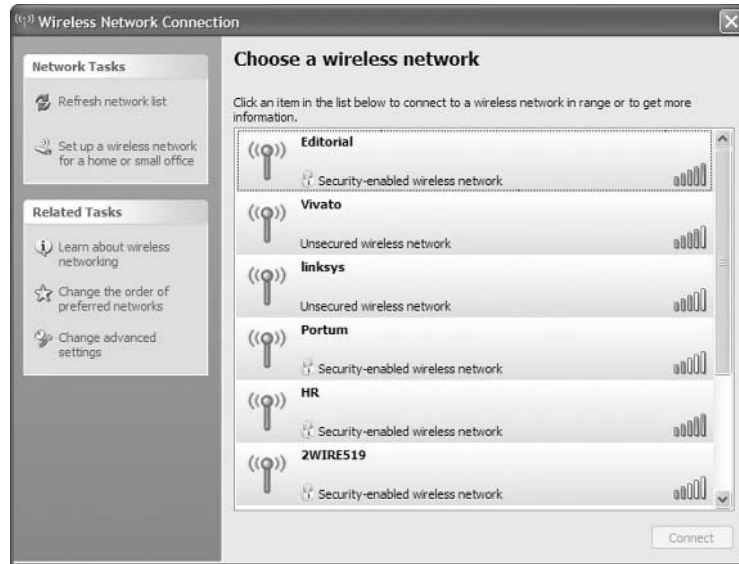


FIGURE 6-2 The wireless network connectoid gets a big overhaul in Windows XP Service Pack 2.

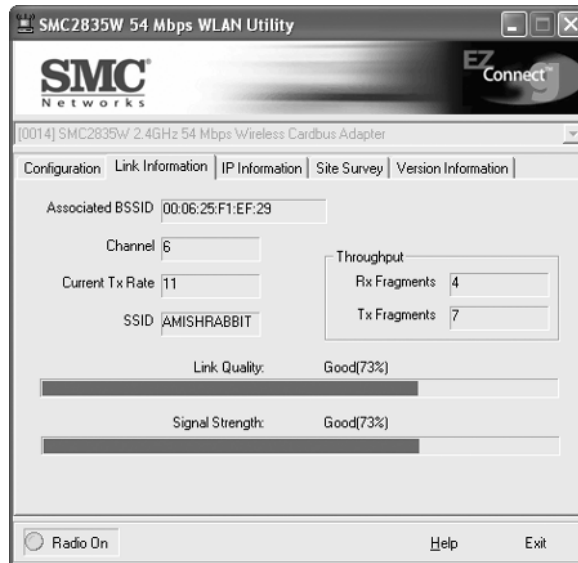


FIGURE 6-3 SMC's 54 Mbps WLAN Utility displays a numeric value indicating the signal strength of a wireless access point.

Configure Your Wireless Hardware

While it's important to set up a protected link between the gateway and the laptop, it's equally important to protect the gateway itself from intruders.

Few people who own a gateway change its factory-preset configuration, since it seems to work just fine when they take it out of the box and plug it in. But an unprotected, unconfigured gateway can cause you a lot of headaches. Anyone who comes within range of an unconfigured gateway can *associate* (connect) with it. If that person knows the default settings for your model of gateway (such as the administrator password), they can log into the gateway's administration panel and make changes to the setup of your wireless network.

The gateway isn't the only potential source of hardware-related security problems. You also need to configure settings on your laptop so that it doesn't inadvertently become the weak link in your chain of network security.

Password-Protect the Gateway's Administration Console

If you do nothing else, change your gateway's default administrator password. This is the password you will use to log into the gateway to make changes to various settings—be sure to keep track of the password!

The method for changing the password in a gateway varies slightly from manufacturer to manufacturer, but it's fairly simple to do. You'll start by logging into the gateway as an administrator, and then you'll change the password.

You'll have to enter the gateway's IP address in your Web browser, and then type in a factory preset administrative username and password, which the manufacturer usually prints in your gateway's manual or quick start guide.

Once you've logged in, you will see what is commonly called the gateway's *administration console*. This is really just a series of Web pages with forms in them (see Figure 6-4). The gateway itself runs a tiny Web server just for this purpose.

Gateways made by different manufacturers won't have the place where you change the administrator password in exactly the same location (see Figure 6-5). You might need to poke around some of the tabs to find it. Consult the manual if you have to, but you should be able to find it within a few mouse clicks.

When you change the default password in the gateway, write it down and keep it handy. Unless you have a specific reason to keep someone inside your house out of your gateway, a label or sticky note with the password (make up a unique one for the gateway) on the box itself is sufficient and convenient—you won't lose the password that way. Optionally, because you'll use your Web browser to connect to the gateway, you can set your browser to remember the password for you, so the next time you have to log into the gateway you won't need to enter it again. (For more about keeping track of passwords, check out the "Make, Manage, and Keep Track of Passwords" in the Spotlight section later in this book.) Most gateways



FIGURE 6-4 D-Link's DI-624 password field is on the Tools tab of its administration console.

will log you out immediately after you change the administrator password, and you'll have to re-enter it to get back into the console and make other changes.

Change Your Gateway's SSID

All wireless gateways have a default setting for their SSID (Service Set Identifier), which is, for all intents and purposes, the gateway's name. Don't leave the SSID at its default setting; that just makes you look like an easy mark—someone who doesn't know how to make even a simple change to their wireless gateway.

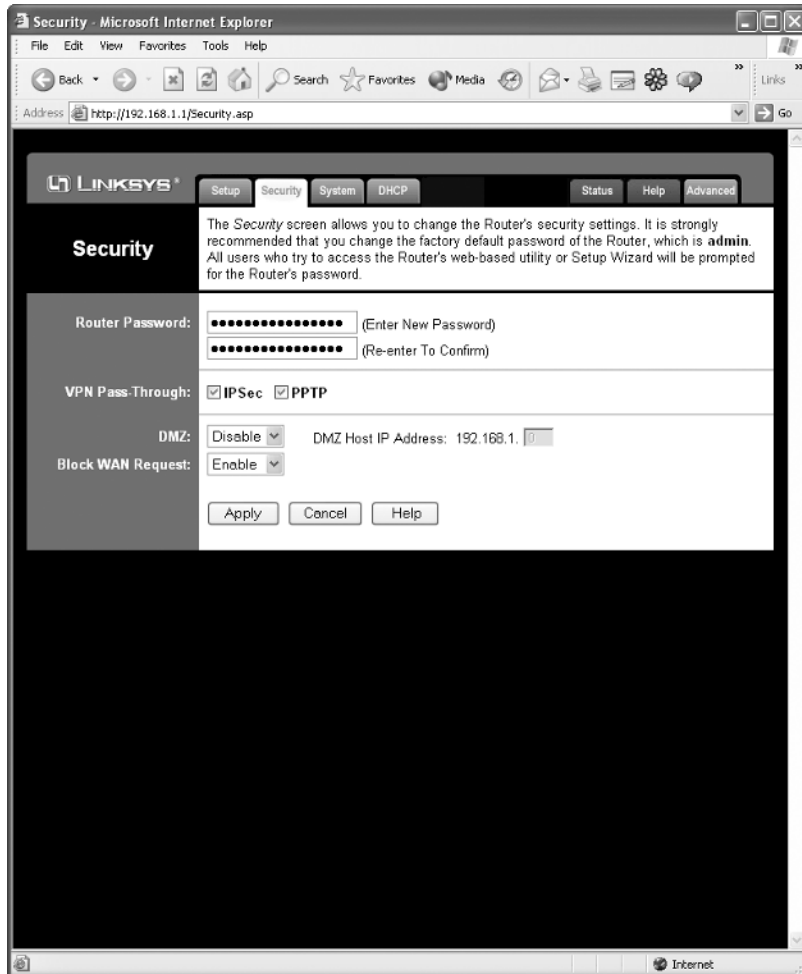
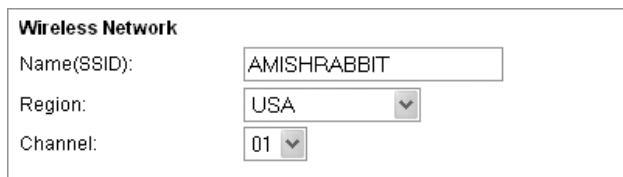


FIGURE 6-5 You'll find the password field under the Security tab on the Linksys WirelessG gateway administration console.

The SSID can be a name, a funny phrase, a word—literally anything you want (see Figure 6-6). Business folks will want the SSID to be meaningful (like “conference room” or “west side offices”), but home networkers can put anything they want in there. Pick an SSID that’s memorable and immediately obvious to you. When you see that name in the list of wireless gateways, you want it to stand out as yours.



Wireless Network

Name(SSID):

Region:

Channel:

FIGURE 6-6 Your SSID can be informational, or it can have personality, but you should always change it from the factory default setting.

One other thing to remember about SSIDs: Don't name your gateway with exactly the same SSID as another gateway, especially one that's using the same WiFi radio channel as yours. The SSID for each gateway should be unique.

6

Keep Your Laptop in Infrastructure Mode

Wireless cards can be used to network computers with or without gateways. When your WiFi card is set up to communicate only to a gateway or access point, we call this *infrastructure mode*. By contrast, when a laptop is wirelessly networked directly to another laptop—without the intermediary of a gateway—we call it an *ad-hoc mode* connection.

In order to switch between these modes, you have to manually change a WiFi card setting, either using Windows XP's wireless networking controls, or with the help of a utility application from the card's manufacturer. By default, Windows XP allows you to connect to either kind of network—a setting you should probably change. Open the Windows XP Control Panel, then click the Network And Internet Connections link. In the window that opens, click the link for the Network Connections control panel.

When that control panel opens, right-click the item labeled Wireless Network Connection, and choose Properties. Select the Wireless Networks tab, and click the button labeled Advanced at the bottom of the Properties window. In the Advanced window that will open, you should select the option labeled Access Point (Infrastructure) Networks Only. If you change your laptop's settings to Computer-To-Computer (Ad-Hoc) Networks Only, you won't be able to connect to a gateway unless you change it back to infrastructure mode.

If, for some reason, you can't connect, and you suspect you switched your laptop into ad hoc mode accidentally, open the Wireless Network Connection Properties page (as just described), click the Wireless Networks tab, and click the Advanced button to check that the card is running in infrastructure mode, as shown in Figure 6-7.

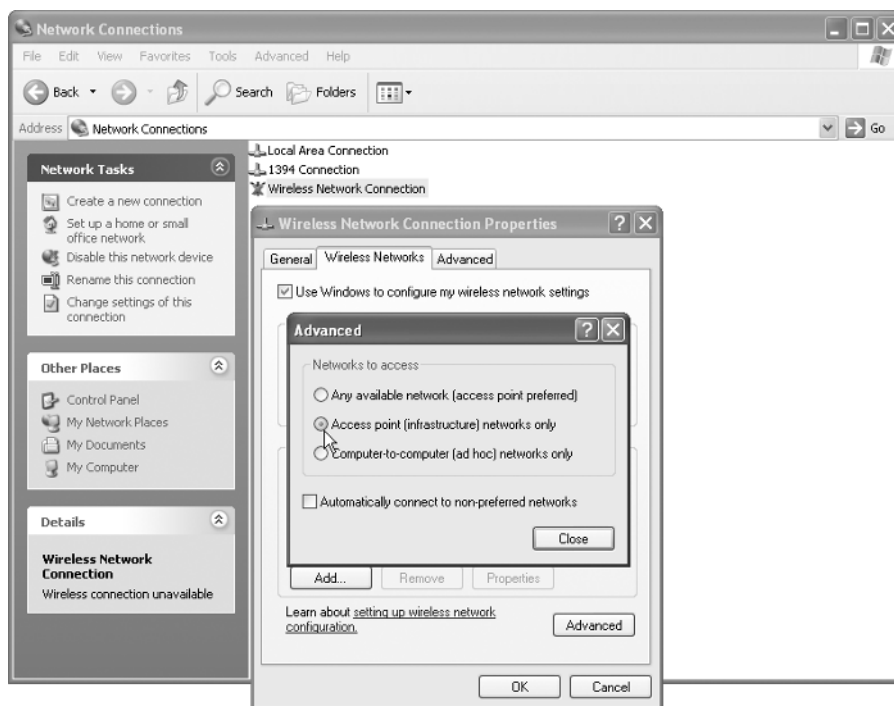


FIGURE 6-7 You should change the default Windows XP setting that could let you connect directly to another computer.

One important detail you should pay attention to is the box labeled **Automatically Connect To Non-Preferred Networks**. While you're poking around in Windows XP's wireless network settings, be careful not to fill in that check box. If you do, Windows won't alert you if your laptop's WiFi card picks up a stronger signal from someone else's gateway and tries to connect to it (see Figure 6-8).

It's not hard to see why you normally wouldn't want your laptop to be able to talk directly to other laptops, so unless you find yourself in unusual circumstances—say, you want to transfer a lot of files from one laptop to another, and you're nowhere near your wireless network—keep that laptop talking to the gateway.

Always Turn off File and Print Sharing on Your Notebook

You should never, ever use Windows XP's File and Print Sharing when you use a wireless network. File and Print Sharing is a huge security loophole; hackers with special software could browse your entire hard drive if you've set up File Sharing

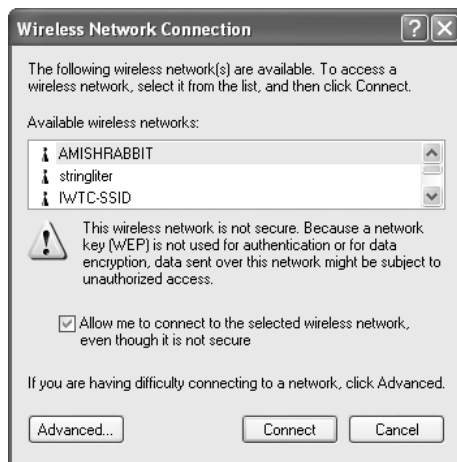


FIGURE 6-8 If you try to connect to an insecure network, Windows XP will let you know.

incorrectly. If you use a wired Ethernet network at home or work, and you turn on File and Print Sharing temporarily, be sure to disable it again before you leave the safe confines of your own wired network.

The quickest way to do this is to disable the Server service in the Computer Management console. This console controls, among other things, the background applications (called services) that keep Windows running. Many of these services are important, so unless you're familiar with what services do, you shouldn't immediately jump into turning off a bunch of them. In this special case, you'll shut off one of these services that you don't normally need anyway.

To get into the list of services, right-click My Computer and choose Manage; in the left pane of the console window, expand the item labeled Services And Applications by clicking the small plus sign to its left, and then single-click the subcategory labeled Services that appears. The list of all services installed on the computer will appear, along with basic information about them, such as whether they're running, if they start up when you boot the computer, and what parts of the operating system depend on the service in order for them to work.

Turning off the Server service will prevent anyone from being able to connect to your laptop and browse the hard drive, but it won't keep you from being able to do the same. Find the item in the right pane named Server and double-click it. In the Server Properties window that appears, click the button labeled Stop and wait a few seconds while Windows shuts down the service.

This will turn off the service until you log out or reboot the computer. If you want the Server service to remain disabled, click the drop-down menu named Startup Type and choose the Disabled option (see Figure 6-9). If, for whatever reason, you need to use file sharing for a few minutes, you can re-enable it by choosing the Manual option from the Startup Type drop-down and then clicking the button labeled Start in the Server Properties window.

Always Use the Latest WHQL-Certified Drivers for Your WiFi Card

Wireless card drivers—the files that allow Windows XP to control the card—can be a big source of headaches in Windows XP. Windows XP introduced Microsoft's first foray into wireless network management tools, and like all first attempts, it tended to be a little buggy. Well, “little” might be too generous: problems with the driver software that lets Windows use your card for networking can cascade into far more difficult-to-troubleshoot problems.

When hardware manufacturers write Windows XP drivers for their devices, they're required to submit them to Microsoft for certification. Microsoft can let the card makers know their drivers don't have bugs that break other things in Windows XP.



FIGURE 6-9 If you set the Startup Type to Disabled, the service won't run at all; setting it to Manual will let you start and stop it at will.

These certifications from the Windows Hardware Qualification Lab, or WHQL, are an important indication that the driver will work properly and won't cause other problems.

But when you buy a new wireless network card for a laptop, the drivers on the CD in the box may not be the WHQL-qualified drivers. When you install these drivers, Windows will throw an error message in front of you. You may be accustomed to clicking the Continue Anyway button, but in this case, consider not installing the driver at all until you can get the latest WHQL version (see Figure 6-10). However, if you look on the manufacturer's site and find that they don't offer a WHQL-compliant driver, go ahead and install the noncompliant driver anyhow, but keep in mind that this might cause connectivity problems down the road.

NOTE

When looking at updated drivers on the manufacturer's site, you may see more than one version of the driver software available for download. These can include newer, pre-release versions that haven't been qualified, and slightly older versions that are already certified to work correctly with Windows XP. Carefully choose the latest qualified drivers, not just the newest ones.

If you're an experienced computer user, you may not even need to use the CD. You can go ahead and download the newest WHQL drivers and/or utilities from the manufacturer's Web site before you install the card. Once you have a working copy of the drivers on your laptop's hard drive, you can use the driver CD for its other, more practical purpose: putting your drink down on it before you leave a ring on your desk.



FIGURE 6-10 If you see this dialog box while installing your drivers, stop the installation, download the qualified drivers, and then continue installing your card.

Survey Your Wireless Network with NetStumbler

Sometimes, the simplest way to illustrate the vulnerability of a wireless network is by probing it with the same tool an intruder would likely use. NetStumbler (available as a free download from www.netstumbler.com) is just one of a number of freely available war driving tools that serve a dual purpose: it can help you secure your network by showing you exactly where its weaknesses are.

NetStumbler works by switching your WiFi card into what's called *promiscuous mode*, where it stops transmitting and simply listens intently, taking in details about every WiFi signal within range. Not all WiFi cards can be switched into this mode, and NetStumbler doesn't work with all of the ones that do, so be sure to browse the list of supported WiFi cards on the Web site before you download the program.

NetStumbler's main window will display a list of every gateway, laptop, wireless PDA, or any other kind of WiFi device within your card's "earshot" (see Figure 6-11). Among the information it can collect, you'll see the SSID and MAC addresses of most gateways, what channel they're broadcasting on, and whether they have their WEP or WPA encryption enabled. You may also be able to determine whether a gateway is running a DHCP server (which assigns an IP address to any computer that associates with the gateway; see Chapter 3 for more about DHCP), what computers are connected to that gateway, and their IP and MAC addresses.

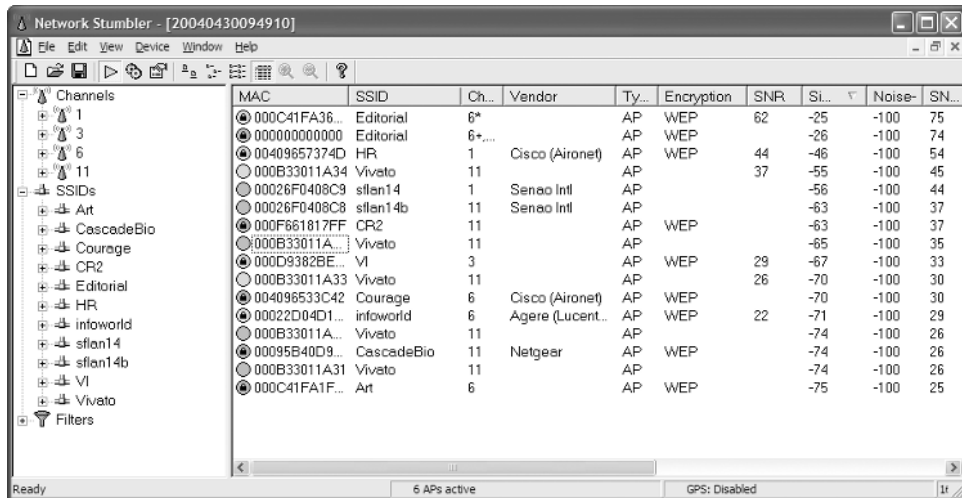


FIGURE 6-11

NetStumbler's list of discoveries can quickly grow, depending on how many people in the immediate area are running WiFi gateways or have wireless laptops.

Most importantly, though, the program lists the signal strength of each device it can detect. Most war drivers use this feature almost like a Geiger counter to find the location of a gateway. You can use this feature, as you walk around your home or office, to see how much of your gateway's radio signal is reachable from the road, the sidewalk, the café across the street, or anywhere else an unwanted visitor might be able to try to connect to your WiFi network.

How to ...

Cut Through WiFi Traffic Jams

6

When lots of neighbors use WiFi in close proximity to one another, they can overload the WiFi radio band, causing everyone's networks to slow down or stop working altogether. That's because most wireless network devices use the same radio frequencies by default. When enough networks come together, all using the same frequencies, the whole system grinds to a halt.

WiFi devices can be set up to use any of 13 different WiFi "channels," but only three of those channels—1, 6, and 11—are completely separated so that their broadcast signals don't overlap with the adjacent channels. Most networking gateways sold in the U.S. default to using channel 6. If your gateway is set to use channel 6, and enough people around you all have their gateways set to the same channel, pretty soon you have a radio logjam of epic proportions.

With enough gateways in a relatively small area, the gateways can quickly overload the channel. Pretty soon, every gateway will try to "shout" louder to be heard above the crowd, and everybody's network—yours and your neighbors'—will slow down as a result.

Fortunately, there's an easy solution to this problem: change your channel. When you use Netstumbler, you'll be able to see which channels the other nearby networks are using, and how strong each signal is. If both your network and most of the other ones with a strong signal are using channel 6, for example, change your gateway's wireless network setting to use channel 1 or 11.

Changing channels can solve a lot of hard-to-diagnose performance problems, though you'll periodically want to use Netstumbler to make sure you're still using a different channel from most of the other networks around you.

Keep Your Data Secure over Your Wireless Connections

Your gateway can *encrypt* (or make unreadable to casual observers) the wireless connection between itself and your laptop, PDA, or other WiFi-enabled device. The built-in encryption provided in gateways is the most important security feature you can use to protect your data when you use a wireless network.

Two kinds of encryption standards exist for WiFi networks; each has certain benefits and trade-offs. WiFi Protected Access (or WPA), the newer of the two standards, should be your first choice if the security of your data is most important to you. WPA fixed several serious flaws that severely weakened its predecessor, WEP (which stands for Wired Equivalent Privacy). But WPA's trade-offs are significant: WPA was made a standard addition to wireless network equipment that was sold after September 2003. In addition, you can upgrade some slightly older WiFi cards and gateways so that they support WPA. But many older devices simply can't handle WPA and won't be able to connect to your network if you're using WPA exclusively.

As you've probably guessed by now, the major downside to WEP, the first WiFi encryption scheme, is that it was released with flaws that make it much easier to break into than WPA. However, WEP does have a key benefit: virtually every wireless networking device on the market supports WEP. If compatibility is more important than tough security, WEP will do a decent job of protecting you. It's better than nothing.

WiFi Protected Access (WPA)

WiFi Protected Access, or *WPA*, jumbles up the data in a wireless connection so that a casual snoop cannot simply sniff data out of the air. In addition, it prevents anyone who doesn't have the encryption key from being able to associate with the access point, so unauthorized people can't hop onto your wireless network willy-nilly.

You'll find WPA encryption in most 802.11g (the high-speed, 56 Mbps WiFi) gateways and devices, and in some newer 802.11b (standard, 11 Mbps WiFi) units, as well. WPA has the advantage of tougher encryption mechanisms than the earlier encryption standard, WEP, so it isn't nearly as vulnerable to being cracked by a hacker. It also has a much more user-friendly interface for setting up the encryption key.

What Are WPA's Requirements?

In order to use WPA, you need to make sure all the devices in your wireless network—the access point(s) or gateway(s), and all the wireless cards you plan to use—will work with WPA. Not all do. You might need to check the Web site of your wireless card's and gateway's manufacturer to find out.

Did you
know?

Using a Free Public Wireless Network Is Risky Business

WiFi users in public places, such as at cyber-café, hotels, or airports, need to take special care to protect laptops and PDAs from data thieves. One mistake could result in your delivering the keys to your kingdom right into the hands of those who want to take it away. The rule for using WiFi in a public place is to trust no one—not even the network itself.

Public WiFi networks can be places where nefarious types engage in “sniffing,” where a stranger uses his or her own laptop to listen to all the radio signals in a given area. Cyber-café, or even just regular cafes that provide free WiFi access, make a perfect place for a cyber-crook to hang out all day and collect passwords, or any other valuable data that flies through the air. But sniffing can happen anywhere you use an unprotected wireless network, including at your home or office.

If you use public wireless networks often, do what you can to reduce your risks. Rather than checking your e-mail with Outlook Express, use a Web-based e-mail account that encrypts the connection (Hotmail and Yahoo mail do this, for example, but only if you choose their *secure* setting when you log in), and avoid logging into Web sites that require a login if the page isn’t secure or if you’re not sure (look for the little locked padlock icon at the bottom of your browser window). If you can use a work-based VPN (virtual private network) connection while on the road, use it. And make sure you’re running a software firewall, and that your laptop is up to date with any Windows Update security patches for problems with a severity rating of *high* or *critical*.

You may discover that everything works perfectly out of the box, or that you will need to update the firmware (software on chips inside the wireless card or gateway) for one or more your wireless devices, or download updated drivers or utilities—or a combination of these things. You might also find firmware upgrades that add WPA support to gateways or cards that shipped to stores before WPA was available. You can upgrade many (but not all) older 802.11b products sold between 1999 and 2002 in this manner.

If you find that any of the devices on your wireless network doesn’t support WPA, you’ll have to decide whether WPA is important enough that you need to chuck that older wireless device and buy a newer product, or just use WEP.

WPA didn’t exist when Windows XP was first released, so Microsoft didn’t build support for the scheme into the operating system. Soon after the WPA standard was

finalized, though, Microsoft released a patch for Windows XP that adds in the required support to allow you to use WPA. While the patch has been available for some time in Windows Update, it's not considered a critical patch, so you may not have loaded it onto your system already. Head to <http://find.pcworld.com/42352> to pick up the system patch (you'll find a link to the download near the bottom of the page, labeled "Download the Windows XP i386 package").

Configure WPA on Your Gateway and Laptop

When you use WPA, you protect your network by entering a passphrase (a longish password, from 8 to 63 characters in length) into a configuration page in your gateway's administrative console. Thereafter, anyone who wants to connect enters the same passphrase into their Wi-Fi card settings (these can be located either in Windows XP's network configuration, or in an application that shipped with your wireless card). Without the passphrase, a would-be user can't connect. This type of security is called *WPA Pre-Shared Key*, or *WPA-PSK*, depending on the gateway manufacturer.

The location of this configuration page in your gateway's admin console will vary from manufacturer to manufacturer, but it should be fairly easy to suss out if you dig around a little. Most often, there's a tab or pane labeled "Wireless" you can click to get to all the wireless network settings (see Figure 6-12).

In Windows XP, you'll enter the WPA passphrase into the Wireless Network Connections profile for a specific gateway's or access point's SSID. If you use more than one network, you can set up a different WPA passphrase for each one.

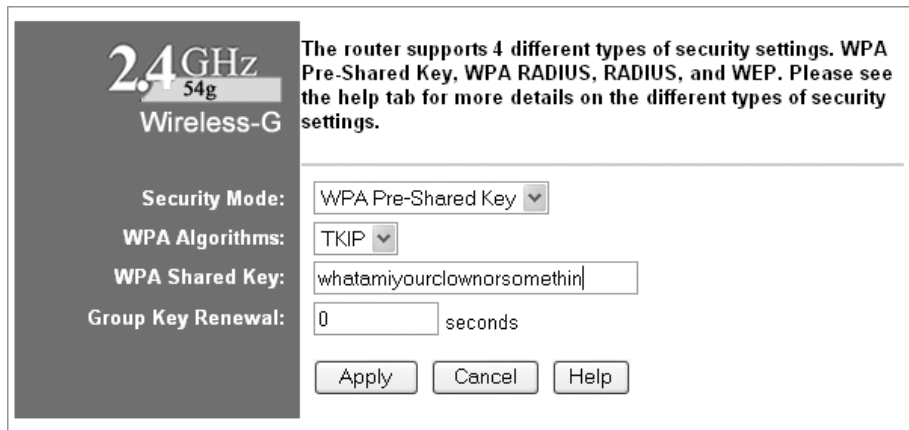


FIGURE 6-12 The Linksys Wireless-G gateway displays the text of your WPA key rather than a row of bullets or asterisks.

To enter the WPA passphrase into your Wireless Network Connections profile, open My Network Places, and then click View Network Connections in the left pane. Right-click the listing for your WiFi network connection, select Properties, and double-click the SSID of your network in the Preferred Networks pane (you'll find it in the lower half of the Properties dialog box). In the Association tab, choose WPA-PSK from the Network Authentication pop-up menu. (Unless you're using WPA on a corporate network, don't choose the plain WPA option.) In the Data Encryption pop-up menu, select TKIP, enter your WPA passphrase (you'll need to enter it twice), and click OK to save the profile. (TKIP refers to WPA's Temporal Key Integrity Protocol.)

NOTE

Though the WPA privacy standard is highly secure, InfoSec News (<http://find.pcworld.com/43306>) reported in late 2003 that a passphrase fewer than 20 characters long, composed entirely of words, could be cracked easily. But at 20 characters or longer, the algorithmic math of passphrases starts working in your favor, and you're safer. You have to have a long passphrase, with some punctuation marks or numbers thrown in, and, unfortunately, most people won't want to go to the trouble.

6

Troubleshoot WPA Connection Problems

If you're unable to connect your laptop to your gateway over a wireless connection with WPA enabled, check that you have done the following things:

- Install Windows XP SP2 (<http://find.pcworld.com/43292>) or the SP1 Wireless Rollup patch (<http://find.pcworld.com/42352>).
- Check the gateway manufacturer's Web site to see if there's a firmware update you can load onto your gateway.
- Check the Web site of the company that makes your WiFi card (or if it's built into the laptop, the laptop manufacturer's Web site) for firmware or driver updates for your card.
- Make sure you're using WHQL-certified drivers for your laptop's WiFi card.
- Connect your laptop directly to the gateway with an Ethernet cable, log into the gateway, and check that the settings for your WPA shared key match those you entered on the laptop.
- Make sure that you've set the gateway to use WPA Pre-Shared Key (or WPA-PSK) mode and TKIP encryption.

If none of these suggestions work, don't hesitate to call the tech support number for your gateway manufacturer and/or wireless network card. Their technicians may know how to fix the specific problem that's preventing you from connecting.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy, or WEP, was the encryption scheme first available for wireless networks, and as evidenced by the name it was given, its creators thought you'd be at least as secure using WEP as you would if you were using a plain old wired network. Boy, were they wrong. WEP is built into every WiFi device, and using it is better than nothing, but its encryption routines are seriously, and irredeemably, flawed.

The most you can say about WEP now is that it keeps casual snoops at bay, though widely available software will let a serious intruder break a WEP key in as little as 15 minutes on a busy network.

Did you
know?

“Channel Bonding” WiFi May Jam Other Networks

Some kinds of gateways or access points use proprietary techniques to double the speed of a wireless network connection. The companies who sell these products sometimes call this technology “channel bonding.” The problem: channel bonding gateways can inadvertently jam other gateways' signals, making it hard (or impossible) for folks who aren't using channel bonding to connect to their own network.

The neighbors of the person running this kind of gateway often don't get it so easy: The channel bonding technology floods several WiFi channels at once with signals, and that can mess up the wireless networks of everyone within range, forcing everyone else's network to drop to the lowest possible speed—if they can connect to their network at all.

It's not always easy to figure out which neighbor has a gateway, let alone which one is using the channel bonding feature. Even if you could, they may not want to (or even know how to) change their gateway's default settings. That's okay, because you can just try blindly switching channels, or you could use Netstumbler, to find out which channels the channel bonding gateway is using, and then change your own gateway's channel to something different from the other, channel-bonded gateway.

Configure WEP

Setting up WEP encryption is almost identical to the process you'd go through to set up WPA. First, you'll enter an encryption key into the WEP security page in your gateway's administration console, and then you'll enter that same key into Windows XP's Wireless Network Properties dialog box.

CAUTION

Always change the setting on the gateway first. If you reverse the order and enter a WEP key into Windows before you set up WEP on the gateway, you'll lock yourself out of your own network.

While the overall process is similar, WEP gateway security settings differ from those for WPA gateways. For one thing, you'll be given an option to use either 40-bit WEP or 128-bit WEP. Choose the latter; you'll be a little safer from snoops, and your network won't transfer data any slower. When you use 128-bit WEP, your gateway will require you to create a 26-character-long shared key.

WPA asks you to enter a simple passphrase (a long password) as the shared key, but it's not as easy with WEP. Depending on the gateway manufacturer, you will be presented with a fairly complicated-looking set of options, some of which will allow you to use a passphrase, and some of which will accept only *hexadecimal* characters (the base-16 counting system uses the numbers 0 through 9, and the letters A through F). For simplicity's sake (as well as for compatibility), we'll assume you'll use the hexadecimal option, which may be labeled HEX in drop-down menu or dialog box options (see Figure 6-13).

Creating a key in hexadecimal isn't hard. You can make up a key using any memorable numbers: birthdays, phone numbers, your street address number, your apartment number. Some people create keys out of a series of words you can spell out with the letters A through F, and the numbers 0, 1, and 5 (which almost look like the letters o, i, and s, respectively). Many make up short words, such as f00d, beef, or f1d0. You can combine short words to make a memorable phrase your WEP key, or you can use one long word. If you're a fan of the classic rock band The Police, for example, you could create a WEP key of deed00d00d00deedaadaadaaaaa. As long as your key is exactly 26 characters in length—no more or less—and uses the hexadecimal characters, you can use whatever you want.

Most gateways permit you to enter as many as four different WEP keys, so you can more easily change them around (see Figure 6-14). I'm going to break with the maximum-security attitude I've taken throughout this chapter and make a compromise for convenience here. Just use one key, and when you need to change it, change it on the gateway and on the laptop at the same time. Letting your gateway rotate through the keys automatically can result in your ending up locked out of your own gateway, which isn't fun.



FIGURE 6-13 Choose the hexadecimal (or hex) option when it's time to enter your WEP key.

Troubleshoot WEP Connection Problems

WEP connections are prone to failure if you've installed non-Windows XP certified drivers. If you're having trouble connecting, run through this checklist of possible remedies:

- Install, or reinstall, the certified drivers for your laptop's WiFi card.
- Flash-upgrade the firmware in your wireless gateway or in your laptop's WiFi card.
- Install the Windows XP Wireless Rollup patch.
(<http://find.pcworld.com/42352>)
- Check the settings for your WEP key.
- Run through the steps outlined on Microsoft's Windows XP wireless networking troubleshooting page (<http://find.pcworld.com/42354>).

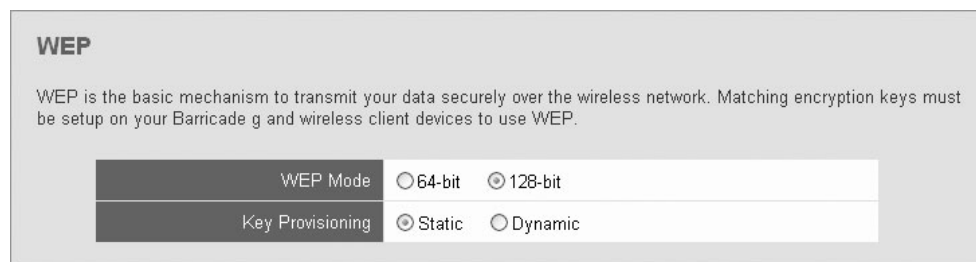


FIGURE 6-14 The WEP key setup page on SMC's 802.11g gateways calls the automatic key rotation feature *key provisioning*. Leave it set to Static, the default setting.

Did you
know?

WiFi Hacking Is a Crime of Opportunity

One thing's for sure: Computer crime pays like almost no other crime. Data can be more valuable than diamond rings, and authorities have a hard time tracking down infocriminals, let alone prosecuting those they catch. To a determined data thief, wireless networks are just another technology they can use against you.

Running an unprotected WiFi network—one where your passwords or credit card numbers fly through the air in the clear—just makes it easy pickings for data thieves. To listen in to a network, all they need is a laptop and physical proximity to a gateway without encryption enabled. Even the most inept, third-rate wannabe wireless hacker can find an insecure WiFi system with almost no effort, let alone snoop on the transmissions for a password or other valuable piece of information.

In most cases, WiFi-sniffing criminals are looking for a crime of opportunity, the data equivalent of a purse snatching. The criminal doesn't necessarily know who you are, or what data you have that's valuable. In short, they're out to get something quickly from the first mark they can find. Your computer equivalent of The Club, the metal bar you lock to your car's steering wheel as a theft deterrent, is encryption—something that makes your network connection at least difficult enough to crack that the crook will move on to someone else. For the average home user, even the relatively weak WEP encryption standard is better than nothing.

As with WPA problems, if you can't sort out the solution quickly, the gateway manufacturer's tech support should be your first stop for help. Most vendors' sites provide searchable online knowledge bases; these can get you an answer fast. Updates to the gateway's FAQ might also reveal the solution to a thorny problem. And don't forget to search for your problem on, or post questions to, the vendor's forum or message board. As a last resort, try the toll-free phone support.

Filter MAC Addresses

Wireless networks always broadcast the Media Access Control, or MAC, addresses of network cards as they transmit data. Virtually all wireless gateways allow you to set up MAC address filtering. MAC filtering lets you specify which wireless cards can associate with the gateway, though sometimes you can use MAC filtering to block only the computers you specify and let everyone else connect.

Used in conjunction with WPA or WEP encryption, MAC filtering adds another layer of protection to your wireless network. D-Link's MAC filtering controls, for instance, let you specify whether the MAC addresses you enter will be denied access, or whether they'll be the only ones able to connect to the network (see Figure 6-15).

But MAC filtering alone isn't as effective at keeping unwanted visitors off your network as when you combine MAC filtering with encryption. Using specialized software, someone listening in on your network can record the MAC addresses that successfully connect to the gateway, and then force their own card to masquerade as a card with a MAC address that's on the access list.

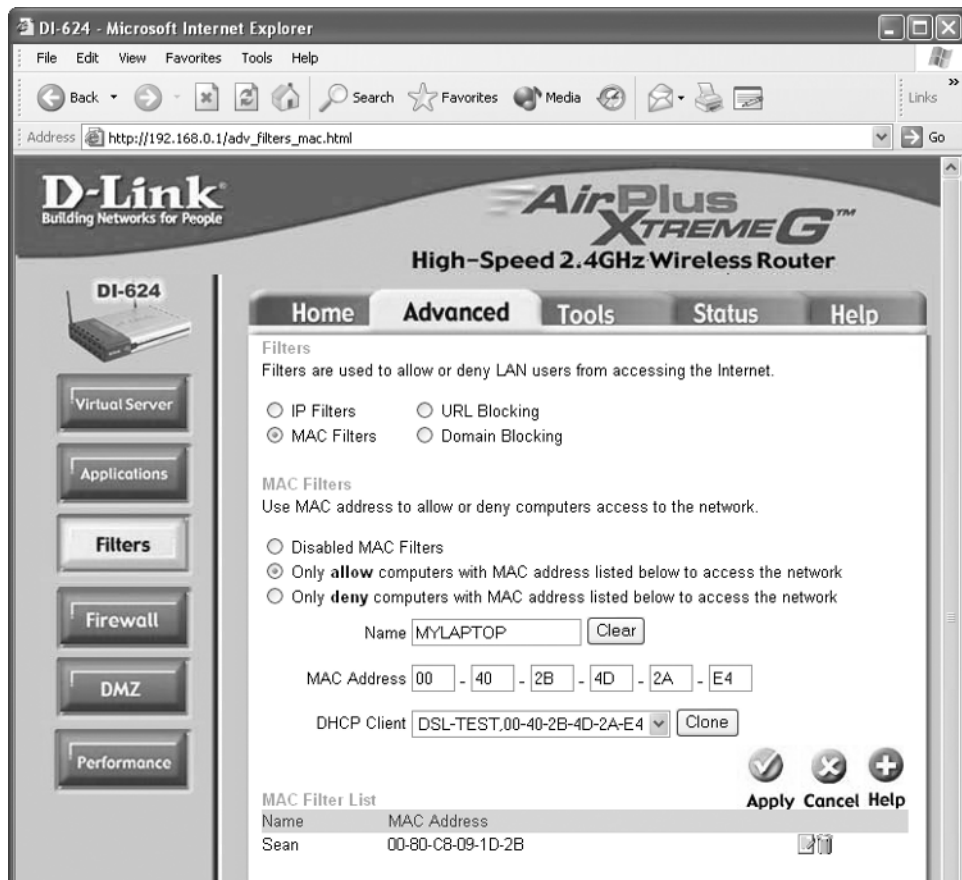


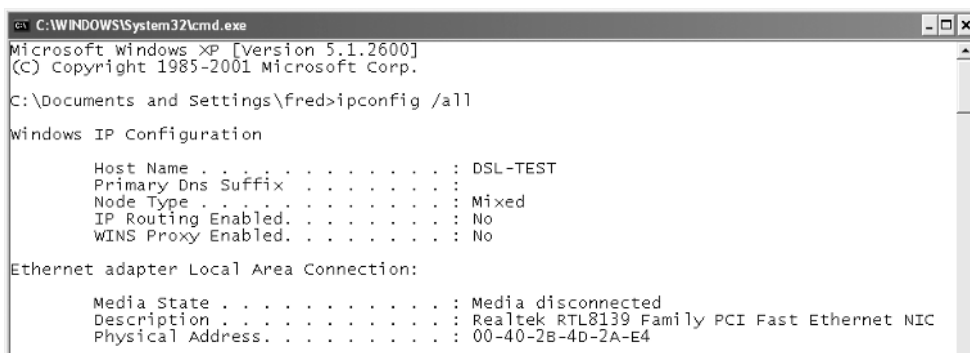
FIGURE 6-15 Using D-Link's MAC filtering controls, you can specify MAC addresses to be denied access or to be given exclusive access.

What's a MAC Address

Every networking device (including wired and wireless gateways, cable and DSL modems, and wired and wireless network cards) has a unique identifier called the *MAC address*. The 12-character MAC address, a combination of the letters A through F and numbers, is always printed on the device itself.

Windows represents MAC addresses as six pairs of characters, with a hyphen between each pair. You can find out the MAC address of any network card easily. Click the Start button, select Run, type **cmd** into the Open field, and then click OK. In the command window, enter the command **ipconfig /all** to list the details about the network cards in your computer or laptop. The MAC address of your network card will be the string of numbers and letters to the right of the label Physical Address (as shown here).

6



```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\fred>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : DSL-TEST
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Realtek RTL8139 Family PCI Fast Ethernet NIC
    Physical Address. . . . . : 00-40-2B-4D-2A-E4
```

Networks use the MAC address like an IP address to move data to the right place. But unlike IP addresses, MAC addresses are permanently set at the factory and cannot be changed. As a result, the MAC address on your wireless card is the only one like it in the world, which makes the MAC address a perfect tool to control who can associate with your gateway and use your network, and who cannot.

What MAC Filtering Can and Can't Do

MAC filtering is only a method of controlling access to your network, though it's not entirely foolproof at doing that. MAC filters can do the following:

- **Selectively block access** Prevent specific computers from connecting to your network.
- **Selectively permit access** Only allow specific computers to connect to the network.

- **Help you track access attempts** Most gateways keep a log of failed attempts to connect to the network. This can be useful for troubleshooting, or to determine the origin of a hacking attempt.

MAC address filtering can't perform a number of other important security-related tasks. Here are a few things that MAC filtering can't do:

- **Encrypt data in transit** It's not all that easy to sniff scrambled packets over the air, so casual sniffers don't bother. Encryption does what MAC address filters can't: It protects the content, as well as the delivery, of information.
- **Protect your privacy** Because MAC addresses always can be tracked back to one computer, anyone sniffing data from the network can quickly draw a one-to-one relationship between a specific MAC address and the person (or family) who uses the computer with a given MAC address.
- **Always be trusted implicitly** People who deliberately want to break into networks can sniff MAC addresses that are able to connect, and then *spoof* those working MAC addresses using their own software.

Did you
know?

You Can Share WiFi Safely If You're Feeling Generous

In kindergarten, we all learned the virtue of sharing limited resources—like crayons—with those around us. Some people continue this tradition well into adulthood by voluntarily sharing their broadband Internet access, by means of their WiFi network, with others around them.

Providing your Fellow Man free use of your broadband connection is truly a virtue. Best of all, it's easy to do so safely—as long as you're aware of the risks involved and know what steps you can take to mitigate them.

If you plan to play the role of bandwidth benefactor to your neighbors, visiting friends and family, or roommates, you can simply give them the WPA or WEP key of your network. If you use MAC address filtering in addition to encryption, you will need to add the MAC addresses of any computer that connects to your network to your MAC list as well.

If you don't mind sharing your broadband connection wirelessly with total strangers walking or driving past your home or office, keep in mind the following important points:

- **You can't use encryption** If you set up WEP or WPA, strangers or guests won't be able to associate with your gateway. It also means that if you want to have a relatively secure connection, you can't use your own wireless network—you will have to plug your PC or laptop into the wired Ethernet ports on your gateway to keep your data private.
- **Secure the gateway first** Don't count on others to play fair with your broadband; by changing the administrator password, you will lock down the gateway itself from remote intruders. This should be the very first thing you do when you turn on the gateway, anyhow.
- **You'll need to enable DHCP on the gateway** Follow the instructions in Chapter 3 to enable the Dynamic Host Control Protocol (or just DHCP) server on the gateway; without DHCP, visitors won't be able to get an IP address, preventing them from connecting to the Internet even if they can associate with the access point.
- **Leave a networked printer turned off unless you're using it** Some practical jokers think it's pretty funny to associate with a wireless network, and then print a thousand pages of nonsense to any networked printers they find. Don't be the next victim—shut off the printer with its mechanical power switch (putting it to *sleep* with a soft power button may not prevent someone from printing to it) or disconnect its network connection when you're not using it.

And if, as some WiFi users eventually discover, one or more people start leeching a little too much from your donated connection, you can clamp down on your bandwidth by turning on encryption or MAC filtering for a while. Hey, after all, you're the one who's paying for this stuff, right?

This page intentionally left blank

Chapter 7

Keep Your Systems Secure with System Updates



How to...

- Maintain Your Security with Patches
- Configure Windows XP Automatic Updates
- Locate and Install Operating System Patches
- Locate and Install Application Patches

In this chapter we will show you how to maintain the security you have worked so hard to establish. You will learn that security is more than settings on your firewall. There are things out there that no firewall can protect you against, namely those intruders you let in through the front door. You surely wouldn't intentionally let attackers access your system, but there are ways they can access it without your knowledge.

Operating systems and computer applications are composed of millions of lines of program code, and just as with any program, there are parts of that code that do not work properly or can be used in a way the original programmer never intended, with a bad result. We call these problems vulnerabilities or "bugs," and there are those who make a living finding and reporting them to the software manufacturers. The problem is that there must be disclosure of the program bugs, and there are those who scan the vulnerability disclosures daily to see what type of program they can write to attack any systems that have not been fixed yet. It takes some time to write the fix for the vulnerability, and some time to exploit the vulnerability. The result is an arms race of sorts, with the programmer hoping to get the patch written, tested, and distributed in time to avoid embarrassment at the hands of the attacker writing the exploit.

In this chapter we will use the terms patch and update interchangeably, for they are, in most cases, interchangeable. Where any special significance for one term or the other is intended, it will be called out at that time.

Why We Patch

It boils down to this: If we want to use programs that communicate with the Internet, we must keep our systems and applications up-to-date with security patches.

Recent statistics from DShield.org state that the average computer with no patches of any sort applied will be attacked and penetrated within the first 16 minutes of connecting to the Internet. Analysts from the SANS Institute estimate unprotected systems will be rendered unusable within 72 hours under the weight of all the malicious attacks they will be exposed to. This does not take into account where the computers are located. Just as there are different neighborhoods in any town or city, there are different neighborhoods on the Internet. And, just as with the town or city, there are those neighborhoods you would not want to be out in after dark.

As home users, most of us live in those neighborhoods. Attackers routinely scan the high-speed Internet networks of cable or DSL subscribers for vulnerable computers. High-bandwidth victims make the best bots and zombies. These systems can be used to conduct all-out attacks against corporate targets or pump out millions of spam messages.

Types of Flaws in Computer Programs

We will spend a little time giving you some background on the types of flaws attackers use to attack your systems to help you understand why it seems sometimes that software makers just can't seem to keep their systems secure.

Buffer Overflows

Programs read their data into storage areas called buffers to hold it while they process the data. An example of this is when you type an Internet address into your browser. This address directs your browser to connect to a remote server and ask for a specific file. The server places the request into a buffer and attempts to work with it.

What would happen if you typed in something that did not exist? Maybe a random filename? Typically, you would receive an error message telling you the file was not found. But if you fill the buffer and keep typing, the data you are typing could possibly overflow the buffer and put data into another area where it could do harm. This is called a *buffer overflow*. Buffer overflows can occur whenever the programmer forgets, or neglects, to validate the data being entered into the buffer for proper form and length.

What if you typed in 256 capital As, followed by shutdown /t0 (a shutdown command for Windows XP)?

Probably nothing. With a little trial and error (I don't know where they find the time), attackers can find the magic combination of As, or other characters, that fills the program buffer and drops the shutdown command where it needs to be to shut down the web server.

Bang! Denial of Service!

The Webmaster wonders why her machine went down, starts it up again, the attacker strikes again on this site and others having the same vulnerability, this time maybe with a command that installs a back-door program that lets the attacker control the machine and spy on its customers.

I'll let you finish that story.

Unchecked Buffers Buffer overflows are not a problem restricted to a single programmer, company, or industry. They have been discovered and exploited in most of the operating systems and many of the applications you will encounter online today. Do a Google search on "buffer overflow" and you will find a long list of affected applications.

The Dangers of a Buffer Overflow Buffer overflows are particularly tricky due to their prevalence. There are billions of lines of program code out there, millions of data buffers, and too many to count that are not validating the data entered into them. It takes a lot of work to review these programs for buffer overflow vulnerabilities and fix them. Organizations typically want to concentrate on new software that will make them more money, not old code that they have already sold. Buffer overflows often come to their attention when a security researcher reports them. There is an understandable time lag while programmers are pulled off other projects to deal with the new patch that must be issued. Meanwhile, the security researcher may have published an exploit to help demonstrate to the programmers how serious the situation is and, in the process, shown the hackers how to exploit the application's new vulnerability.

Communications Protocol Errors

Programs can communicate with each other with communications protocols. An error in the way they use the communications protocol, or a manipulation of the protocol itself, can cause the application to hang, crash, or turn control of the system over to the attacker. We will give examples of a way attackers can attack systems using communications protocols.

Overlapping IP Fragment Attacks The Internet Protocol is the transport backbone of the Internet and is a very mature and reliable protocol. It is designed to work in a large variety of circumstances and be flexible enough to work with many different systems. One way it does this is by allowing its data parcels, or packets, to be divided

up, or fragmented, to allow transmission over mediums that cannot support large packet sizes. Normally this fragmentation results in a group of packets that can be reassembled into data on the other end of the line. One packet might carry the letters A–L of the alphabet, while another brings in M–Z. When reassembled, they spell out the full alphabet.

In an overlapping IP fragment attack, the attacker constructs two or more packets that have overlapping data. One might have A–L, but the other might have G–Z. Alone they appear innocuous, but when assembled, they spell out something completely different, and possibly dangerous for the receiving system. It can be a shutdown command, a backdoor program, even an Internet worm probing systems to see if it can exploit a known vulnerability.

These attacks are difficult to defend against because the danger may not be realized until after the reassembly, which may happen inside your firewall. By then it may be too late. The packets may be reassembled into a malicious program or command that will go to work on your system.

Malformed IP Packet Attacks A similar type of attack is the creation of malformed packets (packets that have been intentionally modified with invalid headers, protocol options, or data) to confuse, disable, or break the communications stack.

They may not actually carry any malicious program, but they may be designed to simply kill the system that receives them. An example of this is the Land attack, which used a packet with the same source and destination address to confuse and crash systems.

Programming Errors

The last operating system flaw we will discuss is the programming error that, by itself, may not be dangerous but can be exploited by attackers to bring down a system.

Program Bugs Exploited for Denial of Service The creator of a computer program may inadvertently allow a condition where the program can be made unstable by the introduction of data that was not expected.

The programmer may discover this fact and fix the program, but without the user finding and installing the update, the program may remain vulnerable. All the attacker needs to do is send the data known to make the program unstable to every system known to be using the program. When a vulnerable system is located, it is brought down by the attacker.

Program Failure States While the preceding example may seem to be only a denial of service (loss of the services of the failing program), there is a more serious concern. If a program fails in a certain way when invalid data is introduced, it can leave certain parts of itself operating. Some programs can even be made to fail in such a way as to leave the attacker at the operating system's command line (a system interface where administrators usually execute their most powerful programs).

The Design/Test/Exploit/Patch/Hack Cycle

Software has a typical lifecycle. It is planned by the designer and coded by programmers. They test the program, and when satisfied it performs its task, they release it to their customers.

Flaw Introduced in Design

Occasionally, a designer may leave something out when planning an application. It may result in the program allowing access to sensitive portions of its operation or to the underlying operating system. These flaws can be found by customers or researchers who are attempting to evaluate the security of the program.

Flaw Discovered by Users or Security Researchers

Often when the customers begin to use an application, they may use it in ways the designers never considered. (Shame on the programmers for leaving them leeway to use the program in ways they shouldn't!) It may work well, or it may fail in unexpected ways. These unexpected failures may be the seeds of an attack method that can be used by hackers.

Exploit Developed

Security researchers may demonstrate the failure of the program by publishing a set of steps or a program that can be used to exploit the flaw. This is usually intended to help the designers fix the flaw, or at least prove how serious it is, but it can also be a roadmap a hacker can use to develop a malicious exploit.

Flaw Found and Patched

The program's designers may examine the exploit, find the flaw, and fix it. They will usually issue a program patch to eliminate the flaw on their customers' systems.

Hackers Exploit Flaw in Unpatched Systems

Sounds like a headline, doesn't it? Well, the news is that not everyone patches their systems. This can happen for various reasons. They may be unaware of the flaw, they may not know how to locate news of patches, or they may simply be too busy

to pay attention to such things. Unfortunately for them, the attackers will not miss the news of the flaw. They will begin scanning the Internet for vulnerable systems and attempt to compromise these systems for their own ends.

Use Windows Update to Maintain Your Operating System Security

We have hopefully made you more aware of the types of attacks your systems will fall victim to if they are not kept up-to-date. We will now begin to show you how to find and install these patches without launching into a second career.

The first tool we will explore is the Microsoft Windows Update site. This site is where you will find all security patches for Windows XP. Programs on the site scan your system and install the appropriate patches to eliminate any vulnerability that poses a security risk to your system.

7

How Windows Update Works

Windows Update uses a type of program called an ActiveX control that runs within Internet Explorer to scan your system for installed updates and provide you with a list of any available updates you do not already have. You then have the option of downloading one or all of the updates and applying them to your system.

NOTE

ActiveX is a Microsoft technology that works only in the Internet Explorer web browser, so you must be using Internet Explorer to use the Windows Update web site.

Use Internet Explorer to Access Windows Update

Windows Update may be accessed via one of the following means:

- On the All Programs Menu, Select Windows Update.
- On the Tools menu in Internet Explorer, select Windows Update.
- Navigate Internet Explorer to <http://windowsupdate.microsoft.com>.

NOTE

You may also navigate Internet Explorer to www.windowsupdate.com, but this address has come under attack in the past and had to be disabled.

How to ...

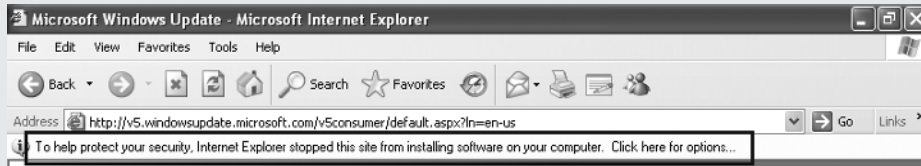
Use Windows Update to Update Your System

Windows Update Provides a list of any security updates along with other recommended updates available to patch your system. We will run through the use of Windows update to apply critical patches on a system running Windows XP with Service Pack 2.

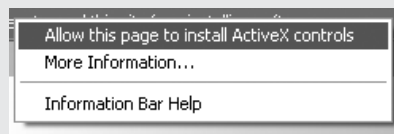
**CAUTION**

Occasionally, a patch will disable functionality you enjoy in a Windows program or break the system outright. If you are concerned about this, use the System Restore utility to take a system snapshot. It is located on the System Tools Menu under All Programs—Accessories on the Start menu. System Restore should take a system snapshot prior to performing any major update, but it never hurts to take one manually.

1. When the Windows Update page loads, you may see that Internet Explorer blocks the execution of the page's ActiveX control. This feature is included in Internet Explorer after Windows XP Service Pack 2 to prevent unknowingly running malicious ActiveX controls (which might be associated with certain web sites).



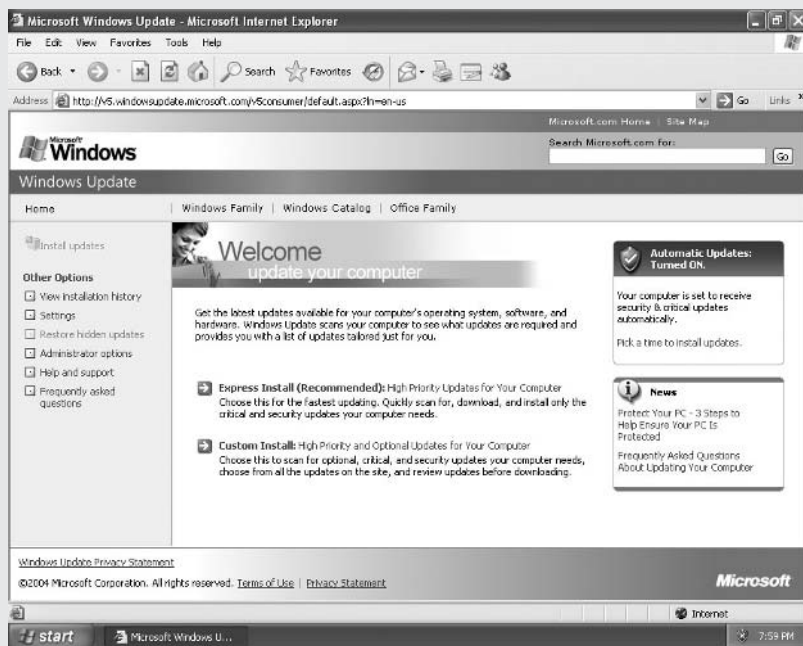
2. Click the message and select Allow This Page To Install ActiveX Controls. This will allow the necessary ActiveX control to load and scan your system for required updates.



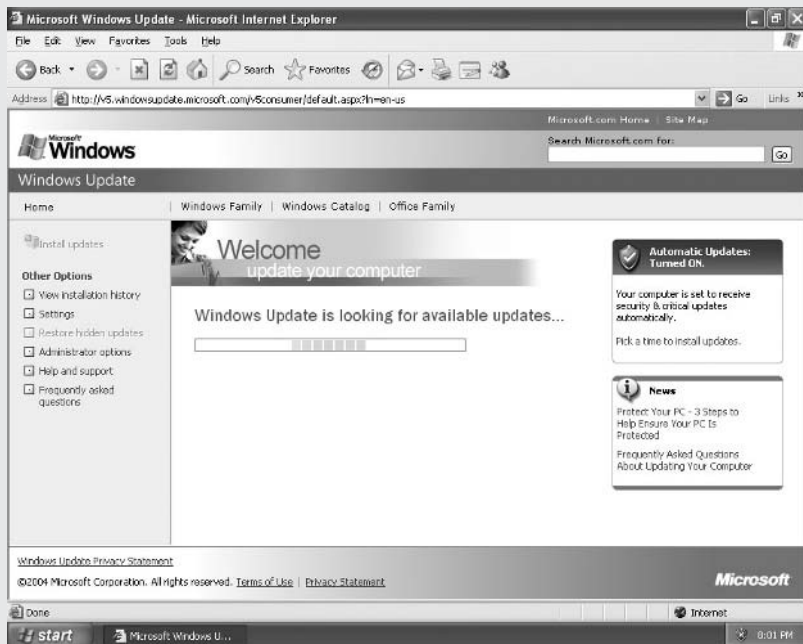
3. Click Install on the Internet Explorer Security Warning dialog box that may be displayed next.



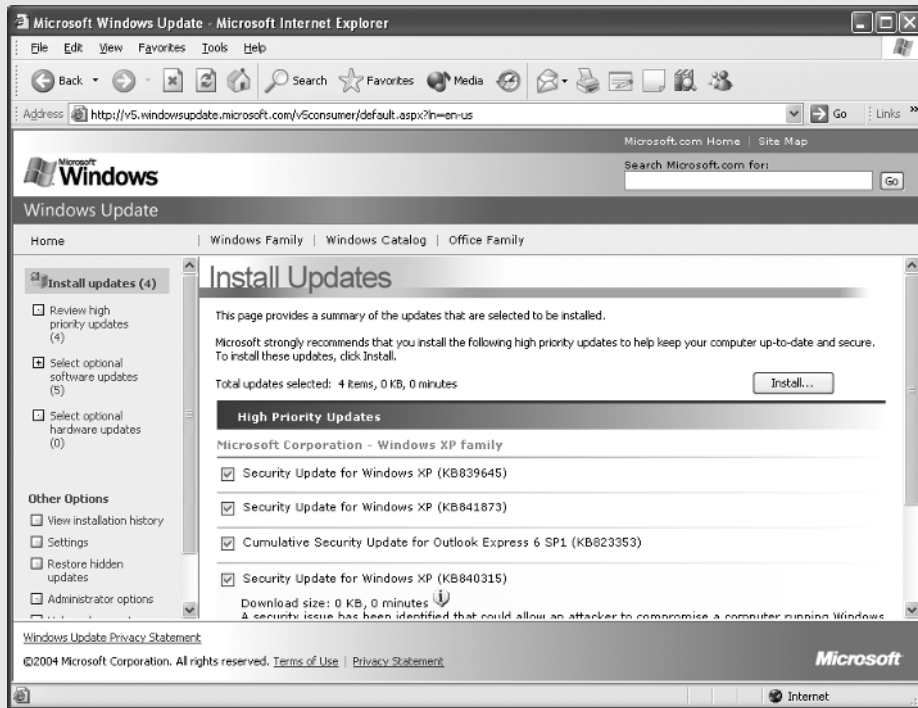
4. Windows Update will display a page giving you the choice to perform an Express Install or a Custom Install. An Express Install will install critical security updates only. The custom install will also give you the option to choose other, less critical patches and device driver updates. For frequent security patching, you will want to use Express.



5. Windows Update will begin to scan your system for installed updates.



6. After the scan, you will be presented with a list of updates you can download and install on your system. Choose the updates you wish to install and click Install. The updates will be installed. Restart your system if requested and you are finished.



Automate Operating System Patching with Automatic Updates

In addition to the on-demand Windows Update site, Microsoft provides the Automatic Update service to help you keep your system up-to-date. This service uses your Internet connection to check for new security updates. When it finds one, it takes one of three actions (depending on how you have configured it):

- Notify you that an update exists, but do not download it
- Download the update and notify you that it is available to install
- Download and install the update on a schedule that you specify

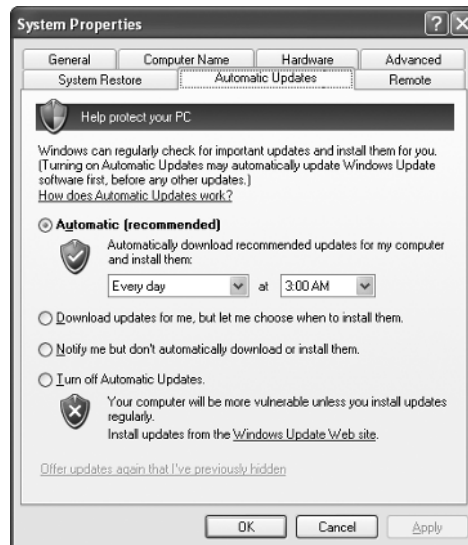
How Automatic Updates Work

Automatic Updates uses a service called Background Intelligent Transfer Service (BITS) to connect to servers at Microsoft to check for and download updates. BITS monitors your use of the Internet connection on your computer and transfers data only when your connection is idle. This use of idle time ensures you do not see any degradation of performance while updates are being downloaded.

After updates are downloaded, the installation routine can be configured to apply the updates automatically at a predetermined time. This time can be set to ensure updates are applied when you will not be at your system. If a restart is required, the Automatic Updates service will restart your computer.

Configuring Automatic Updates

Automatic Updates is configured using the System Properties dialog box, found either by opening the System icon on the Control Panel or by clicking the System icon in Security Center.



Notice the default setting specifies automatic installation of updates. This configuration setting was enabled in Service Pack 2. Prior to Service Pack 2, Automatic Updates had to be enabled before it could protect your system. I recommend you leave the settings as-is for now. This is the configuration chosen by Microsoft to provide the best protection settings by default.

NOTE

Pundits used to recommend varying the installation times for Automatic Updates to balance the load on Microsoft's servers. Before you change the installation time, consider that this is only the time the update will be applied. The download happens whenever you have idle time on your Internet connection. If you need to change the setting, choose a time that your system will be powered on but not in use.

Automatic Updates Settings

The options for installation of updates give you the opportunity to customize it to suit your needs. We will describe each one and give an example of where it might be used.

Automatic (Recommended) This setting is recommended by Microsoft because it ensures updates will be downloaded and installed without user intervention. This is especially important for those who are not aware their systems need protection. In the past, systems were compromised simply because their owners did not know security was an issue. Now these systems are protected by default, and often without the user's knowledge.

This setting is also a good basic setting for most configurations. When an update is available, you will receive notification via a small pop-up message from the Automatic Updates service. You may choose to install the update immediately or wait for the automatic installation process to perform the installation.

NOTE

Service Pack 2 made another change to updates that causes them to be applied any time the system is shut down. Even if you choose to automatically install updates, they will be applied any time the system is shut down regardless of schedule. This ensures they will not be missed if the system is powered off at the time they were to be installed.

Download Updates for Me... This setting will still download the update and notify you when it is available, but it will not automatically perform the installation. Some prefer this option because it allows them to personally ensure the updates are applied. Others prefer it because they can ensure updates happen while their systems are powered on. The change brought about by Service Pack 2 to install updates any time a system is shut down eliminates the need for this, but the setting remains for those who prefer it.

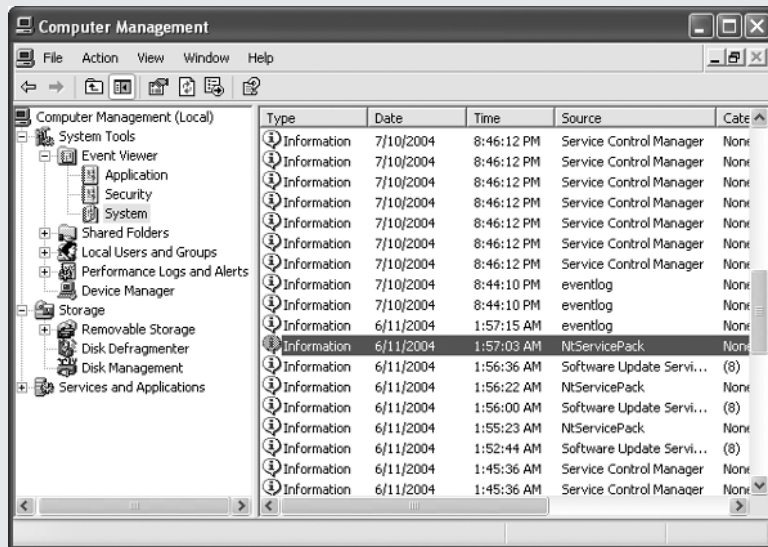
Notify Me... This option will look for updates and notify you when they are available. This is for those who may be on such a slow connection that they would rather wait until they get to the home office before they start the download.

Turn off Automatic Updates Please don't. Some experienced users leave updates off, but it requires a good deal of discipline to keep up with patching manually. At least getting notification of the availability of a patch is better than letting your guard down once and getting "wormed."

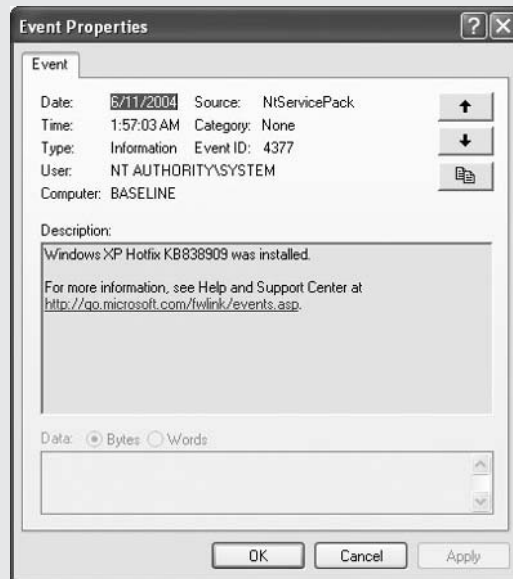
How to ... **Verify Your Automatic Updates Are Being Applied**

When your system automatically installs updates, it can be like the proverbial tree falling in the forest. How do you know they are applied when you are not there to witness it?

When Automatic Updates receives an update, it logs the receipt in the System Log. You can view this event by opening Event Viewer. Right-click My Computer and click Manage. You will see the Computer Management console. Expand the Event Viewer and select System.



Look for events titled “NtServicePack.” The details of the event will give details about which update has been applied.

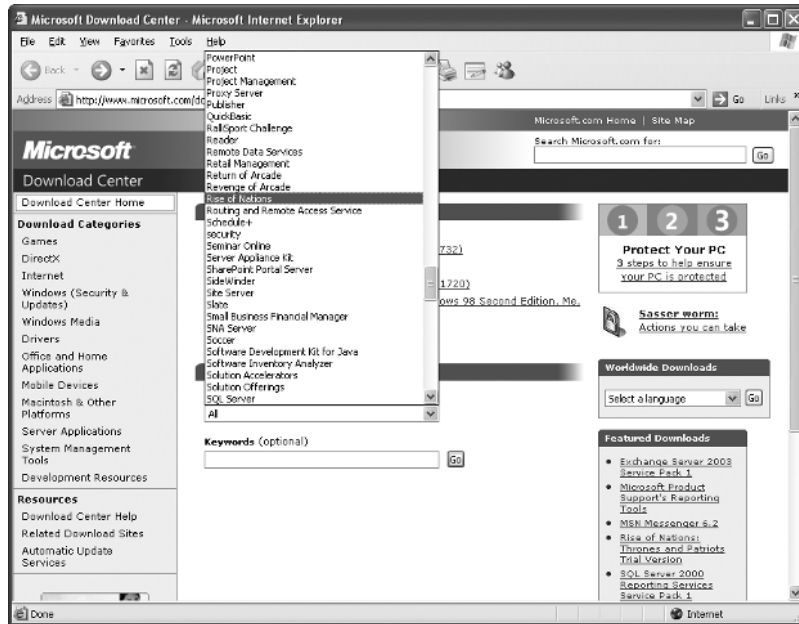


Maintain Microsoft Applications with Updates

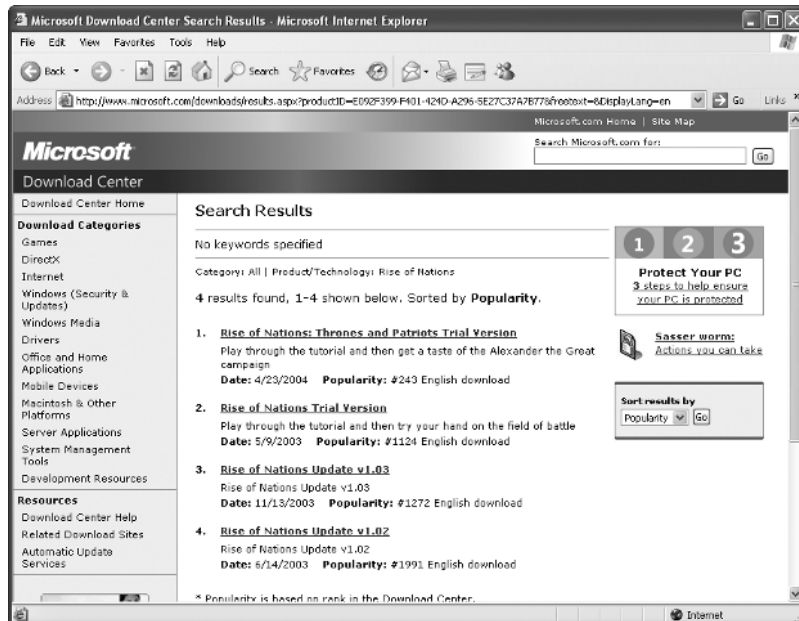
In addition to updates to the Windows XP operating system, Microsoft provides updates to the applications they produce. These updates can be for performance issues with the applications, security vulnerabilities in the application, or feature sets added to the application after its initial release. In this section we will show you where to look for updates for your Microsoft applications.

Locate and Download Updates for Microsoft Applications

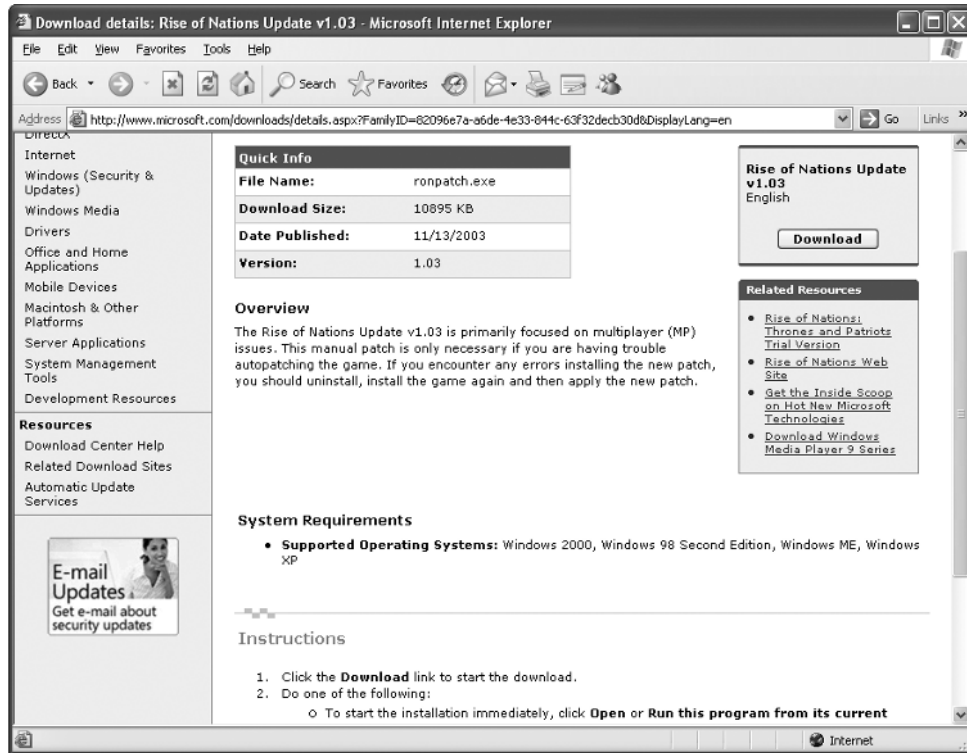
For those applications bundled into Windows, you will receive updates via Windows update and Automatic updates. For any other applications, you can find updates at the Microsoft Downloads site located at www.microsoft.com/downloads. This web site maintains a complete list of all Microsoft applications and lets you search for updates for them.



You can select the product you want to download updates for and get a list of all security, performance, and feature updates available for that product. The list can be sorted by popularity, title, or date of release.



When you select a patch, you will be presented with a screen detailing what the patch is intended to fix and providing installation instructions for installing the patch.

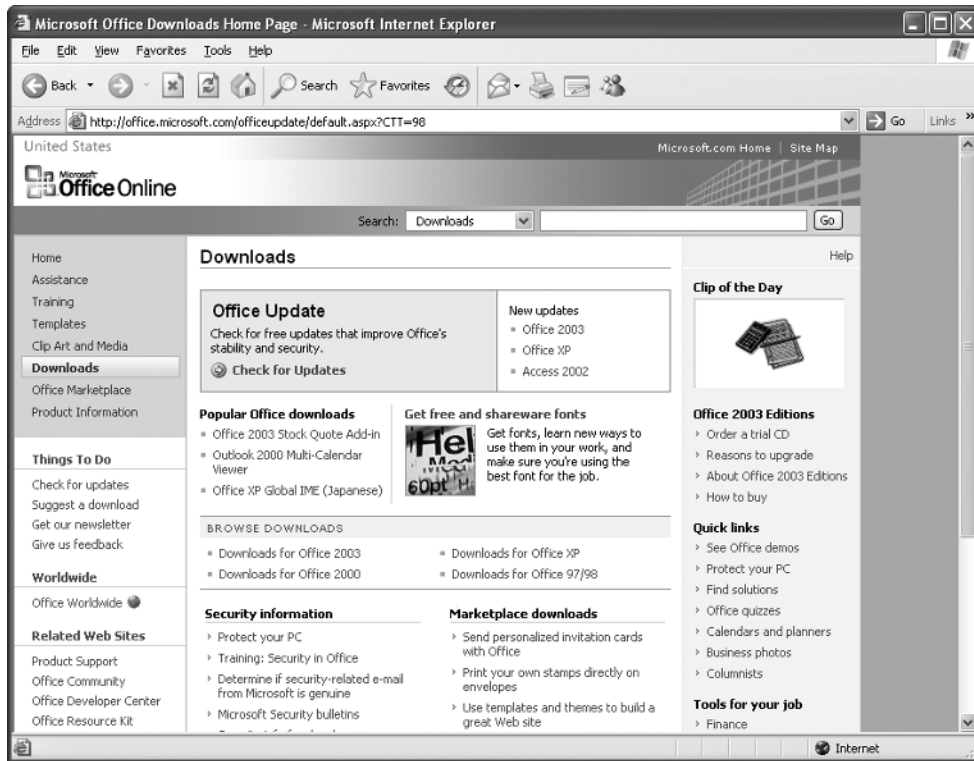


After clicking the Download button, you will begin downloading the patch. Follow the instructions to complete the installation.

Use Internet Explorer to Download Office Updates

The Microsoft Office application suite consists of many different Microsoft applications bundled into a comprehensive suite for interoperability and—let's face it—marketing. Keeping these applications patched would be a Herculean task if there weren't some way to help automate the process.

Enter Office Update.

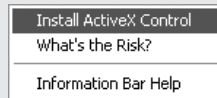


In the same way Windows Update finds and installs patches for Windows XP and its bundled applications, Office Update finds and installs patches for the Microsoft Office suite of applications. Visitors to <http://officeupdate.microsoft.com> will be presented with an ActiveX application very similar to the one used at Windows Update. Using the application, they will scan their computer for installed updates and download those they do not have.

How to ...

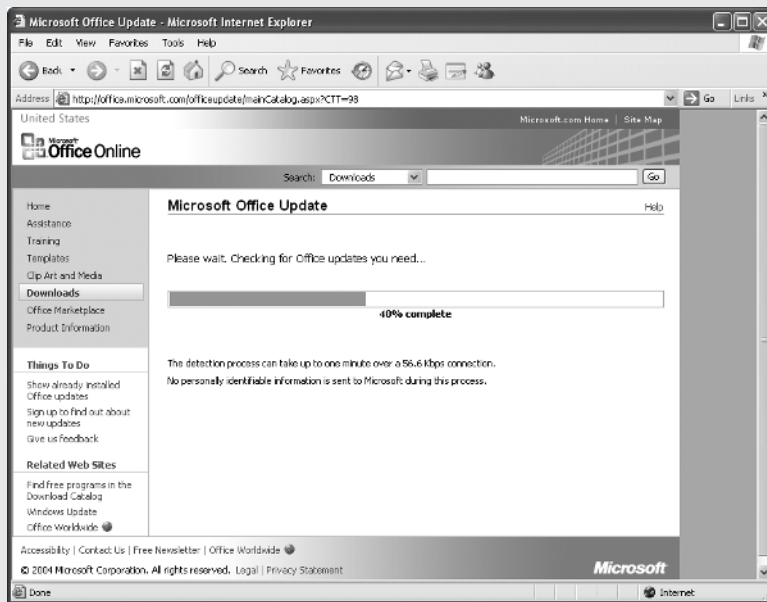
Use Office Updates to Install Microsoft Office Updates

The process of installing Office Updates is very similar to that of installing Windows Updates. The Office Update application is an ActiveX control that must be approved for installation just as Windows Update must be.

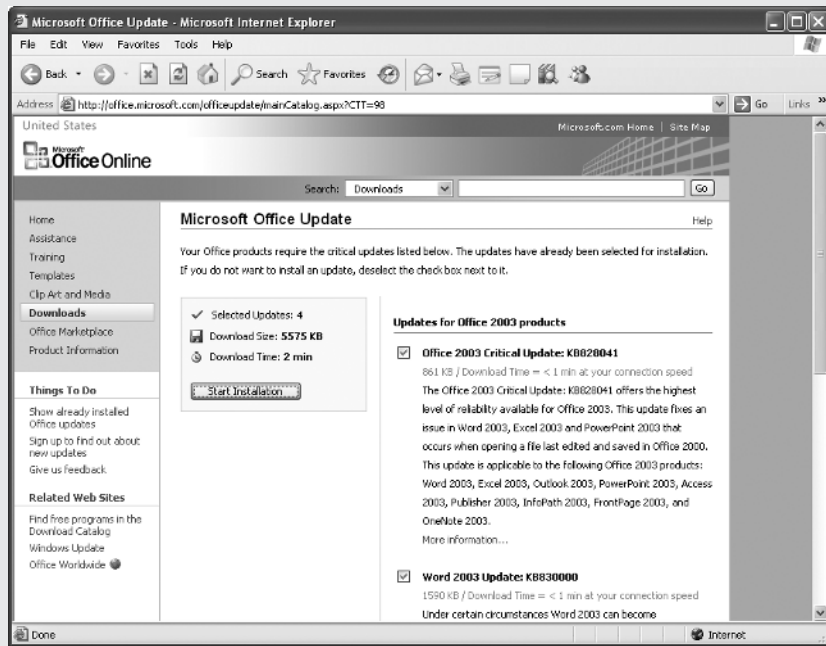


After the ActiveX control loads, it begins scanning your Office Applications for necessary updates.

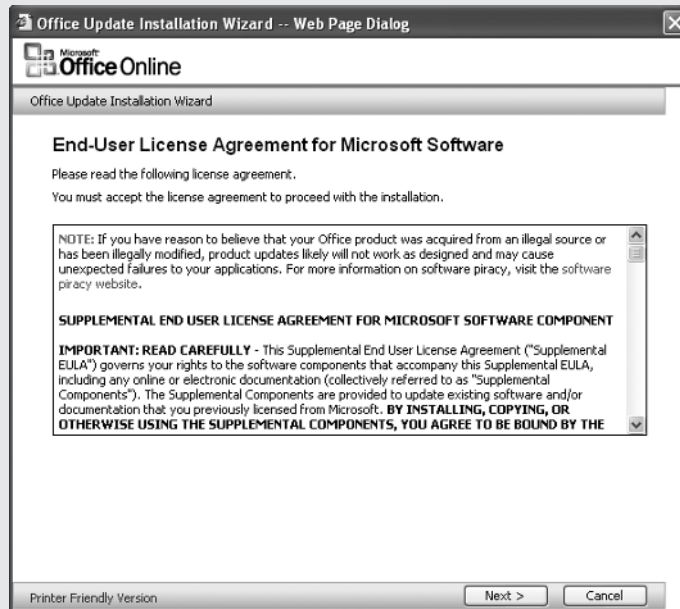
7



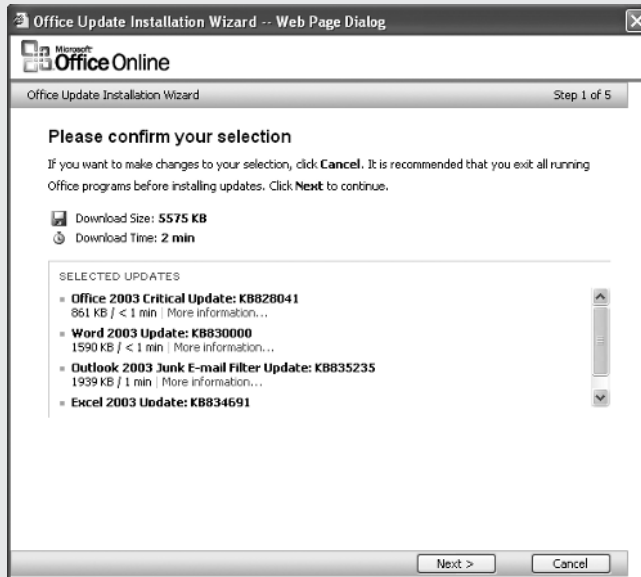
After determining which updates are needed, the application displays a list that you can choose from. A download size and an estimated download time are given. You may choose not to install all updates at once. If you unselect some, they will appear next time you use Office Update.



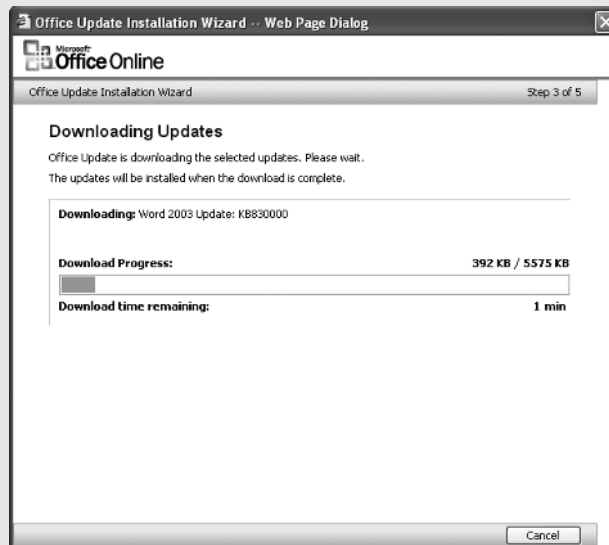
Office Updates then launches the Office Update Installation Wizard. This presents you with an End User License Agreement (EULA).



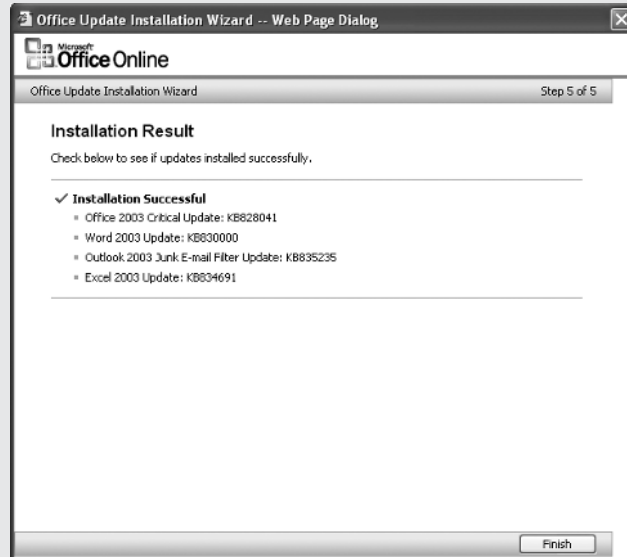
After reading and accepting the EULA, you will see a final confirmation screen.



After you accept the selections, the download and installation process begins.



After installation, you will see the Installation Results page. Check the status of the installation to ensure there were no errors during the download and installation process.



Maintain Non–Microsoft Application Security

Applications not produced by Microsoft are not immune to their own security problems. After listing the applications on your computer, do a quick Google search for the application name and the word vulnerability or the word exploit. You will get pages with information related to any known vulnerabilities your application may be prone to.

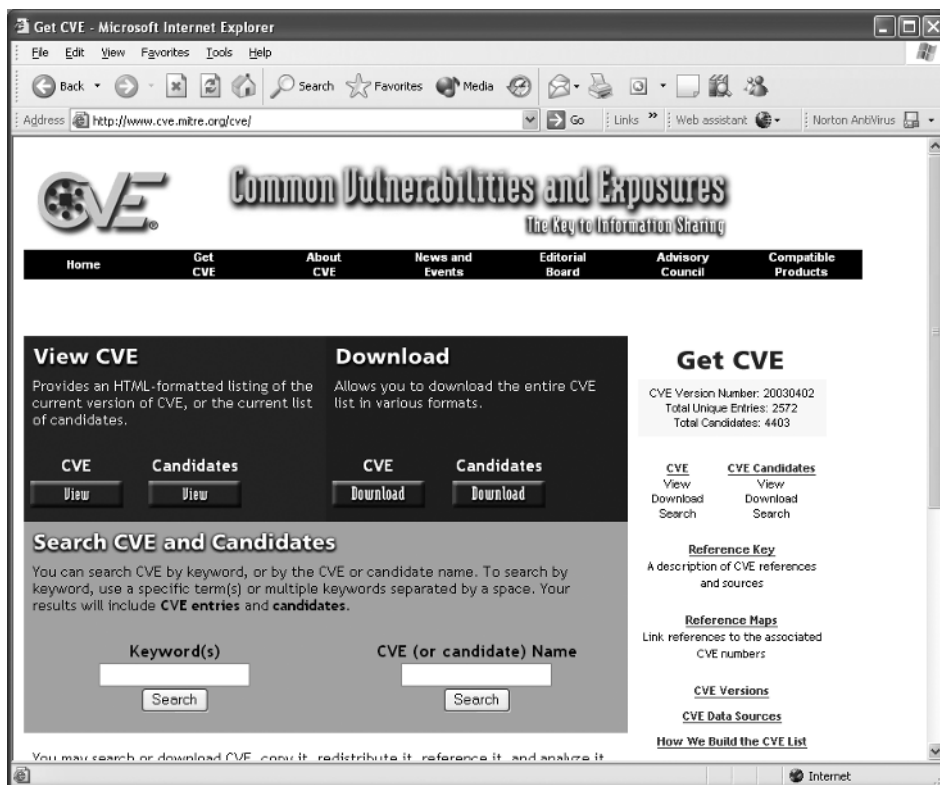
Locate Security Updates for Non-Microsoft Software

There are many places to look for information related to vulnerable applications. Hopefully you gain the ability by reading this book to know about these before the attackers do.

In this section we will describe sources of information on vulnerabilities and how to use them. Among these are the Common Vulnerabilities and Exposures (CVE) list, the Security Focus web site, and the web site of the software manufacturer.

Use the Common Vulnerabilities and Exposures list

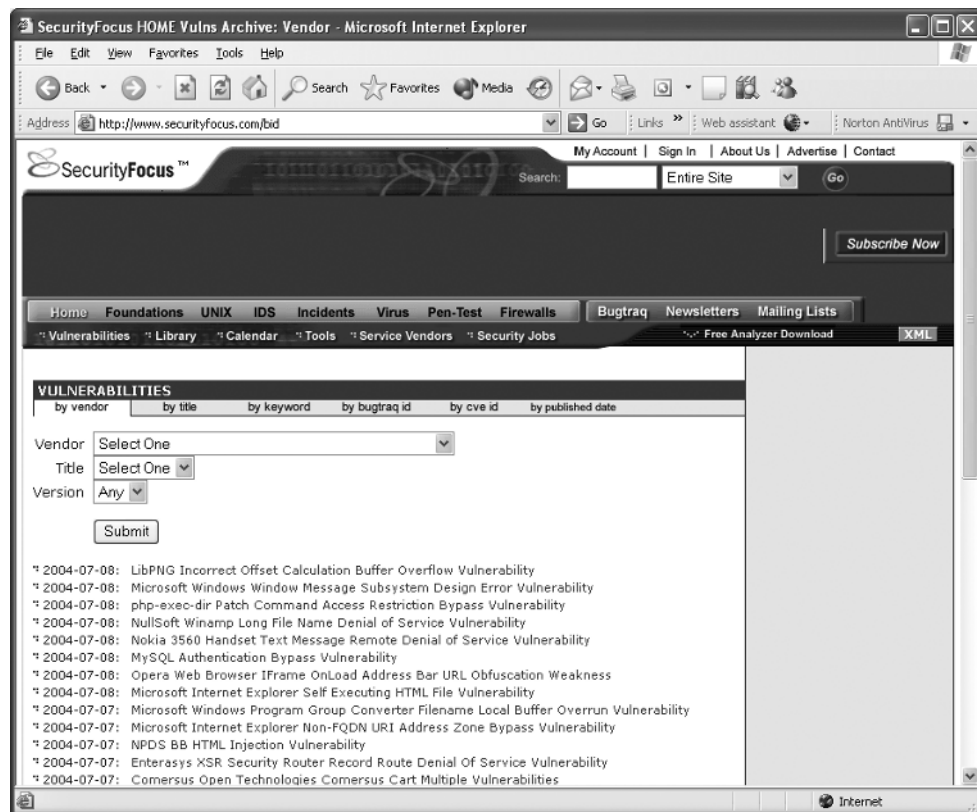
There are many lists that track vulnerabilities, but perhaps the best known and most widely used is the Common Vulnerabilities and Exposures (CVE) list (www.cve.mitre.org) maintained by the Mitre Corporation and funded by the U.S. Department of Homeland Security. This list of vulnerability advisories contains all known vulnerabilities reported to the CVE Editorial Board, a group of representatives from industry organizations that must agree that the vulnerability merits listing on the CVE list.



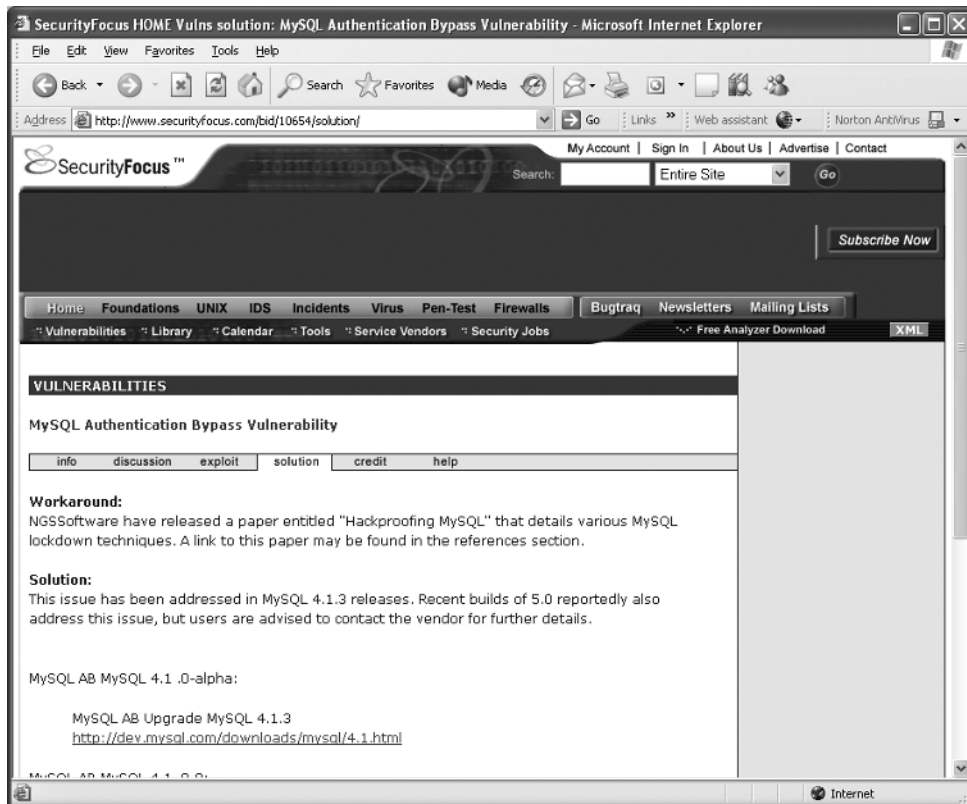
Listed vulnerabilities include a list of references to additional information on the vulnerability. Among these references you will usually find information on how to fix the vulnerability.

Security Focus and the Bugtraq Mailing List

Security Focus maintains an extensive list of known vulnerabilities on their web site (www.securityfocus.com) and distributes notifications of vulnerabilities via their Bugtraq mailing list. This service interfaces with the CVE and assigns CVE numbers to listed bugs and notices when applicable. The online vulnerability database is searchable by product name and is a very good way to locate information about your products.



The Security Focus database also lists the solution for each vulnerability as soon as it is available. The solution will be either information on locking down the application or information on where to obtain a patch for the vulnerability.



Vendor Web Sites

Responsible vendors will make you aware of vulnerabilities and patches on their web sites. The only problem with this is that they will (understandably) not put it on the home page. You will probably have to locate the product support page for your product to find the information you need. You are often better off using a service like Bugtraq and following a link to the vendor's fix from there.

Apply Security Updates for Non-Microsoft Software

Security fixes and updates take on a number of forms. Sometimes it is an executable program. At other times, it will be a configuration change or a single file to download and copy to a specific location. Be sure they come from a reliable source, and scan them for viruses before applying them to your system.

Installation of updates to these applications is no more difficult than installing application updates from the Microsoft Downloads site, you will just have to be certain to read the instructions thoroughly and be sure you understand what they are doing before you attempt to fix the application. If you have any questions, ask the vendor for help installing the update.

Chapter 8

Set Up an Effective Antivirus Solution



How to...

- Distinguish between virus, worm, and Trojan horse attributes
- Evaluate antivirus solutions
- Install and configure an antivirus solution
- Select and use alternative antivirus solutions

Thus far, we have helped you build a network and outfit it with defenses against direct attacks. It is time now to give your network an immune system. Virus-like programs flood the Internet continually, looking for unprotected hosts to infect. Infected hosts become carriers for these digital organisms, further spreading them into corporate networks, private networks, and home networks.

In this chapter we will define virus behavior and help you select the antivirus solution that works best for your home network.

The Role of Antivirus Solutions and Services

From the first computer virus in 1975 to the mass-mailing viruses of today, there has been a game of cat and mouse between virus authors and antivirus vendors. Authors of computer viruses have used techniques ranging from simply writing bits of the virus into program files to creating advanced viruses capable of updating themselves from Internet servers.

Antivirus vendors have not rested either, developing sophisticated methods of detecting and cleaning virus infections. Modern antivirus programs can be described as digital immune systems, capable of adapting to new strains of viruses and defeating them.

Viruses, Worms, and Trojan Horses

In *The Art of War*, Sun Tzu wrote, “Know your enemy...” It is important to know what threats exist in the Internet to know best how to protect your networks and PCs from them. In this section we will describe the traits of viruses and virus-like malicious applications. We will describe the methods each use to infect your computers, and explain why each is a particular threat to your home network. After that, we will show you how to select an antivirus application that will help protect your systems from these threats.

Identify Virus Activity

Computer *viruses* are self-replicating programs that infect programs and files in computers and copy themselves into other files on the host system, thus spreading their infection. They are characterized by the necessity of human action to release their payload. This is accomplished by someone either copying the infected file onto their system, running infected programs, or opening infected documents. Once released, the infection is spread to other files on the computer or e-mailed to other targets using the victim's address book.

Viruses have employed several methods to avoid detection. Early viruses were detected because they modified the beginning of an executable file to include their operating code. Virus scanners were able to detect them by scanning the first few bytes of each program for patterns of known viruses. Virus writers began just adding small hooks into the beginning of programs and inserting the virus code into another part of the program. After this strategy became known, they took to writing viruses that mutated or morphed (polymorphism) into slightly different versions as they spread.

Viruses may carry damaging components called payloads that destroy data, render systems unbootable, or display embarrassing messages to users.

Did you
know?

The First Computer Virus Was Written Almost 30 Years Ago

The first computer virus was developed by a man named John Walker in 1975 as a way to distribute a computer game to UNIVAC computer systems. The virus, named Pervade, copied the Animal game to systems Mr. Walker never intended, with copies even ending up on software distribution tapes for new UNIVAC systems.

The first microcomputer (personal computer) virus was written by a ninth-grader in 1982. The virus, Elk Cloner, would remain in system memory and infect floppy disks inserted into the system. After the fiftieth boot from an infected disk, the virus would display a short poem.

From these beginnings, virus writing escalated to the number one source of computer annoyances before being supplanted in 2003–2004 by unsolicited e-mail (spam).

Identify Worm Activity

Worms differ from viruses in that they spread without human interaction. Using vulnerabilities in applications or operating systems, they spread from system to system, going to work to scan for and infect other systems. Some of the largest global outbreaks have been the result of worm infections.

Some worms carry payloads to damage data on infected systems; others are designed only to spread to other systems.

Identify Trojan Horse Activity

Trojan horses may spread through virus or worm mechanisms and are typically thought of as a particular payload of these pathogens. What characterizes them as Trojan horses is the resemblance they bear to the mythical Trojan horse of Greek legend. Like the Trojan horse, they masquerade as helpful programs or information and act behind the scenes to open back doors into your systems to allow control by hackers.

Other Virus-Like Malware

Often delivered as the payload of a virus or worm, malicious software such as *bot* or *zombie* programs can make your system an unwilling accomplice in international cyber attacks. Major Internet sites have been disabled by these attacks due to the large bot armies that have been amassed by hackers for the purpose of conducting distributed denial of service (DDoS) attacks. (If you missed Chapter 5, a distributed denial of service attack is a mass flood of data directed against a particular host from a large number of zombie systems under the control of a single individual.)

Spyware and *spybots* are a recent development designed to spy on your surfing habits, sometimes even logging keystrokes to expose personal secrets that hackers might find of value. Some also act as spam remailers, using your bandwidth to launch floods of unsolicited e-mail out over the Internet.

Blended Threats

One of the latest developments that has received some press is known as a *blended threat*. This type of attack blends two or more different types of attack into a comprehensive assault on your system. In this scenario, you might encounter a worm or a spybot that installs Trojan horse programs or other malware as an additional payload.

A well-publicized blended threat case is that of the June 2004 release of the Scob worm, which was designed to infect Microsoft web servers with a JavaScript program that would attack Internet Explorer web browsers. Internet Explorer would

be directed to connect to a server in Russia to download the payload, which consisted of a backdoor program that had been modified into a keystroke logger. At periodic intervals, Internet Explorer would be directed to upload the captured keystrokes to web sites in Russia.

How Antivirus Applications Protect Your System

During the 1990s *antivirus* programs had to be constructed to attach to operating systems in an almost parasitic fashion. They hogged resources and often caused as much instability as the viruses themselves. They were processor-intensive, memory-intensive, running on operating systems that were not that stable to begin with (Windows 9x), and when removed, they often left their host system unusable.

As a consequence, many users of antivirus stopped using the real-time protection functions and simply conducted file scans periodically. Some even removed antivirus completely. Often, if you were careful, you could avoid viruses by just being careful.

Now, with blended threat attacks, worm attacks, and attacks coming from compromised web servers, it is more important than ever to protect your system with a comprehensive antivirus solution. With some of these threats gunning for your private data, you can no longer afford the consequences of catching one of these pathogens. More than your data is at stake.

8

File Scanning

The traditional role of antivirus is to locate and disinfect virus-infected files and programs. This still remains a top priority, but it is now only a part of the overall effort required to protect your system.

Infected files are located by two different, but complementary, means: pattern detection and heuristic analysis.

Pattern Detection *Pattern detection* scans a file for known structural traits that act as a signature or pattern by which a virus can be recognized. This can be a file with a specific length, a certain pattern of data within the file, or a specific filename.

Pattern detection is used by all major antivirus suites to detect infected files during virus sweeps. Virus sweeps scan your entire disk or a selected folder for infected files. They can be scheduled or initiated manually.

Heuristic Analysis *Heuristic analysis* is the ability of an antivirus application to monitor the behavior of a program as it is executed. It watches for signs of virus-like behavior, such as attempting to write to restricted portions of the hard disk, or initiation of certain types of communications. When suspicious behavior is detected, an alert is sent to the user that an unknown virus may have been detected.

Symantec's Norton Bloodhound and McAfee ActiveShield are two brand-name examples of heuristic scanning technologies incorporated into antivirus solutions. Other manufacturers, while providing the same services, may choose not to give them a brand name. Look for the keywords "heuristic" and "real-time protection" when you evaluate different antivirus solutions.

E-Mail Scanning

E-mail has been a favorite delivery system for virus writers. Many of the most damaging viruses included the ability to mass-mail themselves to additional victims using your e-mail program's address book. This ability masks the virus by making it appear to come from you and greatly increases the virus' ability to spread when it encounters large address books.

Antivirus vendors apply both file scanning and heuristic analysis to e-mail scanning. In addition, many antivirus vendors are now including antispam capabilities in their antivirus suites.

NOTE

For more on antispam, check out Chapter 9.

Communication Protocol Analysis

By watching for suspicious communication patterns, some antivirus suites recognize and prevent Internet worm attacks. Incorporating personal firewall technology allows antivirus vendors to become one-stop solutions for Trojans, viruses, worms, and spyware. Personal firewalls, discussed in Chapter 5, block communications that do not fit in with typically expected patterns of communication. Many, such as Zone Labs' Zone Alarm, use intrusion detection capabilities to alert you to the fact that a program is attempting to use your Internet connection to communicate with the Internet. Seeing odd program names or communications you do not expect are a sign you may have picked up a Trojan or backdoor program.

Additional Services

Many of the leading Internet protection suites also add features designed to offer additional protection to your systems. Among these are ad blocking, intrusion detection, privacy protection, and child protection or antipornography. We will discuss each in turn and describe how it is used.

Ad Blocking Also called pop-up blocking, ad blocking prevents annoying pop-up ads from appearing on your screen. Besides being an annoyance, many of these ads are the vehicle that carries spyware and other malicious attacks.

Ad-blocking software can range from a program that suppresses all pop-ups to more sophisticated applications that allow certain pop-ups that you can classify as “safe” or “allowed.” Some examples of free ad-blockers are the pop-up blocking capability of the Mozilla Firebird, Opera, and Internet Explorer (with Windows XP Service Pack 2) web browsers, the Google toolbar available from google.com, and STOPzilla from stopzilla.com.

Some of these programs cross over into antispyware as well. STOPzilla includes abilities such as adware blocking, cookie control, and spyware blocking into their product.

Intrusion Detection *Intrusion detection systems* (IDSs) are programs that alert you to attacks in progress and then react to the attacks to protect your systems. Often these programs work in concert with your personal firewall to dynamically block communications from attacking computers. They add an extra measure of protection for your system. IDS programs can be integrated with an antivirus suite, as is the case with Symantec’s Norton Internet Security, or they can be stand-alone, as is the case with free IDS programs such as Snort, AIDE, and Tripwire. The suites are often easier to configure but may lack some of the power of the dedicated applications.

Privacy Protection Programs that stop spyware and manage cookies also fall into the category of privacy protection. We will only introduce these features here, as we have devoted an entire chapter to protecting your privacy. For information on how to protect your credit, your identity, and yourself, check out Chapter 12.

Child Protection There are Internet neighborhoods you just do not want your children exploring. Child safety programs such as Net Nanny and CYBERSitter control the amount of time your children spend online, filter out inappropriate material, and prevent them from giving out private information about themselves. You can get a very good explanation of tools available for this and their features at the Internet Education Foundation’s web site at www.getnetwise.org.

In addition to these dedicated tools, antivirus suite vendors are getting into this area. Symantec’s Norton Internet Security suite offers Parental Control settings for this purpose.

Choose an Antivirus Solution

We have discussed some of the features and capabilities of antivirus applications and suites. In this section we will show you how to select the best package of protection for your system. We will discuss performance ratings and reviews and

Did you
know?

Not All Viruses Survive “In the Wild”

“In the Wild” means the virus has been spotted in distribution on the Internet. The WildList organization (www.wildlist.org) is a group of antivirus researchers that tabulate the occurrence of virus sightings into a list of all viruses known to be active and spreading in the world at one time.

where to locate them. We will also show you how to locate evaluation versions of most popular antivirus applications so that you can try them before you make a final decision.

Antivirus Solution Ratings

Several organizations provide reviews and ratings for antivirus applications and suites. The West Coast Labs, which you can find at <http://find.pcworld.com/43480>, has a system of antivirus product testing called Checkmark. Antivirus products strive to be classified as Checkmark Level 1 (detection) or Checkmark Level 2 (disinfection). These tests determine how good the application is at detecting and disinfecting viruses currently known to be “In the Wild.”

Another organization that tests antivirus products is the ICSA Labs, a division of TruSecure Corporation. In addition to detecting all In the Wild viruses, ICSA tests antivirus applications against their own proprietary library of viruses before issuing certification. Their ratings are also separated into detection and disinfection.

Periodical publications such as *PC World* also publish reviews and ratings frequently, often citing ICSA and Checkmark results. In addition, they will typically mention the additional features of suites, such as antispam or antispyware, in their reviews. These reviews can give you important information on the effectiveness of a product suite in comparison with other suites.

Select the Appropriate Feature Set for Your System

As you zero in on your antivirus solution, you will need to decide which type of product best suits your needs. If you are most concerned about viruses you might receive in e-mail, you may be protected best by an e-mail scanning service such as those offered by Hotmail and Yahoo!. If you are concerned about protecting yourself from viruses in software downloads, you will want a traditional antivirus

application. But if you need firewall protection, protection against spyware or other threats, and content filtering, you might choose to evaluate suites. In this section we will discuss the strengths and weaknesses of each approach.

Best of Breed or Stand-Alone Applications

Single-purpose applications exist because they do one thing and they do it well. In some cases, they will perform that one task better than any other application of that type. This type of application is known as a best-of-breed application.

While it is certainly possible for a suite to include the best available instance of each type of service, it is natural for each suite to have its own strengths and weaknesses. To get around this problem, you might choose to build your own custom suite of best-of-breed applications.

This approach is likely to give you the most comprehensive protection and may be best if you need to travel in bad neighborhoods (digitally speaking), but it also will come at the cost of additional complexity and the chore of maintaining updates on each application separately. This is not an insurmountable task, but still something to consider when selecting your applications. This approach may be best if you only need the features on one or two types of applications.

Antivirus Suites

Antivirus suites, now being called “security suites,” combine several types of protective applications under the banner of one comprehensive suite. Major antivirus vendors offer these suites to enhance the value of their core antivirus products and offer customers a one-stop shop for their digital security.

While they may not be best-of-breed in all aspects of their operation, they will usually provide adequate protection for most Internet users and are an excellent solution for those without the time or skill to maintain a stable of applications. They are an excellent choice for those who are setting up a system for their elderly relation who really wants only to send and receive e-mail and is not likely to know about security patches and updates. Set up Automatic Updates on Windows XP, set up the antivirus suite to retrieve updates automatically, and they will be almost as protected as if you visited the system daily.

Trial Versions

Most antivirus vendors let you test-drive their software with an evaluation version before committing your money to it. This is an excellent idea if you have narrowed the field down to one or two prospects. If you are still working with a long list, try

to avoid this step until you are fairly sure about one or at the most two solutions. Installing and uninstalling antivirus suites runs the risk of introducing instabilities into your system. Some uninstall more cleanly than others, and there are times you might have to reinstall your system if things go wrong on an uninstallation.

NOTE

You can use Windows XP's System Restore utility to remove an antivirus application too, but you must realize that if you do, any other settings you have changed or programs you have added during that period will be gone as well.

If you choose to use a trial version of an application, be sure to install it at a time you will have time to test it out. If you let it sit for 15 days (the typical trial period), you won't have an opportunity to test it, and you will lose any protection it has before you have a chance to fully evaluate it. While you are testing it, obtain antivirus test files and see what type of alerts it gives you. You can download antivirus test files from www.eicar.org. EICAR is the European Institute for Computer Antivirus Research. They provide a test file you can use to test your antivirus scanner. It comes in different versions, an executable, a text file, and two compressed archives to test the ability of your scanner to detect the virus in different mediums. Figure 8-1 shows an antivirus application detecting Eicar hidden in a compressed archive file.

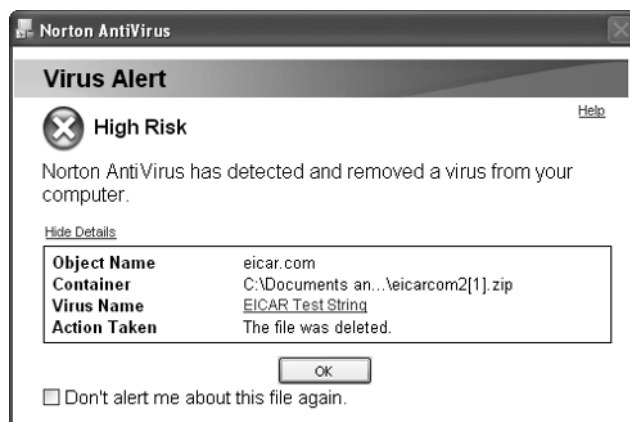


FIGURE 8-1 Norton AntiVirus Detecting Eicar during a test run

How to ...

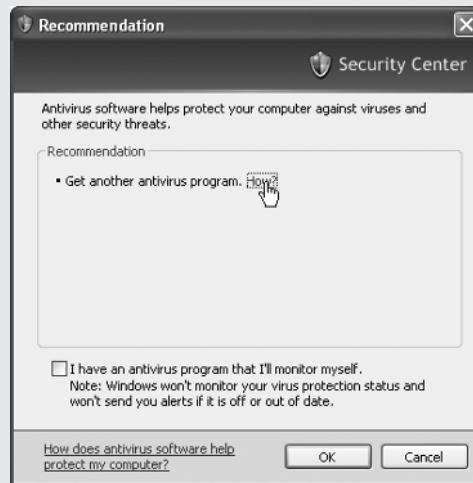
Find Antivirus Vendors' Best Trial Offers

When you launch the Windows XP Security Center in Windows XP Service Pack 2, you will be warned if no antivirus is installed. Security Center will explain that antivirus applications are important for the protection of your system and give you more information about how they help protect your computer.



8

In addition to this warning and explanation, you can obtain additional information on prospective antivirus vendors and even receive some excellent offers for free trial versions. Use the Recommendations button to open the Recommendation dialog box.



Clicking the How? hyperlink in the Recommendation dialog box will launch a Microsoft web page listing antivirus vendors that have made free trial offers for users of Windows XP. Some of these extend for up to a full year. This is a deal you may not be able to find elsewhere, so it is worth checking these offers out.



CAUTION

Installing more than one version of antivirus applications simultaneously is likely to create severe performance problems on your system. These programs access very sensitive system components and do not share with each other very well. If you have finished the evaluation of one and want to try another, uninstall the first completely before installing the second.

Other Antivirus Solution Purchase Options

Occasionally you will be asked to look at a friend's or relative's computer because it is acting strangely. You may suspect virus or worm activity but not want to take the time to install a complete solution. While this is not recommended for long-term operation (each computer you are responsible for should be running desktop antivirus at a minimum), you can conduct scans with free online scanners.

Another level of protection you can investigate is e-mail antivirus subscription services. Most web-based e-mail services offer virus scanning as part of their service. In addition, many Internet service providers offer e-mail antivirus scanning free or for a small monthly fee.

8

Use Online Scanning Tools in a Pinch

Online antivirus scanners are a great resource when you are caught out on the road without antivirus (by now you should know better!) or someone wants you to take a look at their system. Free services such as Trend Micro's HouseCall and McAfee's FreeScan, as shown in Figure 8-2, load a virus scanning tool onto your system to perform a scan. Their disinfection abilities are not as effective as those of dedicated applications, but they are a great way to check a system quickly. If the scan detects a virus, there are often free removal tools available for the virus, or instructions you can use for removal.

Subscription E-Mail Scanning Services

As a service to their customers, many major providers of free e-mail services offer antivirus scanning as part of their service. In addition, those who subscribe to the enhanced versions of these services have the ability to scan outgoing e-mail as well.

Your Internet service provider may also offer antivirus scanning on e-mail services. You might check with them to find out rates and coverage. These services can offer an important second set of eyes looking at your e-mail. Antivirus vendors vary in their speed of providing detection for the latest viruses, and having two sets (especially

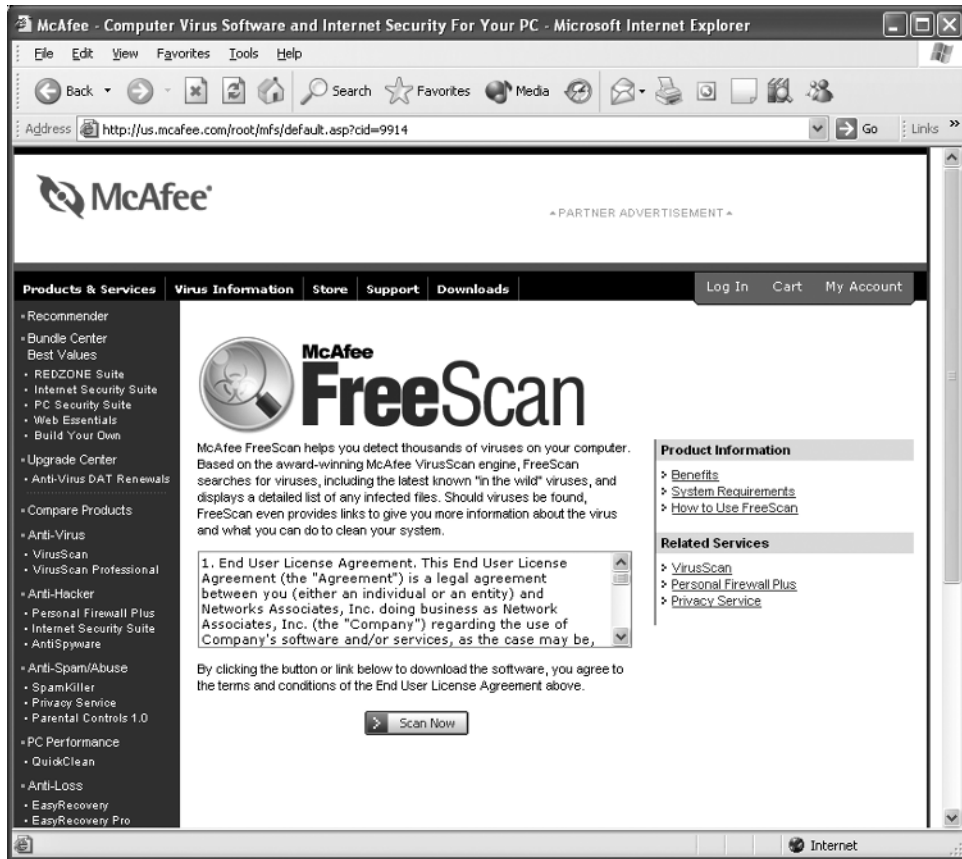


FIGURE 8-2 McAfee's FreeScan

if the two are from different vendors) between you and the bad people doubles your chances of preventing e-mail-borne viruses from affecting your system.

CAUTION

Relying on e-mail scanning alone will not protect your systems against viruses from web sites or attacks from Internet worms. For the most comprehensive protection, you will want to employ the principles of defense in depth, using a personal firewall, antivirus, and possibly antispyware. This will ensure your protection from direct attack, worm attack, and e-mail viruses.

Install and Configure Your Antivirus Application

As you know, selecting your antivirus solution is only the first step to protecting your system from viruses and other malicious software. The antivirus application must be properly installed and maintained to ensure it serves as an effective defense. In this section we will install Symantec's Norton Internet Security, a suite of protection applications from Symantec Corporation. We will install and configure the suite, concentrating on antivirus configuration.

Whether you obtain an antivirus application by purchasing it in a computer store or by downloading it from the vendor's web site, you will be buying a product that is days, even weeks, old. We will show you how to obtain updates, and explain why this update process is the most critical part of your overall protection plan.

Initial Installation

We have chosen Symantec's Norton Internet Security Suite, not as a product endorsement, but as an example of a full product suite with personal firewall, antivirus, privacy protection, and parental controls. There are others—McAfee Internet Security Suite, Trend Micro PC-cillin Internet Security, F-Secure Internet Security 2004—the list goes on. Any suite of this caliber would be an excellent choice for protecting your system, as long as it is well maintained and updates are applied consistently. During this installation we will pay attention to features such as real-time protection, manual scans, and scheduled scans that are part of every suite.

The steps for installing an antivirus suite are very similar from one product to the next:

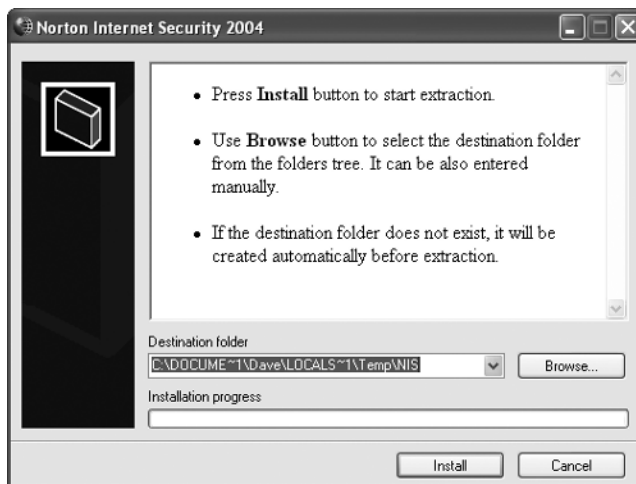
1. Execute the installation program.
2. Choose the appropriate installation options.
3. Configure real-time and scheduled scans.
4. Update application and detection signatures as soon as possible.

Installation

Whether downloaded from the Symantec web site or installed from CD-ROM, installation of Norton Internet Security follows a similar path. The principle difference is that the downloaded version will have to be unpacked first.

Unpacking the Downloaded Installation Files If you have downloaded the installation files, you may have to extract them to a folder on your system. This procedure usually progresses quickly and is fairly straightforward.

1. Executing the downloaded file is usually enough to begin the unpack process. You may receive a confirmation dialog similar to the following to allow you to choose a folder to unpack the installation files into:



2. Windows XP Service Pack 2 affords the ability to monitor executables for digital signatures that will prove the application is created by the party who signed it. If you execute the downloaded version of an antivirus application, you may see a confirmation dialog similar to the following:



3. After verifying the source you obtained the file from is reputable (you may have to take their word for it), you may continue the installation by clicking Run.
4. You may wish to control the location the installation files are unpacked to. If so, browse to a location on your system and create a folder for the files.



5. After you select the folder, the unpacking process will begin.

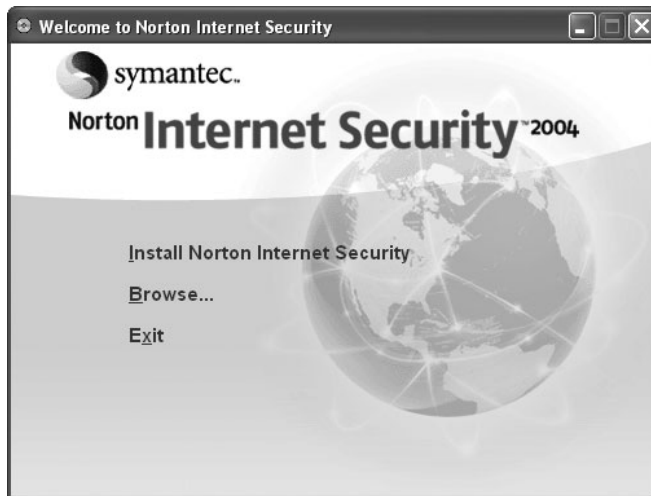


TIP

With Norton Internet Security Suite, you can copy the installation files to a CD-R/RW or DVD-R/RW disc at this point to have a backup copy in case you ever need to reinstall the application. Other suites may unzip their files in this way, may offer a backup CD, or may allow extended periods (up to a year) for downloading the installation files for future installations.

Beginning the Installation After the completion of the unpacking process, the installation application will appear. From this point onward, the installation process proceeds the same for both downloaded and CD-ROM-based installation programs.

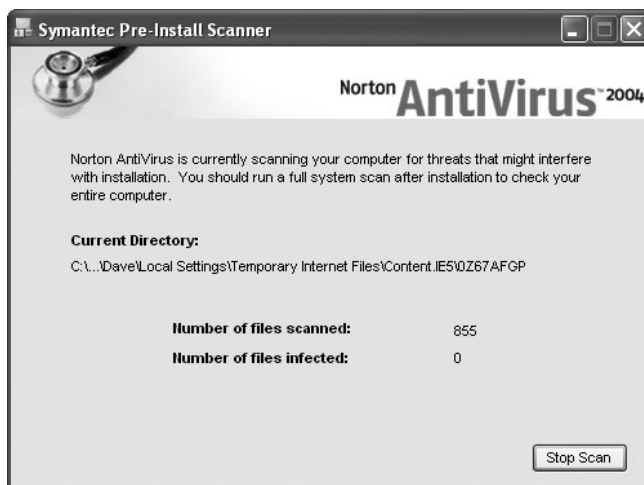
1. Begin the installation by clicking the Install choice. For products other than Norton Internet Security, this may simply be the next step in the installation wizard, but it should be readily apparent at this point.



2. Norton AntiVirus offers to conduct a pre-install scan for viruses. Other suites may do this as well, or they may initiate a scan as soon as they are installed.



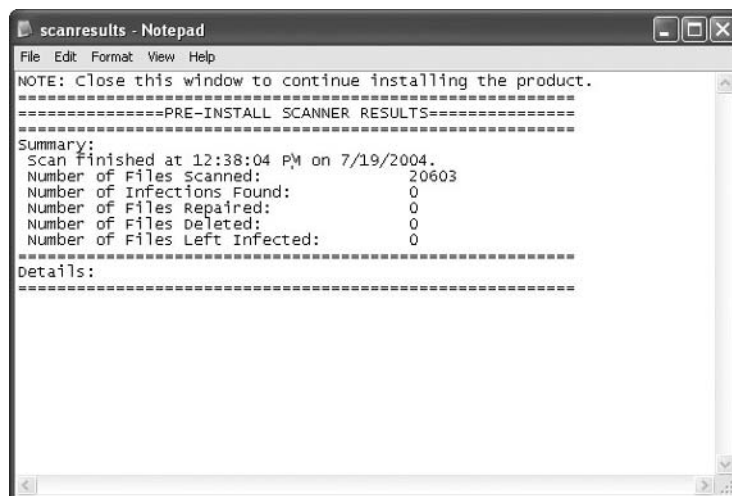
3. This is a very good option and ensures the application is not installed over any virus infections, making them harder to remove. Click Yes to begin the scan.

**NOTE**

The pre-install scan will detect only viruses known at the time the installation package was assembled. It could miss any viruses released after the packaging date, so it should not be relied on as a clean bill of health. After the installation, we will download the latest detections and perform another scan.

8

4. After the pre-install scan completes, you will be presented with the results of the scan.



5. After viewing the results, you may continue the installation (in this case, by closing the results file).
6. Now we are entering the installation program itself. You will typically progress through an installation wizard.



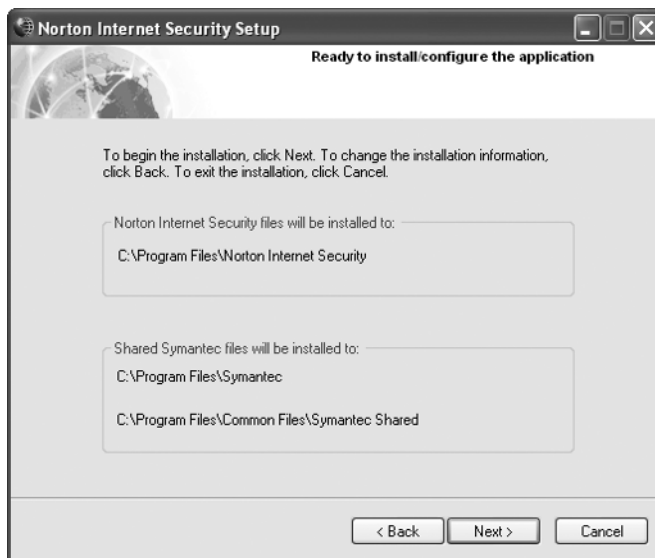
7. During the course of the installation wizard, you will accept the end user licensing agreement. Please read this carefully. It details acceptable use of the program and outlines your rights (as the software publisher sees them).



8. Next, you will typically be offered the opportunity to select which components of the software you wish to install. The default setting is selected by the software provider to give the best performance and protection. We will choose this option.

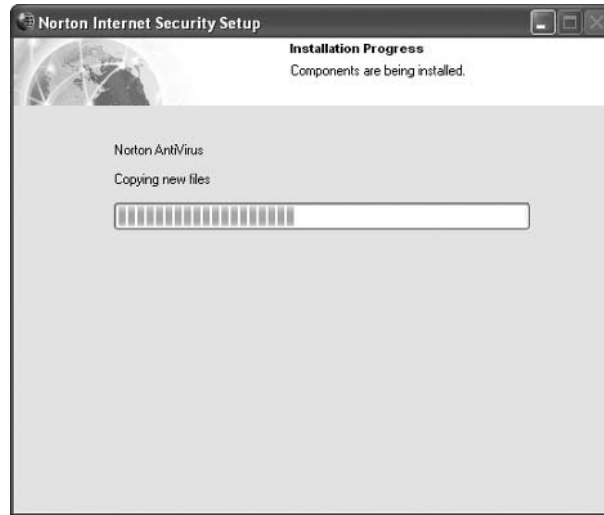


9. Typically, you will be given one last opportunity to back out before the installation wizard begins to copy files to your system. Click Next.

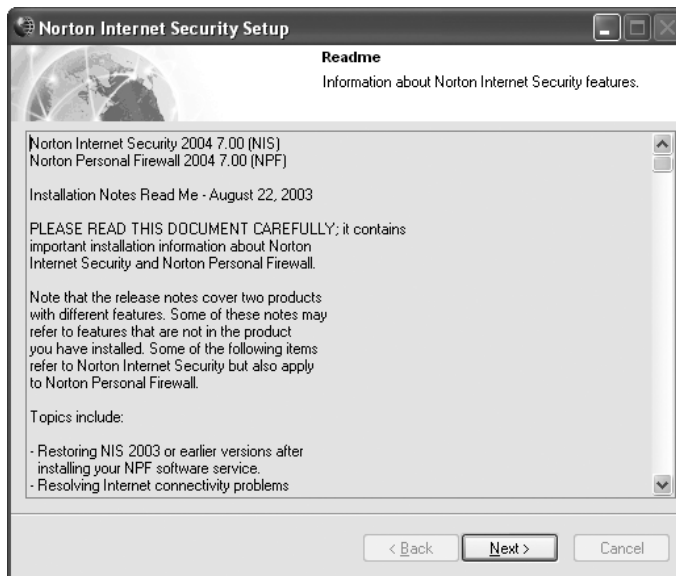


Completing the Installation You have reached the phase where the installation program will begin to make changes to your system.

1. The installation program will copy files and begin to set up the applications.



2. After the installation is completed, you may be presented with a lengthy text document called “read me notes.”



NOTE

Often you can find these “read me notes” on the disk somewhere, but it is a good idea to print them at this time. If you do not see a print button on the dialog box, use your mouse to select all the text and press CTRL-C to copy it to your system’s clipboard. You can then paste it into a blank document and print it from there. In the case of Norton Internet Security, this printout presents details about troubleshooting Internet connectivity, troubleshooting compatibility problems, and other late-breaking information about the applications. Take time to read this document, as there is often information here that will save you time later.

3. After viewing the “read me” notes, you will see the success message. It will usually offer to restart your computer. Make sure you are not running any other applications, and then accept this option, as your system is usually in a vulnerable state at this time and will take a restart to put the final pieces in place for proper operation. Skipping the restart at this time may lead to instability or a corrupt installation.

8

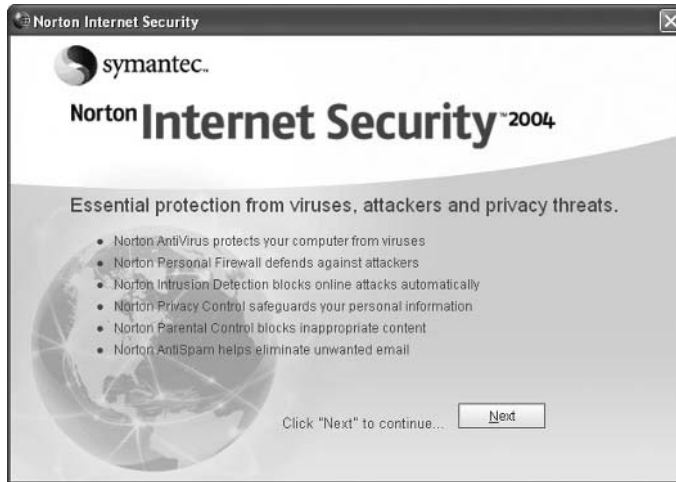


Application Configuration

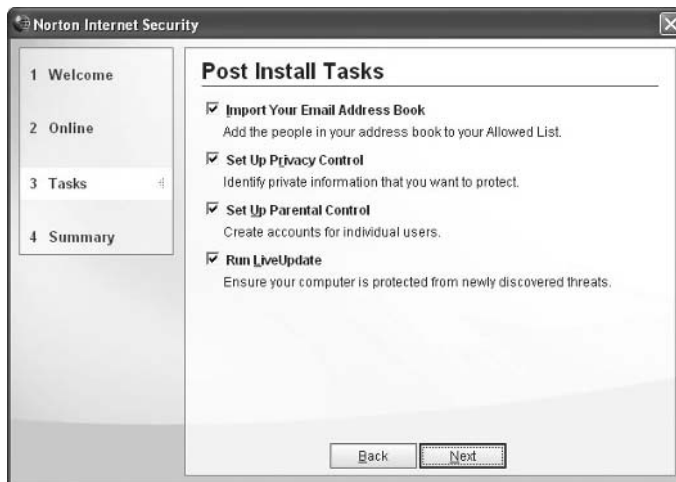
After restarting your system following the installation of antivirus, you will usually be presented with a configuration wizard to help you properly configure the

application. As you step through this process, watch for items we will discuss in this section.

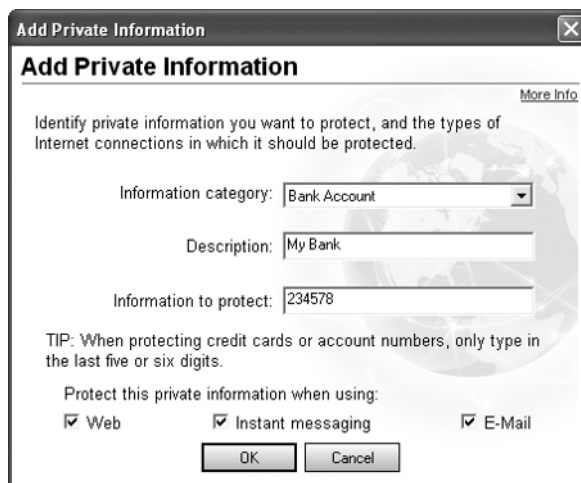
1. As you have probably noticed by now, Windows application installation wizards almost always begin with a welcome page. Having a trouble-free first step always boosts the installer's confidence. Click Next.



2. Norton Internet Security displays a checklist before beginning the configuration process. You can choose which components you wish to configure at this time. Unless you really need to get antivirus on immediately, you should perform the initial configuration steps outlined in this wizard.



3. Internet Security sets up privacy features and antispam features before launching LiveUpdate. Privacy Guard protects sensitive information from being transmitted. To accomplish this, you enter the protected account information you do not wish to have sent out.



8

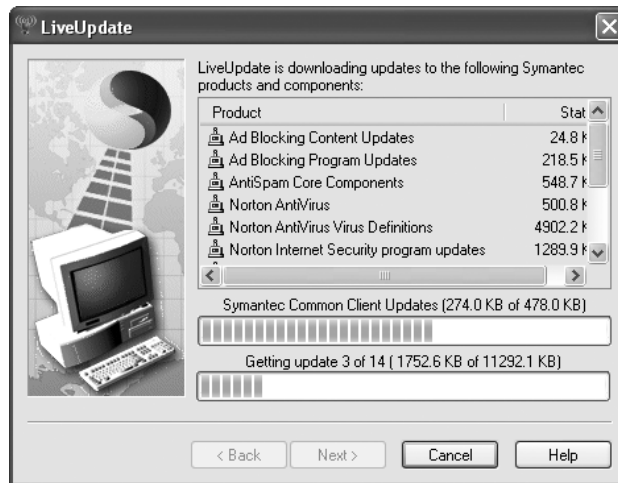
4. After you set up privacy and parental controls, LiveUpdate will be launched. Clicking Next begins a scan for updates to the Internet Security Suite.

NOTE

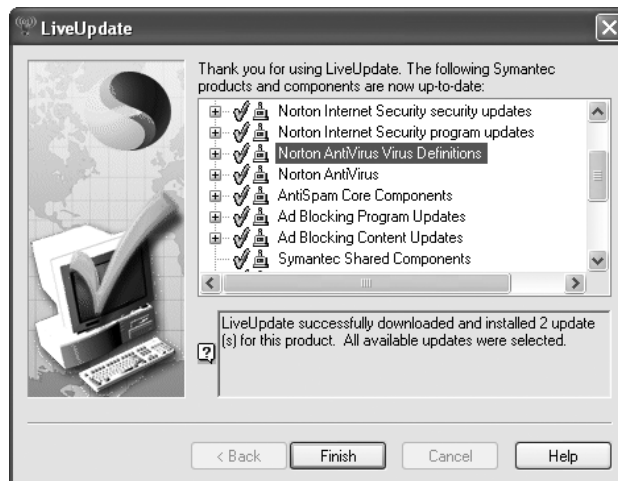
LiveUpdate is Norton's method of automatically updating the applications and virus signature files. Other suites will have automatic updates as well, but they will have other names for them.



5. After determining which updates are required, you can click Next to begin the download. This would be a good time for coffee if you aren't lucky enough to be downloading over a broadband DSL or cable connection!



6. The installation process begins as soon as the updates are downloaded. When this is completed, verify everything installed successfully. If there were any problems, complete the wizard and restart your computer. Run LiveUpdate again to retry the update.

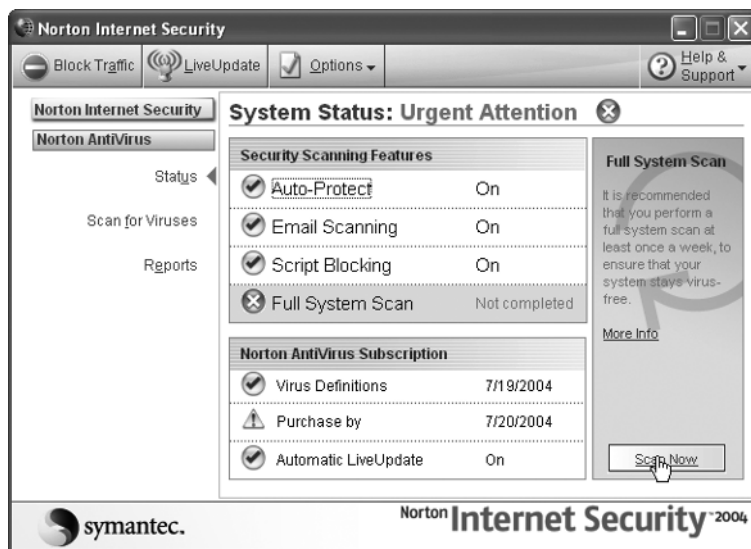


7. After the LiveUpdate process is completed, you will be asked to restart your computer. Restarting will allow live components such as real-time scanning services to be updated and to be restarted properly.
8. After the restart, components like the personal firewall begin to pop up notices. At first this may be annoyingly frequent, but they will quickly slow down as the applications learn about your system.

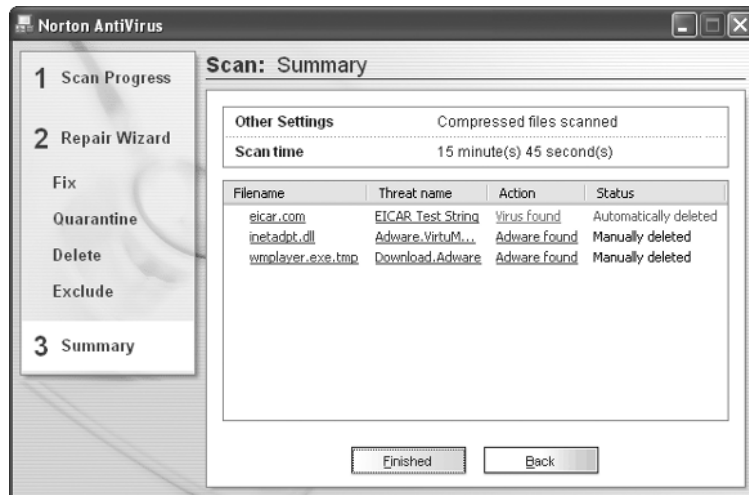


8

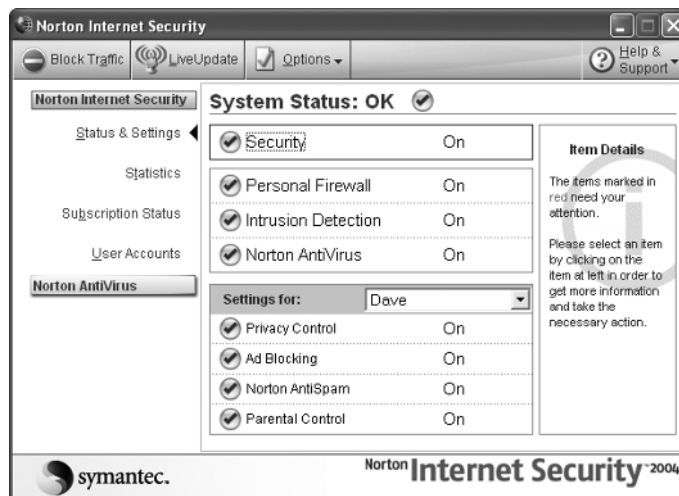
9. Launching Internet Security again displays the status of all components. We can see that Norton AntiVirus is unhappy. We need to conduct a full virus scan to change Norton to a happy green.



10. After the scan, you can get a summary of viruses and other malware detected.



11. After the virus scan, everything is satisfied, and Norton Internet Security gives you a System Status: OK.



Application Updates By default, Norton LiveUpdate checks for updates when you start your system and every four hours thereafter. If you feel the need to force an update (you have heard of a brand-new threat), you may click the LiveUpdate button on the main menu to launch the LiveUpdate scan.

You can select which components LiveUpdate will verify by choosing Norton Internet Security options from the Options menu and selecting the LiveUpdate tab (see Figure 8-3).

Real-Time Protection Real-time scanning options are configured in the Norton AntiVirus options available on the Options menu. You can enable or disable AutoProtect and configure how it responds to a virus detection (see Figure 8-4).

NOTE

Disabling real-time protection is not usually advised, but there are times when you might want to do this. Disk-intensive tasks such as defragmenting, backup, and text searches for files may be slowed by the real-time scans. If you aren't actively working with documents from the Internet, you can safely disable it during one of these processes. Just be sure to enable it when you are done.

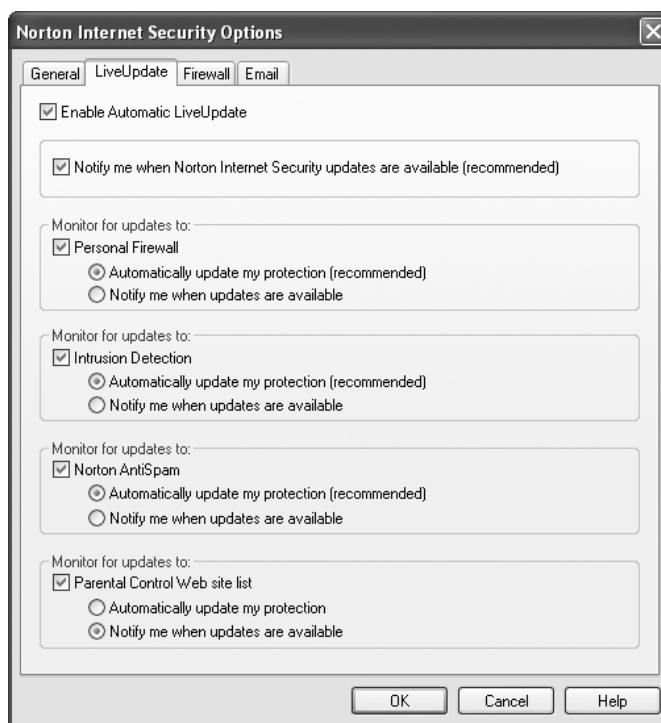


FIGURE 8-3 Configuring LiveUpdate Settings

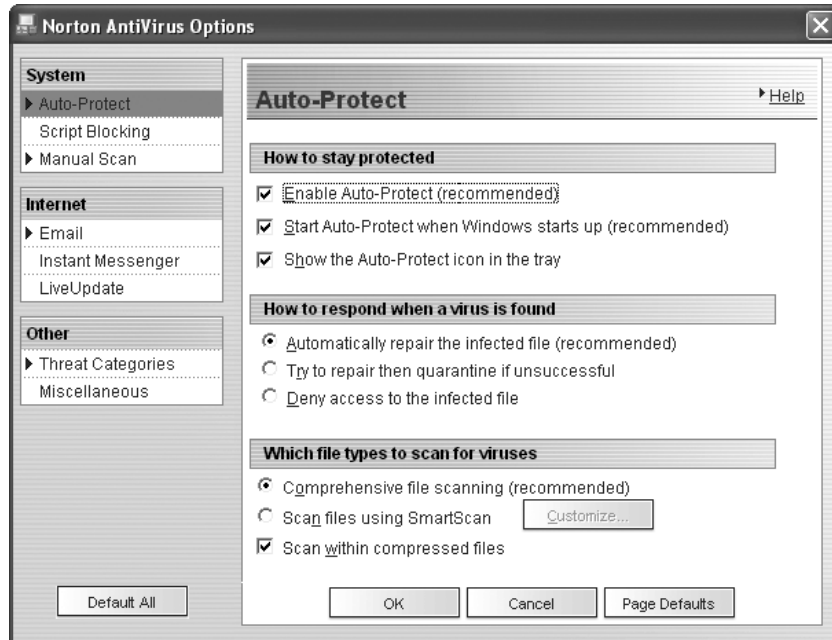


FIGURE 8-4 Configuring Real-Time scanning options

Scheduled Scans You may also schedule scans in the Scan For Viruses section of Norton AntiVirus, as shown in Figure 8-5. Schedule scans for periods when your system will be turned on but not likely to be in use.

NOTE

While the different antivirus applications differ in their implementation (and naming) of important features, look for common aspects in the configuration of the application you choose. It will all begin to make sense when broken down into components. Look for real-time protection settings, update settings, detection settings, and scheduled scan settings. If you are looking for the individual components, rather than just browsing the menus, they will be much easier to find.

Do not hesitate to call the support line for the solution you choose. You have chosen an important piece of software and deserve the full attention of a competent support professional if you have any questions or concerns.

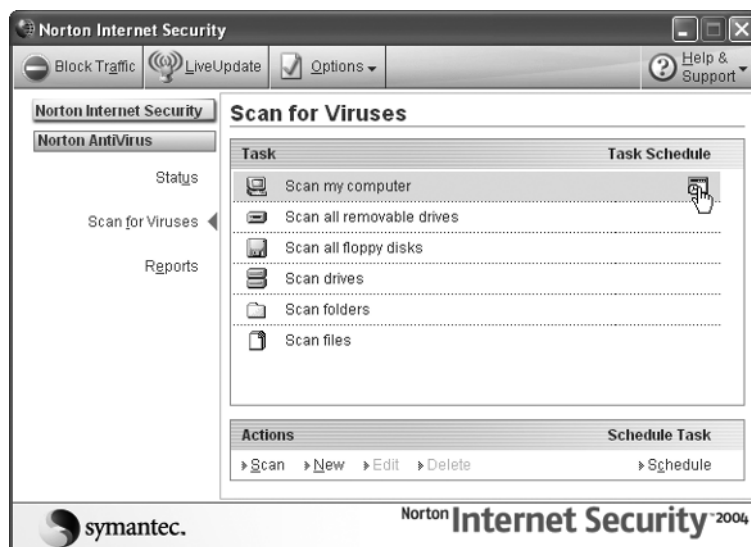


FIGURE 8-5 Creating a scheduled virus scan

Operate and Maintain Your Antivirus Solution

Beyond the initial configuration of your antivirus solution, and monitoring automatic updates, there is very little day-to-day maintenance involved to maintain your protection. The antivirus application should download updates automatically and will notify you if your computer must be restarted. Application updates will arrive in the same way, updating one component at a time to keep your protection up-to-date.

There are some actions you should take when you become aware of a new threat. We will discuss them in this section and finish with a few tips on handling virus detections.

Perform Manual Virus Sweeps When You Suspect Malicious Activity

Your system is doing something odd. No problem; it's Windows. It does weird stuff all the time, right? Well, not always.

With frequent usage, you come to know what behavior is out of the ordinary. If your system is suddenly slower than normal, or begins to restart spontaneously, update your antivirus signature files and start a manual scan. It takes only about 20 minutes and could stop a virus before it does real damage.

React to Virus Outbreaks with Manual Updates

You hear about a news report of a new virus that is sweeping the world. It has infected the systems of thousands of unsuspecting Internet users. You have a moment of concern about your system at home. You know it's online. Is it safe?

Well, if you follow the advice we have given in this book, your home system will be less vulnerable than most.

Your Internet gateway and personal firewall should protect you from direct assault, Automatic Updates and application patching should have eliminated any vulnerability in your operating system and applications, and you will update your antivirus signature files as soon as you get home. Right?

Well, it may not be quite as easy as all that. After a new virus is detected, it takes some time to update your applications. The antivirus vendor must first develop new detection signatures, and then you must receive them and apply them to your system.

If it takes the vendor 12 hours to get a new signature file out and everyone and his sister is downloading it, you may not receive this file until almost a day after the initial outbreak. In virus time, 24 hours is an epoch. This is where our defense-in-depth training comes into play. Hopefully, your efforts to apply patches will have eliminated any vulnerability the virus or worm uses to get a toehold into your system. In addition to that, a personal firewall and your continued vigilance should fill in your defenses. You should be especially skeptical of any e-mails during this period.

If necessary, wait until you receive your antivirus update before reading your e-mail or browsing any but the most trusted web sites. Know your enemy. Read up on the virus's infection method. If necessary, take any steps recommended by security sites such as SecurityFocus or antivirus vendors' web sites.

When an update is available, download it and run a manual scan on your system.

What to Do When You Find a Live Virus

You are downloading the latest version of a free game where you smash acorns with a halibut or something. Suddenly, a message pops up that looks like Figure 8-6.

Well, forget about acorns, you now have a bigger nut to crack. Read the message carefully. Note carefully the action that was taken. Often this means the virus is copied to a quarantine folder in your system. If you have no need to play with the virus, leave it alone. The quarantine folder is managed by the antivirus application, and it should be safe in there.

If you are concerned, update your signature files and perform a manual scan. Then look for another game to play.

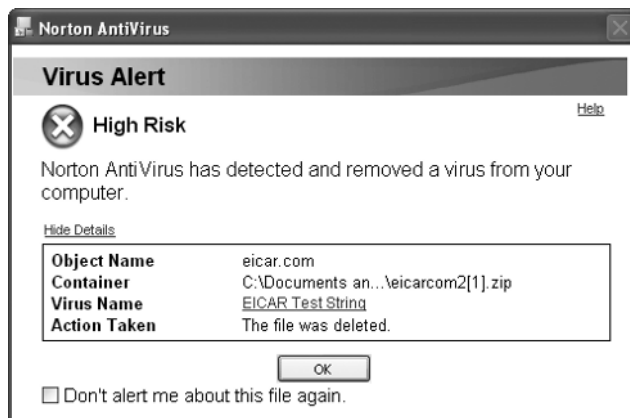


FIGURE 8-6 Norton AntiVirus detecting a virus in a download file

What to Do When You Suspect a Virus

While opening a Microsoft Excel worksheet, you are informed that it contains macros. You did not record any macros in the file, so you decide to scan it for a virus.

First, update your pattern files. Then, right-click the file and select the option to scan it for a virus. This may be worded differently, depending on your antivirus vendor, but should be available with a right-click. If it does not detect a virus, send the file to your antivirus vendor for analysis. This is how they find out about new viruses, and it is just possible you are one of the first to see it.

Each antivirus vendor has a slightly different way of receiving virus submissions. Look under Help in your antivirus application for information on submitting viruses for analysis, or go to their web site and look for a submission link. Wait for them to respond to your submission before opening the file. If there is no virus, they will tell you so, and they may work with you to verify there is no macro.

This page intentionally left blank

Part III

Communicate Securely



This page intentionally left blank

Chapter 9

Fight the Junk E-Mail Plague



How to...

- Cut down the spam you're already getting
- Prevent spammers from getting your address
- Develop e-mail habits that will protect your address
- Learn how to use spam filtering applications on your PC
- Stop spam closer to the source
- Avoid future spam problems before they affect you

Put an End to Your Spam Problem

Spam, sometimes called unsolicited commercial e-mail, bulk e-mail, or just plain old junk mail, has been around for quite a bit longer than many folks realize. Spam—the unwanted e-mail that clogs our inboxes with advertising and tries our patience—actually dates back to the earliest days of the Internet, before there was a World Wide Web, when the entire network consisted of only a few hundred computers distributed among universities, research firms, and parts of the Department of Defense. On May 3, 1978, Gary Thuerk, a salesman for mainframe maker Digital Equipment Corporation, invited all 594 people on the Internet to a product demonstration. It caused an uproar at the time, and it's only gone downhill since then.

Today, with millions of people on the Internet sending billions of e-mail messages a day, it's hard to believe how bad the spam problem has become. MessageLabs, a large spam filtering service used by Internet service providers (ISPs), has estimated that spam made up more than two-thirds of the entire e-mail volume worldwide in mid-2004, and that it will probably hit the 75 percent mark by the beginning of 2005. MSN Hotmail, for instance, receives more than two *billion* spam messages each and every day, targeted at the users of its free e-mail service.

Defend Your Inbox, Lest You Drown in Spam

Spam's inauspicious beginnings have led to one of the biggest “arms races” in the history of computing. As spam-fighters learn new techniques and devise new tactics to combat the menace, spammers (the folks responsible for sending the junk) develop new tools to defeat the antispam crowd using ever-increasing technological sophistication. For every advance the spam filter companies make, spammers always seem to figure out a new way to work around them.

Where they once needed long lists of working e-mail addresses, spammers no longer need to even know the e-mail addresses of their victims before they strike. With increasing frequency, spammers are turning to highly advanced, automated tools that take advantage of the legitimate functioning of e-mail servers in order to deduce real e-mail addresses. If you don't get spam at an e-mail address that isn't protected with some form of spam filter, it's only a matter of time before you do—it's as simple as that.

That's why it's so important to learn how to take advantage of spam filters. Spam filtering tools have become, without a doubt, an indispensable tool for virtually every computer user. Later in this chapter, we'll introduce you to two of the best filters, and we'll show you how to use them to your greatest benefit.

Fight Spam on Your Terms, on Your Turf

Nobody except a spammer loves spam. If you're frustrated with spam, you're not alone. Fortunately, some very bright minds are working on solving the spam problem—after all, they're getting spammed, too.

The first step to cut your spam is to understand how spammers get your e-mail address in the first place, and then to avoid taking part in activities that may reveal your real e-mail address (such as using chat rooms on AOL, or posting messages to Usenet newsgroups) in such a way. This will keep the spammers from *harvesting* your e-mail address(es). For situations where you won't need to maintain contact for long, you can use free services like the Mailinator (www.mailinator.com) or SneakEmail (www.sneakemail.com) to create addresses you can simply throw away after one or a few uses.

But engaging in safe computing practices won't protect you. Even if you do everything right, spammers have other ways to discover your e-mail address. As a result, every e-mail address, no matter how well protected, will eventually get spammed.

Short of trashing your existing e-mail account and creating a completely new e-mail address for yourself, only *filtering* spam can rid your inbox of much of the spam you already receive. Fortunately, you can use any of a number of very good spam filtering tools—some that you run on your PC, others that your ISP provides—that will cut your spam intake down to nearly nil.

Avoid Getting Spam in the First Place

Before you worry about spam filters, take a moment for some self reflection. How, to whom, and under what circumstances you divulge your e-mail addresses to others directly affects how much spam you're likely to receive. Certain kinds of behaviors

can lead you to getting more spam; developing good habits can cut a large percentage of your spam load. And if an e-mail address becomes inundated with spam beyond your capacity to care about the address anymore, you can just ditch it and create another.

Develop Habits That Will Protect Your E-Mail Address

Some people give their e-mail address out to anyone and everyone. They fill it in on sweepstakes entry forms and sign up for information from companies. Others keep their e-mail address close to their chest, only giving it out to colleagues or family. Can you guess which kind of person gets more spam?

We've discussed how certain kinds of behaviors can bring more spam to your e-mail accounts. Here are several habits and practices that will help you moderate the amount of spam you're likely to get.

- **Rarely give out your e-mail address** If you have a choice, don't divulge any e-mail address you want to keep spam-free to anyone you don't personally know, to any company, or to any Web site for the purposes of "registration"—meaning, any time you fill out a form (either on paper or on a Web page).
- **Keep your system patched** Spammers have begun to employ some of the same tools that virus writers use, building worms that sneak onto insecure computers to steal the list of e-mail addresses from the address books of unsuspecting users. Keeping up to date with critical system patches can also protect your e-mail.
- **Read Web site privacy policies** If you are in the process of buying something online, stop before you fill out any form, and read the company's privacy policy. Don't assume that the existence of a policy means "we'll protect your privacy." The policy might say "if you give us your e-mail address, we'll spam you to high heaven."
- **Consider the value of your time** As an example, let's say online pet supply store #1 has the rabbit food you need for \$5 less than online pet supply store #2. In order to buy the rabbit food, you have to fill out an order form and provide a real e-mail address. But the privacy policy for store #1 says that they will sell your e-mail and postal mailing address to lots of their "partners," which usually means that you'll get a lot of spam, as well as "real" junk mail from the postman. If that one-time savings of \$5 will result in half an hour of dealing with spam every day from then on, ask yourself: Is it worth it?

- **See if you can fake it** Don't let a Web site bully you into giving them your real e-mail address, especially if you never want to, or need to, get an e-mail message from the owner of the site. (The one exception here is when you sign up for a message board or private site where the site will e-mail a password to you—those sites will need a real address.) Most Web sites won't be able to tell the difference if you put a fake e-mail address into a form, as long as there's an @ sign in there somewhere, and a ".com" at the end.
- **If you must divulge a valid e-mail address, use a throwaway** Just because a form or a Web site asks for your e-mail address, it doesn't mean you have to give them the keys to your e-mail kingdom. Create one, or several, disposable e-mail addresses (you can start with a free Web mail service, like Yahoo or Hotmail) that you use only when you register for Web sites. Use the address once, to get the password, and then ditch the account. Advanced users may prefer the Mailinator (www.mailinator.com) or SneakEmail (www.sneakemail.com) for their disposable address needs.
- **Make your address hard to screen-scrape** Spammers sometimes use automated tools that scour the contents of Web pages looking for anything with an @ sign—a process called *screen scraping*. If you insist on posting your primary e-mail address, try using words instead of the normal punctuation marks in your e-mail address. For example, joe_blow@amishrabbit.com becomes joe *underscore* blow *at* amishrabbit *dot* com. You could also add an obvious "remove me" message to the e-mail address itself (like joe_blow@amishrabbit.IREALLYDONTLIKESPAMcom). Humans will be able to see what they need to do immediately, but automated screen scraping tools will probably just add the address in its entirety, junk text and all.

Skip Online Activities That Make You More Likely to Get Spam

Certain kinds of things you can do online make it more likely that you'll get spammed. In many cases, however, you can still engage in these activities and prevent spammers from harvesting your e-mail address. Here's our list of antis spam don'ts:

- **Don't use your primary "screen name" for e-mail on AOL** Even with AOL's highly touted spam filters, you can expect to get lots of spam in the e-mail box for the screen name you use most frequently. In AOL, you can't change your main screen name—the one you use to log into the service—without dumping the other screen names you use on your account. But

you can create a number of other screen names for e-mail. So, just do that instead, and leave your primary screen name alone.

- **Don't use just letters in the first part of your e-mail address** It's strange but true: E-mail addresses with one or more numbers in the part that comes before the @ sign, sp1ke@amishrabbit.com, for example, get less spam overall and are less likely to get spammed in the first place, than addresses that are composed of letters alone. Creating an e-mail address with a number in it doesn't guarantee you'll never get spam—it just means the spammers won't be as likely to try out the address.
- **Use a free Web mail address if you post to Usenet newsgroups** Usenet, the world's largest and most diverse message board, is archived by Google under the name Google Groups (groups.google.com). Any message posted to any Usenet newsgroup since Usenet was created 30 years ago will be archived here, along with the e-mail addresses of the message posters. Spammers know this and regularly screen-scrape Usenet to get new target addresses. Don't be one of their victims!

Ditch Your Extremely Spammy Identity

In a worst-case scenario, when the spammers really get your e-mail address in their sights and just won't relent, you may have no choice but to completely stop using a particular e-mail address in order to cut your spam load. While this is probably the least desirable option for most people, changing an e-mail address is the quickest way to start with a clean (and spam-free) slate. The older your e-mail address, the more likely that the address is on the mailing lists of a whole slew of spammers.

Fortunately, many ISPs make dumping an e-mail address a snap. Many ISPs will give you the ability to create anywhere from two to five additional e-mail addresses, and will help you migrate from using your old address to a new one.

Filter Spam on Your PC

Spam filtering software you run on your computer is one of the hottest fields for technological innovation at the moment. These programs use a complex set of rules and filters to sort through mail in your inbox, removing the spam while leaving the “good” e-mail messages behind. For most people, running spam filter software is the most effective way of ridding your e-mail of unwanted junk, and the process adds only a few extra seconds to the time it takes you to download the e-mail.

Try the Software That's Free, or That You've Already Got

Outlook and Outlook Express both have a mail filtering system built in. Despite that, many people opt to augment or improve this feature with spam filtering software. You can try it out for yourself before opting to add additional software, but we're pretty certain you'll want something more than it can offer. In addition, filters can help you more easily separate your desired mail from spam.

Outlook Express delivers the most rudimentary of filters: you manually program each one. The filters check each incoming piece of mail against a set of *rules* you program that determine a response. For example, if your friend makes really good pies, you might want to give a high priority to any messages with his name and the word "pie" in them. Outlook Express' *message rules* mechanism lets you do this.

To create a new rule, click Tools | Message Rules | Mail, and then click the New button (see Figure 9-1).

Alternatively, you could select a message typical of the one you want to filter, and click Message | Create Rule From Message. In so doing, the message rule OE creates is filled out in advance with the From: address of the e-mail message you select (see Figure 9-2).

9

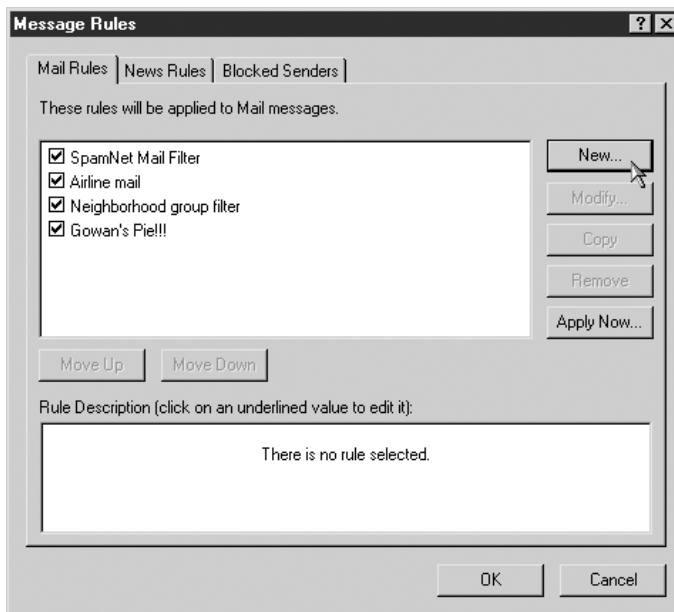


FIGURE 9-1 Manage filtering rules in Outlook Express' Message Rules window.

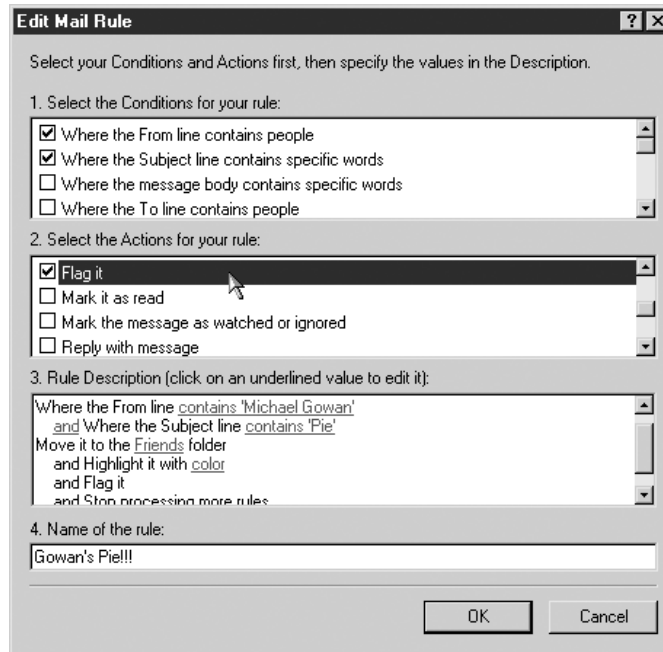


FIGURE 9-2 Pre-fill a message rule with the message's From: address.

Just as you can add additional rules to specify under what circumstances the program should do certain things, you can add and customize *rule actions* to take action when a rule is (or isn't) followed (see Figure 9-3). Anything you can do to a message manually—highlight it, delete it, move or copy it to different folders, send a reply, or forward it elsewhere—you can turn into a message rule action.

One important thing to keep in mind while using message rules is this: If a message contains elements that apply to two or more rules, the actions each rule takes can interfere with the others. But they won't do that if you set one additional action in a rule. Unless you have a specific reason for a message to have two (or more) rules take actions on it, fill in the check box next to Stop Processing More Rules when you're scrolling down the Actions box (see Figure 9-4). If you do that, OE won't apply any other rules against messages that “set off” the rule you just made. Click OK when you're done.

However, spammers constantly change the words (and the creative spelling of the words) they use in the body or subject line. So your preprogrammed spam filter may catch *Cialis* but not *Cialis* (with a numeral 1 instead of a lowercase l). Outlook Express' filter is just too literal.

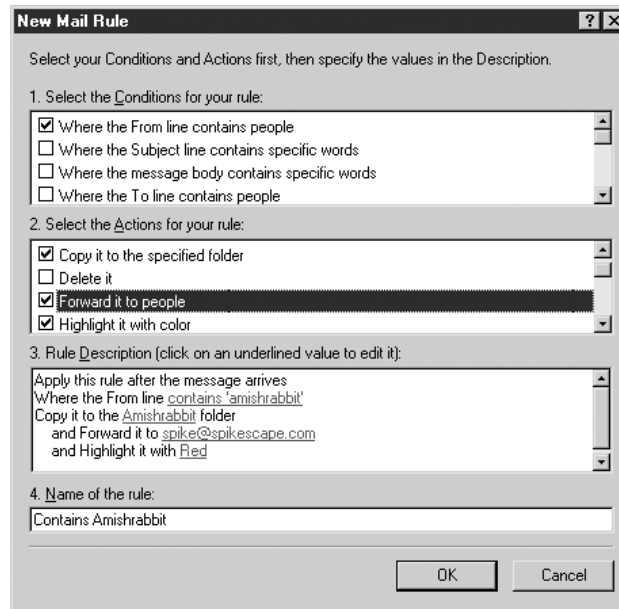


FIGURE 9-3 Customize rule actions to automate tasks.

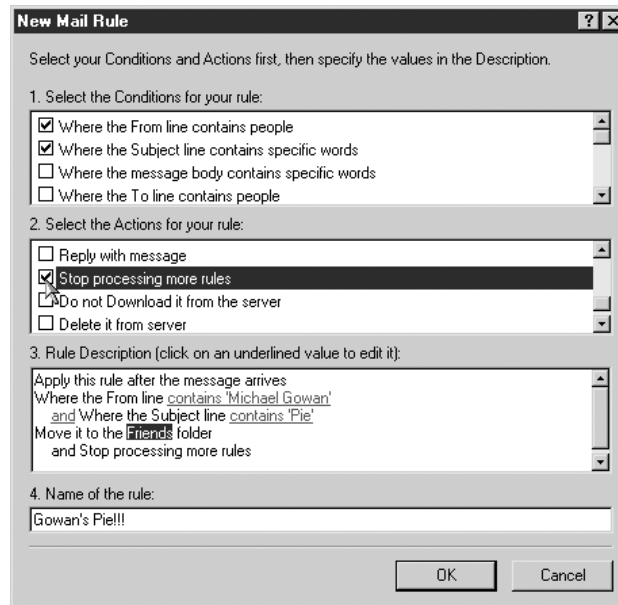


FIGURE 9-4 Tell OE to stop applying other rules if this one is applied.

The same can't be said for the filter built in to Microsoft Outlook 2003 and XP. Outlook sports a more robust antispam technology, accessible through its Program Settings menu. But in our experience, Outlook's spam filter, while better than nothing, still allows a lot of spam to slip through into your inbox (spam filter users call these spam messages that don't get filtered *false negatives*), and occasionally filters a legitimate message as spam (which is called a *false positive*). Both kinds of mistakes are common, though false positives can be more troublesome if, for example, you never see an important e-mail because it got bumped into your spam folder, where you might not look for it.

Shop Around for a Good Spam Filter

At last count, we found more than 120 spam filtering applications available for Windows computer users. They vary greatly in levels of sophistication, effectiveness, and ease of use. Some won't cost you anything, though most spam filter makers either charge a monthly fee to use their product (such as SpamNet, covered later in this chapter) or sell their software for a fixed price. We'll show you how to choose the best one for you, and how to get started with a couple of decent spam filtering applications.

What to Look for in a Spam Filter Application

When shopping around, ask about (or look for) the following features:

- **How often does the program update itself?** Spam messages change literally from minute to minute, and filters—the rules that govern how the filter software determines whether a message is spam—quickly get out of date. Your application should be able to update itself at least once a day, but preferably several times per day (every two hours is probably sufficiently frequent for most people).
- **Does it integrate with my e-mail program?** Does the spam filter add a convenient menu or command into your e-mail reading program of choice? An integrated filter can be controlled from within your e-mail reader. All of this is handy stuff.
- **Can it perform whitelisting?** Will the spam filter make a *friends list* for you? Some filter apps automatically allow messages to pass if they come from people on your address book. This list, sometimes called a *whitelist*, makes it much easier to get the mail you really want to get.
- **Is the filter able to scan previously downloaded mail?** Some filters can only sift through mail for spam as you download it from the mail server. It's more convenient if your spam filter software can sort out the junk from mail you've previously downloaded and stored on your hard drive.

- **Will it blacklist an entire e-mail domain?** The process of *blacklisting* means the filter will automatically block e-mail from certain senders. But sometimes, you don't care whether the spam is coming from `zzzygot@yahoo.com` or `syzygy@yahoo.com`—you just want to stop getting any mail at all with a “yahoo.com” (experts call this *mail domain*) at the end. Not all filters can blacklist an entire domain.
- **Can you adjust how aggressively it filters mail?** Spam filtering software uses highly complex sets of rules to determine what mail is spam, as determined by the contents of the messages. On some products, if you find that a lot of spam slips past the filter, you can change a setting in the program's preferences that will force the spam filter to take a harder line with messages the filter thinks might be spam.
- **How much does it cost?** Filtering tools needn't be expensive, but as in most endeavors in life, you get what you pay for. By all means, download and try out as many free spam filters as you like. If a free filtering application does what you need, keep it. If not, you're not out any cash, and you can try another. We've included steps to get you started with two commercial spam filter products because, in tests performed by *PC World* in June 2004, they were the most effective filters. If you're going to dole out cash for a filtering tool, it should be at least as good as these.

Get Started with Cloudmark's SpamNet

SpamNet is a commercial spam filtering program from a company called Cloudmark. In many ways, it looks and works like many other spam filtering tools you can run on your PC. But SpamNet stands apart from the majority of spam filter tools, and not just because it uses a particularly effective technology to filter out spam. The users of the SpamNet network themselves are a part of the solution; each time a user of SpamNet uses the program, they help Cloudmark improve the accuracy of the SpamNet filters for everyone who uses the software. And with more than a million satisfied users signed up for the service, they must be doing something right.

Download and Install SpamNet

In order to filter your e-mail using SpamNet, you have to use one of the two Microsoft e-mail programs—Outlook or Outlook Express—to check and read e-mail. SpamNet costs \$4 per month to use, but you get the first month free to try out the service. Head over to <http://find.pcworld.com/42920> and click one of the two links to download the version that works with the e-mail program you use.

The installation process is simple: Just double-click the file you downloaded. SpamNet will install itself and add a small icon to the System Tray. When you

launch Outlook or Outlook Express for the first time after installing SpamNet, you'll notice a row with two new buttons (labeled Block and Unblock, respectively) and a Cloudmark drop-down menu right next to them, in the toolbar above the main window. You should also see a new mailbox, appropriately called Spam, which is where the junk you filter out will end up.

Filter Your Spam Using SpamNet

Filtering is about as easy as it gets: Just check your mail. SpamNet will kick into action as soon as your mail is downloaded into your inbox. The first thing you'll see is a dialog box asking if you want SpamNet to filter your mail (see Figure 9-5). You won't hear angels singing when you click Yes, but you might think you died and went to heaven when you see what happens next. Nearly all your spam will simply disappear into the ether, never to be seen again (unless you want it to).

SpamNet does a very good job of removing the majority of spam from your inbox with no user intervention, but part of what makes the software so accurate is how the program carefully watches which messages you choose to block. Invariably, a few spams will sneak through the filters. When they do, don't delete them the normal way; you can delete them by highlighting the spam messages (you can select more than one by holding down the CTRL key while single-clicking each spam message) and then clicking the Block button (see Figure 9-6).

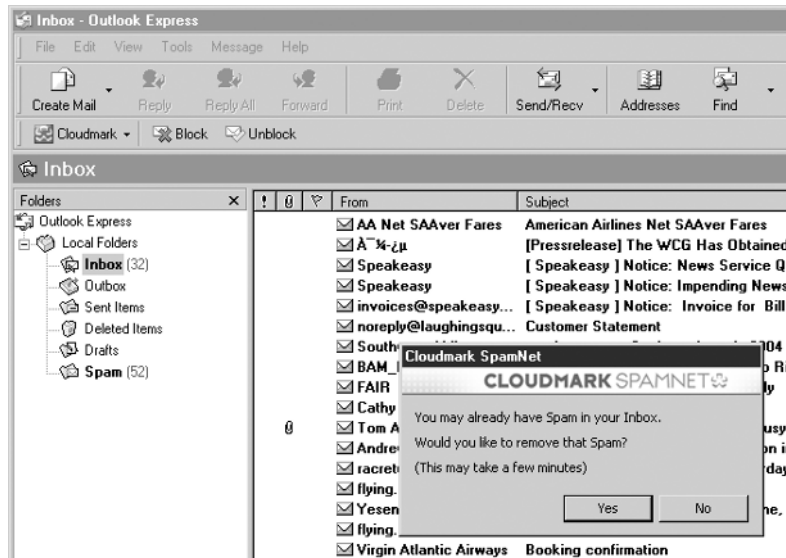


FIGURE 9-5

The first time you run SpamNet, the program will ask you if you want it to filter mail you previously downloaded. Click Yes and it will take care of your spam from then on.

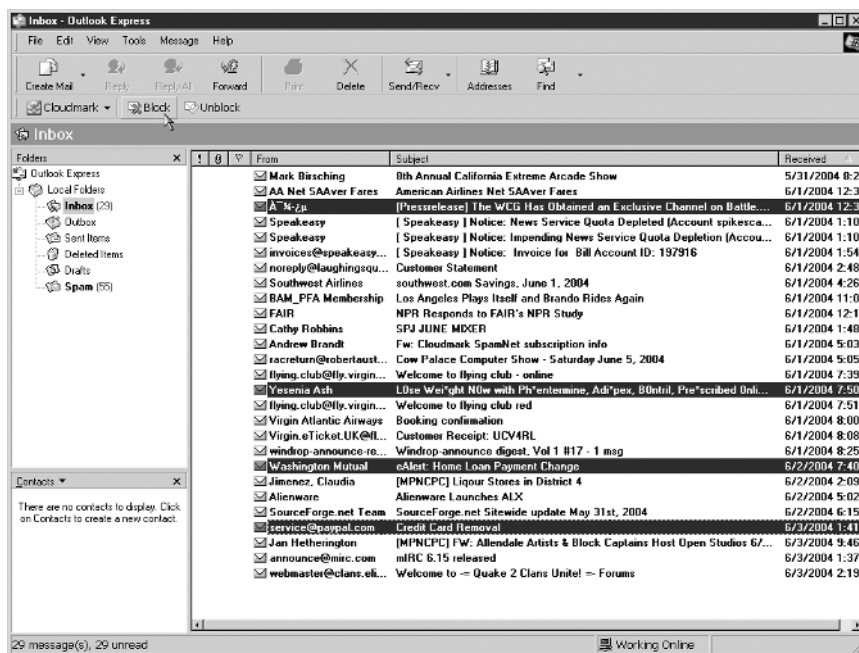


FIGURE 9-6 Select any spam messages that get through, and then click the Block button to take them out.

By using the Block button to delete your messages, you not only rid yourself of the junk in your inbox, but you help improve the accuracy of the filters for everyone who uses the service. The program even thanks you for your contribution to the accuracy of the system as a whole (although after you've done it a few times, you may just want to fill in the Don't Show Me This Again check box in the "thank you" dialog shown in Figure 9-7).



FIGURE 9-7 SpamNet will thank you each time you delete spam; by doing so you make the service more accurate.

SpamNet automatically adds any e-mail addresses from the Outlook or Outlook Express Address Book into its whitelist, so messages from those folks won't end up in the spam bucket. But before you add the addresses to SpamNet's whitelist, take a quick spin through your Address Book and delete those listings that you rarely or never use anymore. Each address in your whitelist becomes a chink in your spam armor, so to speak; the fewer addresses you whitelist unnecessarily, the more effective your filter will be.

In addition, you can manually add the addresses (or domains) to the whitelist of people whose messages you want to receive (see Figure 9-8). Click the Cloudmark drop-down menu and choose Options. In the SpamNet options dialog, click the Advanced button, and then select the Whitelist tab. Click the Add button to type in each e-mail address or mail domain; click OK twice when you're done.

Install and Run Sunbelt Software's iHateSpam

The iHateSpam program (also known as Giant Company Spam Inspector) is a sophisticated spam filter application. Like SpamNet, iHateSpam also networks with a large group of users, which it calls the Spam Learning Network Community. The choices these users make while using the application determine how new filters are created for all users of the program. And iHateSpam runs as a background application in the System Tray, ready for any time you might check your mail.

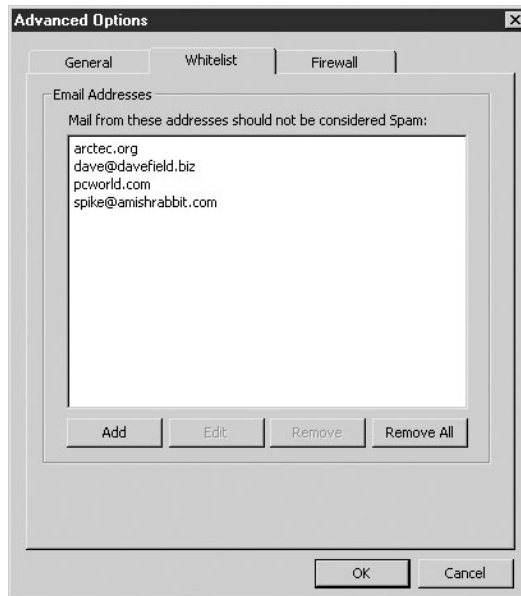


FIGURE 9-8 Whitelisting in SpamNet is fairly straightforward and keeps important e-mail from getting filtered accidentally.

The iHateSpam application has some unique features that set it apart from SpamNet. For one, you can configure the program to assume that mail written in the *character sets* of foreign languages (these look like strings of gibberish text and odd symbols, unless your PC's set up to display them in their correct form) comes from spammers, and block those messages automatically. The program can also filter messages from folders of older mail already on your hard drive. iHateSpam also works with a wider range of mail reader programs than SpamNet: it can sort spam from the Outlook, Outlook Express, Eudora, and IncrediMail clients, and from accounts on MSN's free Hotmail Web mail service (see Figure 9-9).

Download and Install iHateSpam

You can pick up a copy of iHateSpam from their Web site (<http://find.pcworld.com/42918>) and try it free for 30 days. The software comes as a single installation file that loads whatever plug-ins it needs into any of its supported clients and sets up the System Tray application. The program automatically scans the address books of any mail programs it supports and adds e-mail addresses from the Address Book (and from messages in the "Sent Mail" folder) to your whitelist.



FIGURE 9-9 Unlike many spam filtering tools, iHateSpam can filter the junk mail from MSN Hotmail, a Web-based e-mail service.

After you install iHateSpam, you'll step through a series of dialog boxes (as shown in Figure 9-10) asking you about which accounts you want to protect, and the particular spam filter settings you want to enable for each account. iHateSpam will check all the boxes by default; you can comfortably leave them checked as you click Next through them. When it's done, iHateSpam will download the latest spam filtering rules from the Web, but you'll need to reboot your computer in order for the integrated toolbar (more about this in the next section) to load properly in Outlook or Outlook Express.

Filter Your Spam Using iHateSpam

The program begins filtering spam immediately, though it works behind the scenes. It also scans through any mail in your e-mail program's Sent box or Out box and adds any e-mail addresses in there to your Friends List, which helps those senders pass through the spam filter more easily. As you download mail, iHateSpam intercepts it and puts the messages it thinks are spam messages into a quarantine area. To get to the quarantine, right-click the iHateSpam System Tray icon and choose View Spam Quarantine (see Figure 9-11). You should do this the first few weeks you use iHateSpam, every time you check messages.

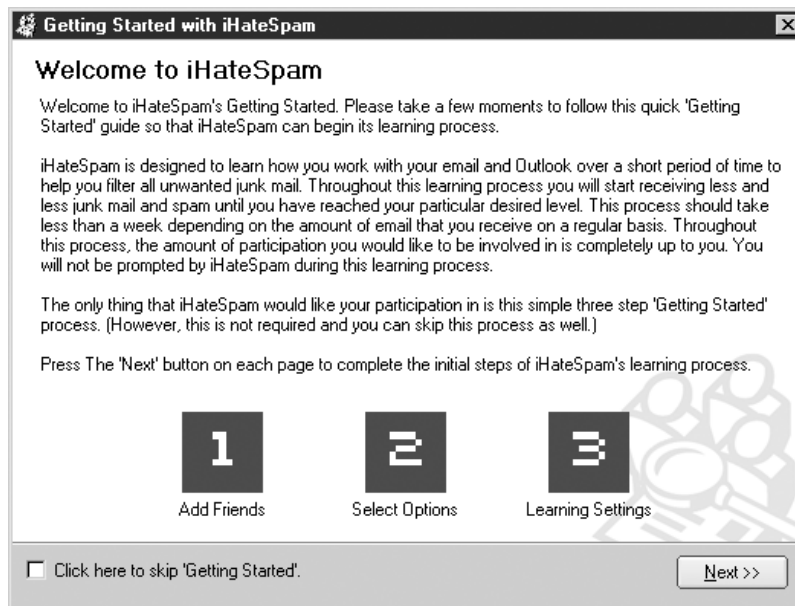


FIGURE 9-10 iHateSpam steps you through the process of deciding how aggressively you want to filter mail right after it installs itself.

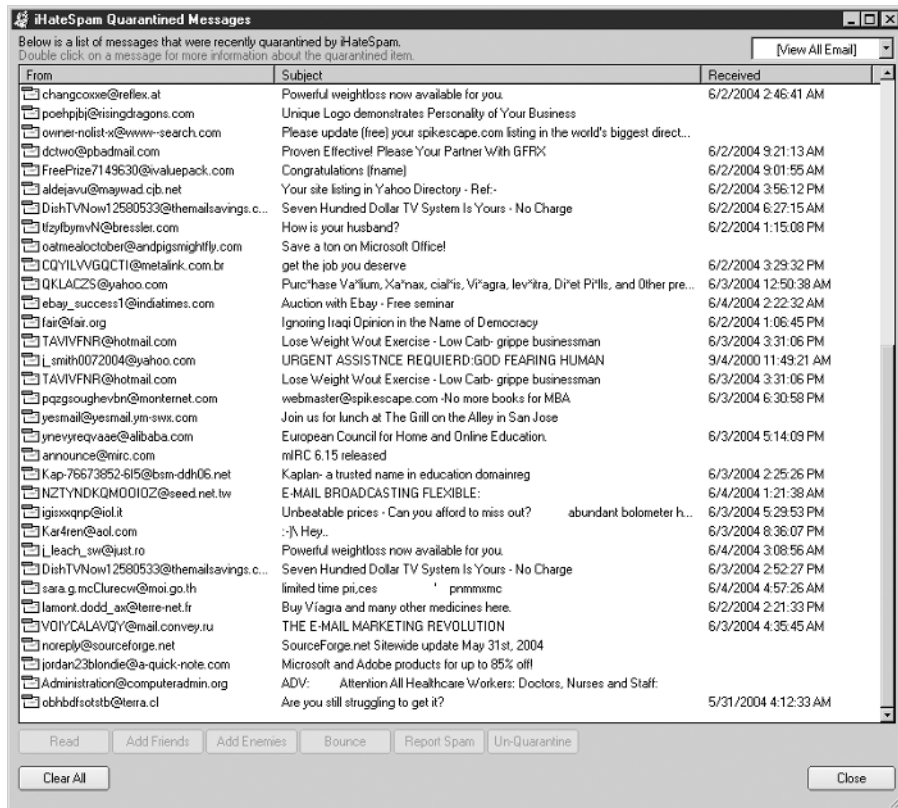


FIGURE 9-11 iHateSpam's Spam Quarantine gives you enough information to figure out whether the program filtered out a legitimate message as spam.

Look down the list of quarantined messages to see if any real messages got filtered, and choose Add Friends or Unquarantine to put those legit messages into your Inbox. The former option whitelists the sender of the message (Figure 9-12), while the latter merely moves the message to your inbox without making any rules for dealing with future mail from that sender.

In Outlook, Outlook Express, or Eudora (version 5 or greater), iHateSpam adds a series of buttons to the mail application toolbar. These buttons help you train the program as well as update the service with newly identified spam that slips through your filters. The Add To Friends and Add To Enemies buttons put the senders of selected messages in a whitelist or blacklist, respectively. The Not Spam! and Is

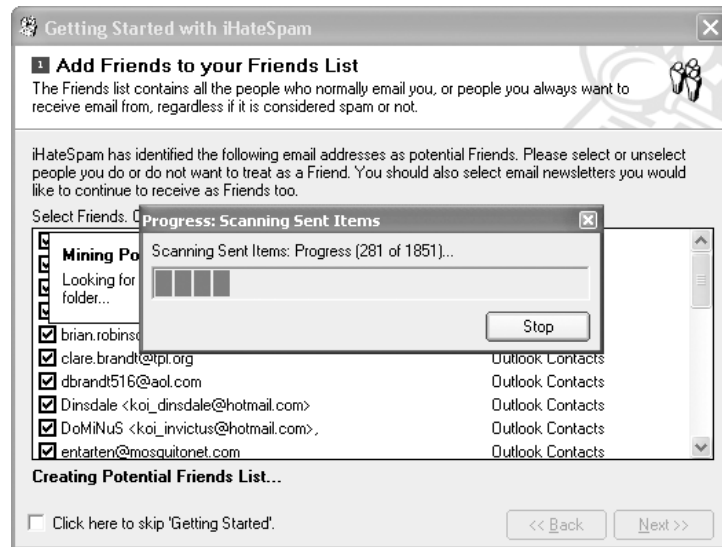


FIGURE 9-12 When you first load iHateSpam, the program scans through your sent mail to create a “whitelist” of senders that will automatically pass through the spam filter.

Spam! buttons let the program know when it’s accidentally filtered a message you want to keep, or when it’s let a spam message through to your inbox. (The latter button deletes the spam message[s] you’ve highlighted while triggering the program to update the Community Network about your decision.)

One of our favorite features of iHateSpam is its ability to sift through mail that you’ve already downloaded and take the junk out (see Figure 9-13). In Outlook or Outlook Express, click the iHateSpam menu, select Clean, and then select Clean An Outlook Folder. Leave the radio buttons in their default positions on the Read/Unread Mail option, and choose the All option for the date range. The program will then go through the mail and dump any spam you may have previously downloaded.

As with most spam filtering applications, you’ll notice the program will improve over time, with training about (and more experience with) your personal e-mail preferences. As you tell it what messages you like and don’t like, it will get better at making educated guesses about spam remarkably quickly.

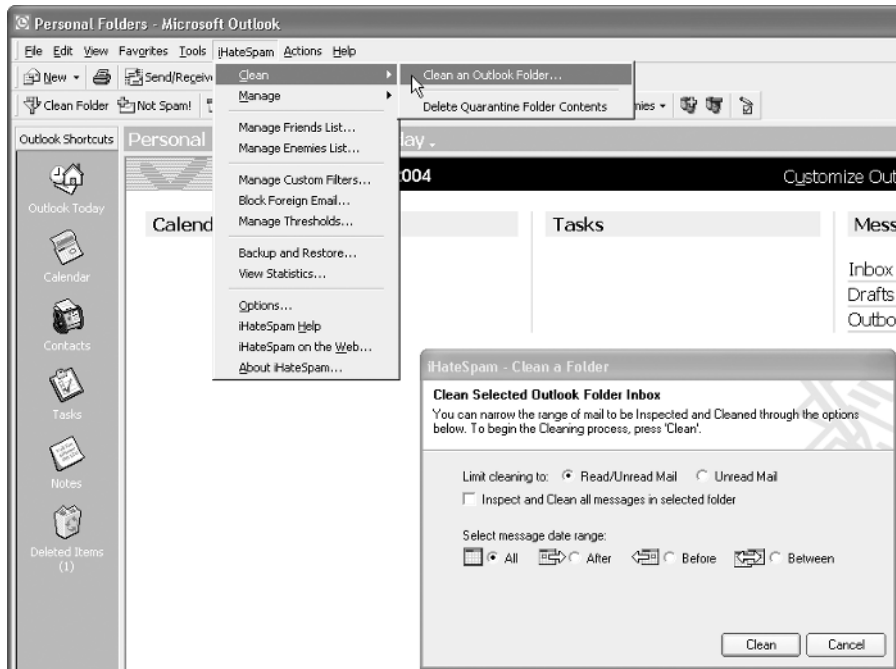


FIGURE 9-13 iHateSpam cleans spam out of folders where you may have previously downloaded spam, a handy feature.

Get Rid of Spam with Less Effort

If, for one reason or another, you don't prefer to use a spam filtering application for your PC, you aren't stuck without help as you would be if you were stranded on an iceberg in the mid-Atlantic. You can also filter your mail directly at the mail server, bypassing the need even to download the spam for the purpose of filtering.

Let Your ISP Filter Your Mail for You

Virtually every major Internet service provider now offers some form of spam protection to their customers. From free e-mail providers like Yahoo or Hotmail to premium services like MSN, AOL, Earthlink, and most broadband ISPs, it's much easier to let your ISP's filtering software do the heavy lifting, eliminating the bulk (no pun intended) of the spam from your inbox before you even get to it.

Many of the ISP filtering services are provided as part of the cost of the service, so you won't see any additional charges on your monthly bill if you decide to take advantage of them. And really, you'd be silly not to. Even if you wanted to keep your spam filter app on your PC, feeding it pre-filtered mail can only improve its accuracy.

In many cases, the filtering is already turned on by default, but you do have the option to increase the tenacity with which the ISP filter sorts spam from mail. With most ISP spam filters, this setting will default to a medium level; turn it up a notch if you're finding that spam still gets through their defenses. Where the ISP puts the control panel for making these changes depends on who you ask; AOL puts their spam filtering settings into the mail area of their service (go to AOL Keyword: Spam for more information). Web e-mail services, Hotmail or Yahoo mail, for instance, locate the spam filter aggressiveness settings in the Preferences section of the site.

What Filtering Is Available at Your ISP?

If you take the time to train Internet provider-based spam filter tools, they can be as much as 98 percent accurate at filtering bad from good, while not accidentally filtering out something you might want. Besides, you can't beat the price. Here are some ISPs and their spam filtering offerings:

- **Earthlink** Their SpamBlocker utility has three levels of spam filtering you can set. The highest level only lets through e-mail messages sent by people whose addresses you've added to your address book, while the middle level uses services provided by spam filtering provider Brightmail. Brightmail's accuracy falls at roughly 96 percent, according to tests performed for *InfoWorld* magazine.
- **AOL** AOL's spam filters offer whitelisting as well as blacklisting, and a couple of tiers of aggressiveness for the logic-driven filtering they perform.
- **MSN Hotmail and MSN Premium/Plus** Microsoft has its own filtering tool built into these Web-based e-mail sites that offers five levels of increasingly tough filtering. You train it over time, and it gradually learns your e-mail preferences. It also gets help from Brightmail.
- **Adelphia** This cable broadband ISP uses Brightmail and a service called a *real-time blackhole list* (or RBL), which helps the ISP block the computers that are sending spam.
- **Comcast** Using a combination of spam filtering tools, the cable ISP also scans its network looking for "spam zombies"—computers that have been taken over by spammers so that they can be used to send more spam. Zombified computers get kicked off the network until they're fixed.

- **SBC Yahoo** SBC not only uses RBLs to block spammy computers that try to flood its DSL customers, but it blocks mail from any computer that sends spam to its network (whether or not it's on the RBL, and even if the machine belongs to one of their customers).
- **Speakeasy** This DSL broadband ISP uses an Open Source spam filter called SpamAssassin to filter messages sent to its customers. SpamAssassin had a 93 percent accuracy rate in tests by *InfoWorld* magazine.

Report Spam to the Authorities

Strange as it may sound, some people actually like to get spam e-mail—the more, the better. Of course, they're not just anyone. Many of these folks who want your spam plan to use it to staunch the flow of spam in ways other than filtering.

Who Wants My Spam and Why?

Several organizations keep track of spam e-mail. Government regulators, for example, want a record of the spam that violates federal truth-in-advertising rules, as well as spam messages that break other guidelines and laws about the content and presentation of spam messages. Using the spam they've collected over the years, the Federal Trade Commission (FTC) has successfully sued some of the most pernicious spammers on the Internet, levying major fines against the violators.

But despite high-profile government action, the spam industry is turning up the heat, and the volume has only risen over time. Some private companies are getting into the spam collection business as well; Matterform Media, a company that sells a popular spam filtering application for the Macintosh called Spamfire, is the main supporter of an organization called SpamCrime (www.spamcrime.com), which has the stated goal of collecting evidence that will help convict spammers of violations of the federal CAN-SPAM Act.

How Can I Automatically Report Spam?

Right now, it's fairly easy to report spam to a spam filtering company, but it's not always easy to report spam to the authorities. Some software applications, such as iHateSpam, add a "Report" button to their toolbar; clicking this button in iHateSpam sends an automated e-mail to the abuse desk at the Internet service provider from which the spam mail originated, as well as to "a number of spam abuse agencies," according to the program's documentation. One such spam abuse organization, Spamcop.com, allows you to paste the headers from your spam e-mail messages into a Web form on its site. You don't need any special program to do this, but it takes time and effort.

Voices from the Community

A Spam-Warrior's Look at Trends in Spam

Enrique Salem, CEO of the anti-spam firm Brightmail, doesn't have an easy job. Companies subscribe to Brightmail's service, which (in tests performed by the magazine *InfoWorld*) filters about 96 percent of the spam from their employees' e-mail before it even reaches their inboxes.

NOTE

McGraw-Hill/Osborne, the publisher of this book, is a Brightmail customer; the author is not.

We asked Salem about current spam trends, which include completely blank e-mail messages, with no headers or body. “[It’s called] harvesting,” says Salem. The spammers throw an entire dictionary-full of names at your mail server.

“If they don’t get any bounces, then they know it’s a legitimate address,” he explains. “They have no *From* address, no subject line, and no body. They don’t even require you to open [the message] now.

“We work to block those types of messages when we see lots of them coming in,” he added. “We determine the IP address ranges where they’re being sent from, and that helps us determine, hey, *that* IP address is sending us a bunch of blank messages. [It’s a] pretty high likelihood that it’s trying to do harvesting.” Then Brightmail blocks any mail coming from that machine for a few hours.

Previously, spammers used web beacons—transparent one-pixel GIF images—to find real e-mail addresses. When you would open a message with a web beacon inside, it would load the image. The act of loading the image tells the spammer you’re there, because a unique URL (encoded with a key tied to your e-mail address) is used for each web beacon. “When you load that image, it tells the spammer ‘Enrique Salem has opened that message,’” Salem said. Once spam filtering companies figured out web beacons, it became a trivial matter to block them. Spam filtering companies are also starting to see a large percentage of spam messages in a range of foreign languages and alphabets, including Cyrillic, Chinese, Arabic, and Japanese. “I’ve seen lots in Cyrillic. E-mail is global. [Spammers] outside the U.S. are buying CDs that have hundreds of millions of addresses, and [send spam to them],” he said. Another emerging trend is the spam with crazy spellings of English words. These messages employ some of the many different ways spammers try to defeat spam filters known as *Bayesian* filters,

which sort through spam by looking for the combination and frequency of certain words within messages. “It’s pretty clever: The first letter and the last letter of a word will be what it should be, but all the letters in between will be scrambled.

“You can still read the message,” he adds, “because the human mind can look at the character patterns and say ‘First letter and last letter are what they should be; the letters in the middle don’t matter.’” But the Bayesian filter might miss the words and let the spam get through.

Finally, Salem warns that you should beware of Active Content: these kinds of spam go fishing (or “phishing”) for your personal information by impersonating a message from your bank or credit card company. “People are using JavaScript in their messages,” Salem says. These scripts can silently load programs onto your PC, which then record the usernames and passwords you use, and send those passwords to criminals.

To grab your headers in Outlook Express, right-click the e-mail listing in the mailbox view (or click File | Properties in the window displaying a message) to open the Properties sheet. Choose the Details tab as shown in Figure 9-14 to see the full headers; you can select and copy the text of part or all of the header section.

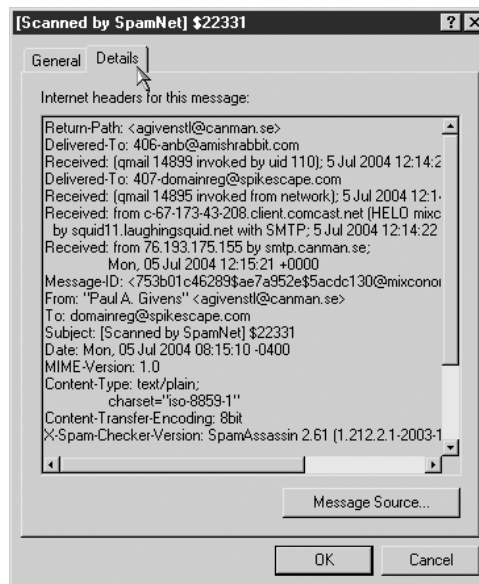


FIGURE 9-14 The Details tab of a message’s Properties contains the full message headers.

When you paste the headers into the form, Spamcop determines which ISP the spam message came from, and automatically sends an e-mail to the Abuse address at the ISP. Spamfire also supports Spamcop.com's formatting requirements for submitting spam to their evidence collection system, so you can use that program as well. Whether this action will do you any good is a matter of debate. Many spammers operate sophisticated operations in which they act as their own ISP. Your complaints to these spammer-owned-and-operated ISPs are likely to fall on deaf ears.

Sam Spade is a free program that allows you to investigate spam on your own (download this handy tool from <http://find.pcworld.com/43400>). If you copy all the headers of a message from your e-mail program and paste them into Sam Spade, you can track down the computer from which a particular piece of spam originated. Since spammers create bogus headers and manipulate real ones, Sam Spade helps you quickly sort out which header is giving real information, and which is made up.

To get started, copy the full headers out of your e-mail program, click Tools | Parse Email Headers in Sam Spade, and then click the Paste and the Parse buttons (see Figure 9-15).

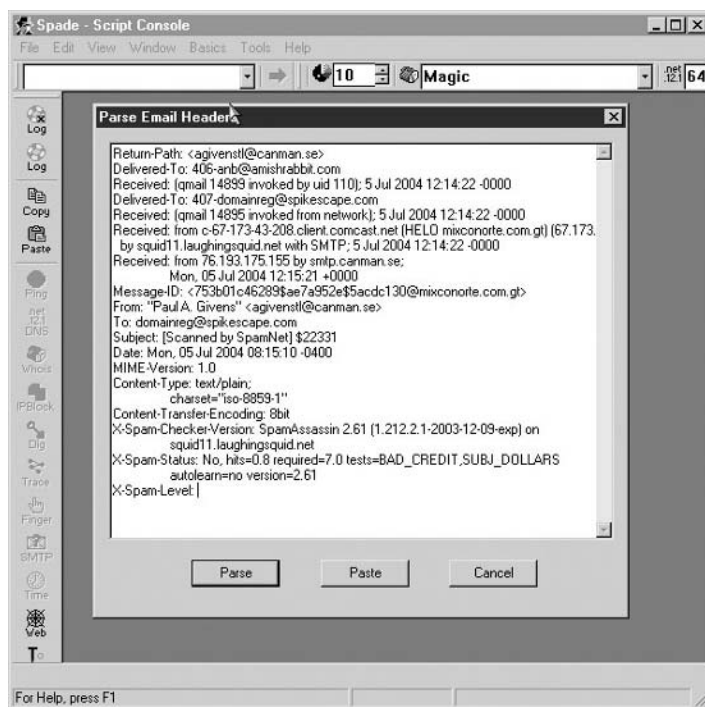


FIGURE 9-15 Paste the headers you copied into Sam Spade's Parse Email Header tool.

When Sam Spade's done, it will display a results window that breaks down each individual part of the mail header and explains (in real English) how to interpret those lines. In Figure 9-16, the mail header shows that a spam message came from the computer of a Comcast cable-modem subscriber, but the spam program that sent the message made it appear to come from a computer based in Guatemala, with a distinctive *.gt* top-level domain. In this case, the Comcast subscriber's computer was probably being used as a *spam zombie* (for more on this phenomenon, see "Attack of the Zombie Hordes" later in this chapter).

Some spammers, however, are trying to take advantage of some people's righteous indignation over spam messages by posing as antispam organizations, and stealing the addresses of people who report spam to them for the purpose of sending more spam to those folks. That appears to be the case with the professional-looking Web site of the Spamming Bureau (www.spammingbureau.com), which is now well known to be operated by a fairly notorious group of spammers. Don't be taken in; the entire endeavor is a clever scheme to harvest the e-mail addresses of people who already hate spam.

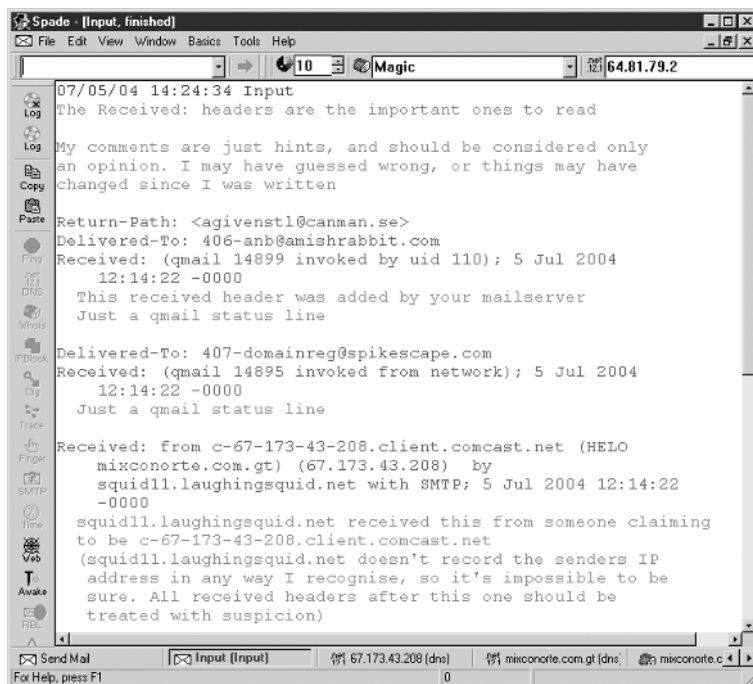


FIGURE 9-16

Why would a PC on a Comcast cable account in Chicago send mail that looks like it came from Guatemala? Something smells fishy here, says Sam Spade.

Who Can I Send Spam to Manually?

The Federal Trade Commission is actively pursuing civil penalties against any spammers it can get its hands on. Already, the commission has put a stop to spammers who were advertising miracle cures for cancer and expensive, fake “medical devices” that could “cure” otherwise terminal diseases. The FTC has also won lawsuits against spammers who put falsified or nonfunctional “Remove Me” links or e-mail addresses in their messages, on the premise that the nonworking link is a form of false advertising. You’ll probably note that most spammers don’t even bother putting a Remove Me link in their spam anymore, since most filters think that’s a fairly obvious indication the message is spam.

If you get a particularly nasty spam message, you can e-mail the message to the FTC at their spam collection address, which is uce@ftc.gov. Don’t expect to get a response; the FTC gets millions of messages every week.

Spam Fighting Looks Toward the Future

In the near term, the fight against spam will be fought with technological tools intended to cut off the methods spammers use to transmit their messages and manipulate the headers of e-mail messages to mask their origins. But further down the road, a new arsenal of tools—some legal, some technical—may become available that could take a serious chunk of the spammers completely out of the picture. In the meantime, we’ll just have to wait and see what comes of these new ways to attack the very nature of spam.

Antispam Legislation Gets Tough

Laws to address the problem of spam are making their way through legislatures around the globe. No fewer than 20 laws forbidding various aspects of spamming are currently on the books or are in debate in the halls of the world’s governments. Some lawmakers believe antispam laws may curb the tide of junk mail, while opponents argue that spammers, who break myriad laws that already exist, couldn’t care less about new laws.

How U.S. Antispam Laws Affect You

The biggest national law aimed at curtailing spam, the CAN-SPAM Act, was passed in 2003 as a first step to put spammers in their place. The law requires spammers to provide a real e-mail and postal mailing address in each message they send out, along with information about how to stop receiving mailings, and some indication in the Subject line that a message contains adult content. Since the passage of the

CAN-SPAM Act, the volume of spam has not only not gone down or stayed steady, but has increased tremendously.

Antispam software firm Commtouch analyzed spam for compliance with the act, and found that, six months after the law took effect at the beginning of 2004, nearly 10 percent of spammers were (apparently) at least partially complying with the terms of the law. As a result, said Commtouch vice president Avner Amram, CAN-SPAM “tells spammers what their mail has to comply with in order to be legitimate in the eyes of the law.”

Through CAN-SPAM, the U.S. congress may have sent the wrong message to spammers, letting them know that, as long as they put some contact information into their messages, they may spam to their hearts’ content. And that doesn’t help anyone but the spammers.

Spam Fighters Take Legal Action

The folks who fight the good fight on behalf of everyday computer users are not just sleeping on the job. Spammers have been arrested, charged with serious crimes, and also sued in civil court. State attorney generals, along with some federal and local prosecutors, are battling the spam epidemic, one spammer at a time.

Uncle Sam vs. Spam

The highest-profile antispam crusader in law enforcement is New York’s state attorney general, Eliot Spitzer, who, together with assistant attorney general Stephen Kline, is taking down spammers one by one. Spitzer might be the closest we have to an Elliott Ness (the legendary Mafia-busting crimefighter who took down Al Capone) of our age; his office confronts spam as it really is: crime that affects all of us in one way or another, but that is so pervasive the cops in your local burg wouldn’t know where to start.

Spitzer’s crusade against spammers even takes a page from Ness’ book, turning classic laws into a wedge that can shut down a spam organization. In one example, he charged one notorious spammer, Howard Carmack, with criminal possession of a forgery device—the spammer’s spam-sending software program—and several other counts of fraud and identity theft for forging the e-mail addresses he used on spam messages. In May 2004 he was sentenced to seven years in prison for the crimes of fraud and identity theft.

In the long run, we may need dozens of Eliot Spitzers in order to stop a substantial percentage of the criminal spammers who wantonly flout laws and the interests of the vast majority of Internet users. For now, we should count our lucky stars we have at least one.

ISP Lawsuits

Internet service providers aren't just sitting idly back while the spam epidemic continues unabated. Companies like Microsoft, AOL, Earthlink, and SBC Yahoo are suing what they call "hard core spammers" for gross violations of CAN-SPAM. AOL vice president and general counsel Randall Boe told a reporter that "congress gave us the necessary tools to pursue spammers with stiff penalties, and we in the industry didn't waste a moment."

The companies filed six lawsuits simultaneously, naming hundreds of spammers, in four different federal court jurisdictions. One of the spam companies sued by the ISPs sent more than 94 million messages to Yahoo customers in one month alone; the messages contained highly deceptive subject lines, intending to draw victims into opening the message. Microsoft sued spammers they alleged sent hundreds of millions of e-mail messages to MSN Hotmail users over the course of several months.

In the end, suing spammers may stop a few of them, but as you'll read later in the chapter, lawsuits may not be enough to stop spammers.

Spammers Turn Up the Heat, and Fight Back

With all the action being taken against spammers, don't think the spammers are taking any of it lying down. Some spammers are turning to engage in vicious, criminal cyber-attacks on the companies, individuals, and organizations that fight spam.

Spammers Attack, Temporarily Shut Down, Blackhole-List Sites

Several organizations operate services that list the internet protocol (IP) addresses of computers or networks from which spam originates. These services, called blackhole lists, are used by ISPs, who set up their mail servers to reject any mail that comes from any of the IP addresses in the list. Blackhole lists are an important component in the ISP's war on spam.

In 2003, however, many of the providers of blackhole lists came under cyber-attack from, it's assumed, spammers who decided to fight back against the services. The blackhole list sites fell victim to what are known as distributed denial of service (DDoS) attacks—in short, the Web servers that hosted the blackhole list files became swamped with requests when millions of computers at once were instructed to connect to the servers. Nobody has ever claimed responsibility for the attacks, but they resulted in at least one organization, Osirusoft, shutting down its blackhole list service entirely. The company was unable to engage in normal business functions after a continuous DDoS attack that lasted for weeks on end without a pause, and stopped its blackhole service in August 2003.

Something Phishy This Way Comes

Starting in 2003, spam victims started receiving e-mail messages that appeared, on the face, to originate from legitimate banks and other businesses. Customers of (among other companies) CitiBank and PayPal, the online payment service owned by eBay, received messages that informed them of a need to log into the service and change their passwords. Research firm Gartner has published estimates that 57 million Internet users in the U.S. have received these kinds of e-mails.

Unfortunately, many of those who received the messages (Gartner estimates about 1.7 million of them, or roughly 3 percent of those who receive the e-mails) simply followed the URL link in the message and submitted their username and password to scam artists, who then used the information to raid their bank and credit accounts. Before long, thousands fell victim to these fraudulent e-mails, which took advantage of a vulnerability in certain versions of Microsoft Internet Explorer and Outlook Express to conceal the true URL the scammers used to host realistic-looking Web pages.

These scams, which came to be known as phishing schemes, have netted hundreds of thousands of dollars from unsuspecting Internet users. And even though the vulnerability that helped the con artists behind the phishing scam hide their identity has been fixed, people still fall victim to phishing e-mail messages every day.

Phishing attacks increased by 180 percent from March to April 2004, according to Dave Jevans, senior vice president at e-mail security firm Tumbleweed Communications. Phishers can rake in \$100,000 per attack, according to Jevans, and it can cost a company \$30,000 to recover from such an attack. He also claims that 30 new phishing attacks occur every day, and on average, the number of new attacks increases by 50 percent from month to month.

Phishers, the con men involved in these scams, aren't immune to the law, and a few are getting caught. In May 2004, Zachary Keith Hill, a 20-year-old from Texas, was sent to prison for a nearly four-year sentence after pleading guilty to defrauding America Online and PayPal customers out of more than \$50,000. But Hill was only the first person convicted of this relatively new crime.

The best advice we can give to anyone who may receive an e-mail message from their bank or an online financial company is this: Type the URL of the company into the browser yourself, with your own fingers, and don't follow any link in an e-mail message. And when a company contacts you about changing your password, never, ever give that password to someone claiming to be an employee of the company. They should never need to know that information, and they are instructed not to ask, so you should never give it out to them.

Attack of the Zombie Hordes

According to a computer security company called Sandvine, 80 percent of spam comes from PCs owned by normal people that are infected with a particularly nasty kind of virus. These computers, called Spam Zombies by security and antivirus professionals, are infected when spammers release programs onto the Internet that break into computers; the programs then send a message back to the spammer and allow the spammer to remotely control some operations of the computer.

Did you
know?

Spam Filters Could, One Day, Help Create Machines That Understand Us

As spammers grow ever more sophisticated and adept at avoiding spam filters, spam filter technology has pushed its own limits. Modern spam filters are marvels of the information age, with more raw human intelligence and research hours being poured into this field than nearly any other in the world of software development.

Take, for example, the advent of Bayesian filtering. This technique, which is now a key part of any spam filter software worth its salt, seems simple enough: Bayesian filters take what they know about spam—as well as what spam messages slip through the cracks—and adjust their own internal filtering rules to account for anomalies and catch more spam. Essentially, the computer learns more about what makes up spam over time just by filtering, and (because what one person considers spam may be another’s legitimate e-mail) figures out how to improve the filtering accuracy for *an individual’s* e-mail preferences, rather than for some global average.

Bayesian filters were the next logical step after the somewhat less intelligent *rules-based scoring* filters, which look at (for example) the number of times a message has the word “Remove” in it, and then issue a ruling about whether the message breaks enough of these rules to make it a likely spam message. Rules-based filters contain hundreds of rules, and each rule has a score assigned to it. The higher the score, the more likely a message is spam. But the scores aren’t perfect, because they can’t adapt to the needs of different people or the changing nature of spam. The number values tend to be arbitrary as well, further complicating matters.

When a Bayesian spam filter looks at a message, it's not looking just at the message body and the words contained in that body (though it does examine those aspects of a message). It's also looking at the message *headers* that indicate where it came from, some of the *HTML* that forms normally “invisible” parts of the message, and how the words in the message are combined to make phrases.

In this way, spam filters have become, almost overnight, the most adaptable, intelligent, almost-sentient software humans have ever created. If there's one upside to spam, you could argue that spam has forced the best and brightest minds in computer science to work hard at developing the foundations of what may be the next step in artificial intelligence—the ability to *parse* written human language, and derive the meaning of messages even when the writer of the message fails to use conventional spelling or grammar. We may not have androids to cater to our every whim today, but the creation of ever more advanced spam filters may help bring that day a little closer to reality.

How can you prevent this from happening to you? The same way you block other kinds of viruses and worms: Keep your system up to date with security patches from Windows Update (windowsupdate.microsoft.com); use an antivirus program to scan your hard drive regularly, and keep it up to date; and use a software firewall, such as the free ZoneAlarm (www.zonelabs.com) to prevent these remote control programs from receiving commands from their distant operators.

Some ISPs are actively scanning their networks, looking for these Spam Zombies. If you receive a message from your provider telling you that your computer is infected, take the message seriously and deal with it as quickly as possible. You may even need to physically unplug your computer from the Internet for a while as you work through the problem. Just remember, if you find out that your computer's been turned into a Spam Zombie, it might be bad but it could have been much worse: next time, a cyber-criminal might try to steal your personal information or log your keystrokes to learn your bank account numbers.

When Is Spam Like a Virus?

The majority of virus attacks that have flooded the Internet of late are being instigated by spammers, according to security experts. The spammers send out millions of worms, which infect machines all over the world, and then the spammers use the infected machines to do their dirty work for them—work that might be going on right under your nose, which can land you in a lot of hot water with your ISP.

In fact, spammers and the tools they use are getting increasingly bold and vicious. “You can’t separate spam and viruses anymore,” said Mark Sunner, chief technology officer of e-mail security company MessageLabs. “Virtually all the viruses this year have to do with spam.”

Two New Threats: Spim & SMS Spam

Spammers know that you’re using spam filtering tools on your e-mail services, so they’ve started branching out and exploring new avenues they can exploit. One of the technologies they’re directing their energies toward is instant messaging, or IM. Companies like AOL, ICQ, MSN, and Yahoo offer these services free of charge, and IM has become popular among business users as well as teenagers. (For more about instant messaging, and how to block unwanted IM messages, see Chapter 10.)

Unfortunately, the immediacy of instant messaging means that spammers can send tens of thousands of messages per second to other Internet users, and because IM clients can tell you whether your message got through, the spammers can immediately know that those users have received the messages.

Spam over IM, or *spim*, is growing in popularity, but IM users have a greater degree of control over who may send them messages than do e-mail users. Most instant messaging client software programs allow the user to turn off any messages that come from people they don’t know. At a bare minimum, if you use instant messaging, this is a great first step you can take to reduce the number of spim messages you receive.

Another form of instant messaging—that takes place over cell phones—is called SMS, which stands for Short Messaging Service. These brief text messages can be sent instantly from one phone user to another, or sometimes from computers to individual phones. But a new class of mass-marketing software is being used in Europe, where SMS messaging is used by virtually everyone, to blast short advertisements at thousands of cell phone users at once.

While the problem is bad in Europe, it looks like SMS spam would be a much worse problem on this side of the pond. In some countries, SMS messaging is free with the monthly charge for the phone; as a result, outside the U.S., virtually every cell phone owner uses SMS regularly for personal and business communications. But most U.S. mobile phone service providers charge the recipient a small fee each time they receive an SMS message. If the SMS spam problem crosses the Atlantic and becomes a problem here, you won’t just have to worry about the nuisance factor, but the fact that you’ll be responsible for all those SMS message charges as well!

Chapter 10

Chat and Send Instant Messages Safely



How to...

- Protect your IM client from being attacked by viruses
- Prevent worms from attacking you in IRC
- Chat with strangers, safely and pseudonymously
- Reduce your risk of being stalked or harassed online

Use Instant Messaging and Chat Wisely

With an immediacy that e-mail can't rival and (for the time being, at least) a dearth of unwanted commercial messages, *instant messaging (IM)* services let you have conversations in near-real time with people around the world. Instant messaging and its cousin, *Internet chat*, can be extremely valuable communications tools: While teens were the first to pick up chat and IM in great numbers, businesses are just starting to discover that IM helps workers collaborate on projects or ask one another questions in a flexible, casual environment.

Chatting is like standing around a virtual water cooler, shooting the breeze; using IM has become a serious business tool, quickly passing messages between team members. Best of all, most IM and chat services cost nothing at all to use, and the software is free.

But IM and chat aren't all wine and roses. Some IM users are seriously bad people, who use IM to track down, harass, stalk, or otherwise make other IM users miserable. Worms or viruses can travel from computer to computer using the file sharing features in some IM or Internet Relay Chat (IRC) clients, but you can set up your antivirus software to automatically scan incoming files in IM and IRC just as it would scan incoming e-mail attachments. You'll also learn in this chapter how to safely interact in IM and chat with people you've never met in person. And IM isn't spam-proof; later in this chapter we'll teach you how to disable features in your IM client software that can result in you getting unwanted messages, and how to block troublesome users.

With tens of millions of daily users, the growing popularity of IM means that even if you don't use IM now, you probably will start using it before too long. And if you use IM already, you might not even be aware how easily you can protect your privacy using the settings built right into your IM client.

Evaluate the Risk IM and IRC Pose to You

Most people spend more time deciding which IM client application to use than thinking about how they use (or plan to use) IM and what the risks are of using IM. After all, you wouldn't want just anyone to have your telephone number; you should put some thought into planning the circumstances under which you give out your instant messaging contact information, and to whom you give it.

The risks instant messaging poses the average person ranges from nuisance-level annoyance all the way up to personal injury (or worse) at the hands of another. Child molesters, say Internet safety experts, use IM to *groom* (gain the trust of, and gather information about) the children they plan to attack. Petty squabbles in online communities have led to unbalanced individuals stalking (and sometimes physically attacking) one or more victims who first met in an online chat room.

Malicious hackers haven't missed the fact IM has been growing at an almost exponential rate. More automated attacks using worms or viruses take advantage of the "click first, ask questions later" reflex most people have, and spread rapidly through swaths of instant messaging users' computers by sending links to infectious files disguised as games or utilities, or to web pages that exploit a vulnerability in Internet Explorer and silently install malicious software.

Determine Whether the Risk of Chatting Is Worth the Benefits

It's hard to give an unqualified answer to the question, "Is IM right for you?" Most people can and do use IM safely every day, combining the use of their own good common sense with a few precautions that don't apply anywhere but on the Internet. Sometimes, people get themselves into trouble for ignoring rules of common sense online in ways that, in the real, physical world, they would never do. Training yourself in the sometimes counterintuitive rules of chatting safely is always preferable to skipping using this revolutionary communications tool.

Cutting yourself off from the promise of instant messaging, simply out of fear of what might happen, is the least desirable outcome. IM and chat can be a source of empowerment for the disenfranchised, or for the disabled. On the Internet, through real-time text messaging services like IM and chat, you can't tell that someone is deaf, or the color of a person's skin. People who are afraid to speak publicly in the real world overcome their anxieties and express themselves without fear online. Communities form, friendships bloom, and even lifelong commitments sometimes result from what are, in essence, short strings of text messages sent from one person to another.

When you consider all that, the trouble of learning what kind of information about yourself you can safely provide to the world seems a lot less odious than the only other alternative: losing the benefits chat and IM provide.

Secure Your Instant Messaging (IM) and Chat Applications

Anyone can download and use an instant messaging or IRC application, but in order to protect yourself, you'll want to change some of the default settings in the clients. In addition, if you create an online profile for yourself in one or more IM services, you'll probably need to revisit that profile to make sure you haven't given away too much personally identifiable information.

Get an IM or Chat Client Application

Your choice of IM service will probably be dictated by which service the majority of your friends, clients, or family already use. That's because the so-called *first-party clients*—the client applications distributed by the IM service, such as AOL Instant Messenger (AIM), shown in Figure 10-1—don't talk to different IM services.



FIGURE 10-1 AIM is a popular first-party IM client.

Eventually, you may end up with lots of IM contacts, but not all of these people will be registered with the same IM service. In these cases, you could run each of the first-party clients individually (and have from two to five additional applications running in the background—not a desirable outcome), or you could use an *aggregator* (also called a “multiprotocol” or “multiservice”) client, which can sign on to, send messages to, and receive messages from multiple different IM services, all within the same application (see Figure 10-2).

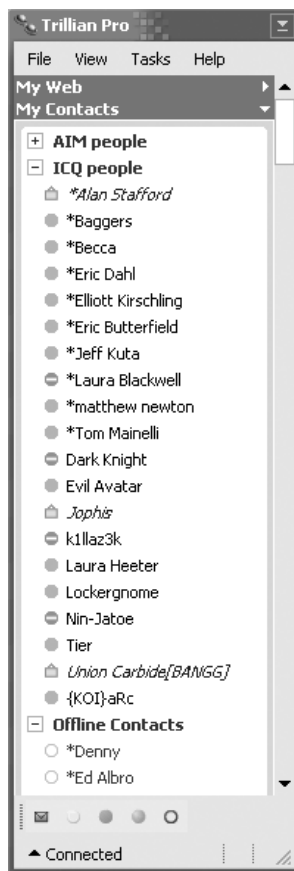


FIGURE 10-2 Trillian lets you connect to accounts on several IM services at once.

Where to Get First-Party Clients

The following short list of the most popular IM services is not intended to be comprehensive, but it will help you find the client applications for those services.

- **AOL Instant Messenger (AIM)** If you don't already have an AOL or AIM account, sign up for the service for free on the AIM web site at <http://find.pcworld.com/43038>, and then download the client at <http://find.pcworld.com/43036>.
- **ICQ** Download the ICQ 4 Lite client (www.icq.com/download), and then install the application. If you have an ICQ account, it will ask you for your login information. Otherwise, click the Get An ICQ Number button in the client to register for the service.

NOTE

Once you're registered with ICQ, different icons of bright green flowers (shown in Figure 10-3) indicate the status of people on your contact list. A flower on its own means the other person is ready to chat. A small document next to the flower means the contact has temporarily stepped away. A padlock icon means they don't want to be disturbed.

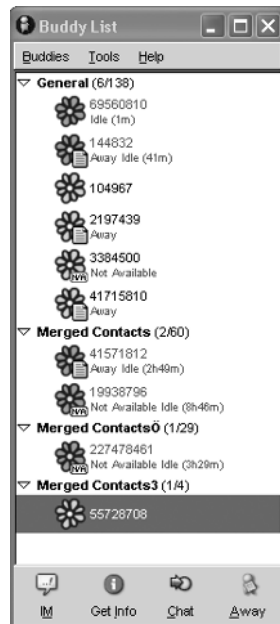


FIGURE 10-3 The flower icon in ICQ shows that people on your contact list are online.

- **MSN Messenger** If you already have an Microsoft .NET Passport account (for MSN or Hotmail), download the client (<http://messenger.msn.com>) and sign in with your MSN or Hotmail e-mail address as the user name (unlike with AIM, include the @hotmail.com or @msn.com of your e-mail address in the login field). If you don't have an account, head to <http://find.pcworld.com/43040> to get one first.
- **Yahoo Messenger** If you don't already have an account with Yahoo, you have to register on the web site at <http://find.pcworld.com/44360> first, and then download and install the client (<http://messenger.yahoo.com>). Otherwise, just download the client and use your Yahoo sign-in name and password.

Did you
know?

One Instant Messaging Client Is Better Than Two (or Three or Four)

The big guys in IM—AIM, ICQ, MSN, and Yahoo—run their own IM service as well as make the client application you'd use to send and receive messages. But not all chat services have their own client software, and if they do, sometimes you may not want to use it. If you want to talk to someone who uses one of those services, but you don't have a client, consider an *aggregator client*, which can connect to more than one IM service at once.

What are some of these services? Jabber (www.jabber.org), for instance, boasts support for its IM service in 85 separate IM client applications (including the three listed next). Gadu-Gadu (www.gadu-gadu.pl), a service based in Poland, has its own client application—but unless you read Polish, you may have a little trouble using it. Zephyr and SILC, used primarily by universities and businesses, are two IM services that are more secure than those offered by “traditional” IM.

The advantage of using aggregator clients becomes pretty clear when you have groups of people you want to IM with who use different services: one application is all it takes to be able to talk to virtually everyone you know. Once you start using an aggregator, you'll probably never look back at first-party clients again.

Get Aggregator Clients

Each of the following IM clients will let you log onto two or more IM services at once and use one application to chat with people who use different services.

- **Gaim** The Gaim client (available from <http://find.pcworld.com/43042>, see Figure 10-4) can communicate with users of virtually all IM networks, as well as with Internet Relay Chat (IRC). In fact, the only service it doesn't support (at press time) is one called Trepia.
- **Miranda IM** Miranda's client (download from <http://find.pcworld.com/43044>) supports all of the major instant messaging services, in addition to IM over the Jabber, Gadu-Gadu, Tlen, and Netsend networks, as well as IRC.
- **Trillian** Cerulean Studios makes a free multiprotocol IM client (Trillian Basic) and sells a more feature-rich client (Trillian Pro) for \$25. (Head to <http://find.pcworld.com/43046> to download either one.) Like Miranda and Gaim, Trillian can send messages to and receive messages from all of the major IM networks and IRC.

Stop Viruses, Trojans, and Worms

No matter which IM service you use, you may receive messages that contain links to web sites that will attempt to load spyware or a worm onto your PC. Occasionally, you may also get an unexpected message that someone who doesn't normally send you files through the IM network is trying to transfer a file to you. These are the two most common vectors for malware that attempts to infect your PC through instant messaging.

Worms and viruses, as you should already know, are serious business. More and more frequently, these malicious programs are being used to steal information that can be used to steal real money or buy real products using your credit or banking information. In the worst cases, these programs can leave your computer under the complete control of someone else, who can remotely use your computer over the Internet to send out more worms or even spam—a tremendously bad thing for everyone involved (except the spammer, who is thrilled that he doesn't have to use his own Internet connection to flood the 'net with junk).

Avoid These IM and Chat Activities

Engaging in certain kinds of activities over instant messaging can land you in hot water and result in a serious breach of your PC's security. In most instances, you can mitigate these risks simply by changing your habits. For example, when someone

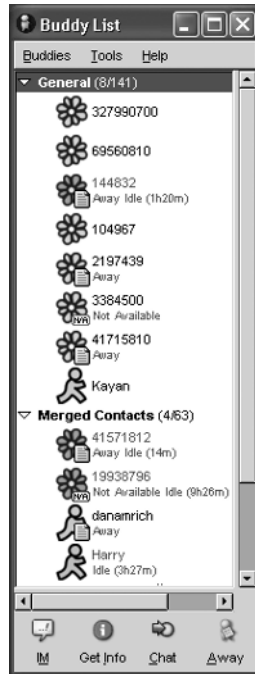


FIGURE 10-4 Gaim can connect you, within one application, to friends who use several different IM networks.

unexpectedly IMs you a link, rather than just clicking the URL, first send a message back to the person, asking what's at the web site they just sent you a link to. Try to break the following bad IM habits, if you have them:

- **Don't click links unless you know exactly where they lead** We can't stress this enough: If you click a link, it could take you anywhere, including a web page that hosts spyware and/or worms, which could take over your computer before you knew what happened. Some of these files can install themselves without your knowledge, when you browse to a web site that hosts them. Internet Explorer is the browser that's most vulnerable to these kinds of malware attacks; to protect yourself, set an alternative web browser, such as Mozilla (www.mozilla.org), to load as the default web browser when you click a link (see "Did You Know? There Are Alternatives to Internet Explorer" in Chapter 5).

- **Don't open file attachments before you check 'em out** In this case, we're not talking about a situation like one where you ask a colleague to send you some work files, and the colleague sends them via IM. In that case, you know exactly what you're getting. Don't double-click the *unexpected* attachments—at least, not until you've contacted the sender to find out what they are, and also not until you scan the file for viruses. (We'll cover how to do this later in the chapter.)
- **Avoid IM automation** You can set up some instant messaging clients to always accept files from certain people, without asking you, as soon as the other person sends the file. In general this is a bad idea, since someone could (inadvertently) send you an infected file while you're away, and when you return, you might forget to virus-scan the file before you open it. If you plan to use this feature, be extra careful, and be sure to set up your antivirus client to scan any files you receive. (We'll show you how to do this later in the chapter.)
- **Deny stalkers your personally identifiable information** While it can be fun to create an online profile of yourself, never include any location information more specific than the city in which you live; don't give out your so-called vital information (your birth date or age, phone number, car license plate, or Swiss bank account number); keep your "real" e-mail address to yourself (use a free web mail address instead); don't include the name of the school you attend or business where you work.

Did you
know?

You Should Take Special Security Measures in IRC

Invented in 1988, Internet Relay Chat (IRC) is one of the most widely used chat mechanisms in the world (we call it a mechanism because IRC isn't run by one company). With a wide range of free client applications available and an open system that permits anyone to host a chat server, IRC's popularity and utility far exceeds that of any other well-known chat system (such as AOL chat) on the planet.

But IRC's openness can also lead to problems. Depending on the client application you use, and the server you connect to, you may inadvertently release information about yourself, or files on your computer, to strangers. And strangers can take advantage of known vulnerabilities in certain versions of IRC client applications to infect your computer or steal information from you. Of course, if you know what to look for (and what to avoid), you can prevent harm to your computer and enjoy the benefits of IRC.

One of the most popular IRC client applications for Windows, mIRC (www.mirc.com) is a shareware program supported by dozens of volunteer programmers and experts. The program boasts one of the largest (if not the largest) number of downloads of stand-alone IRC clients and features sophisticated automation and scripting functions. However, unless you're an advanced user or *IRC scripter*, you'll want to turn off many of these functions to protect your PC.

- **Disable DCC functions** Direct Client-to-Client (DCC) allows one IRC client to communicate directly with another client. Users can send or receive files from one another, operate a *file server* that lets others browse files on one person's PC, and in some cases, send commands directly to the operating system via the mIRC client. Press ALT-O (or click the Options icon, a folder and hammer image, on the toolbar) to open the Options dialog box. Scroll down the Category pane and click the plus sign next to the Other option to expand it, and then select Lock. Fill in all four check boxes bounded by a box labeled Disable: Send, Get, Private Chats, and Fserve. Also, fill in the check boxes just underneath, labeled Disable Commands: /Run, /DLL (see Figure 10-5).
- **Don't give out your real name and e-mail address, ever** When you first install mIRC, it asks you to enter a "Full Name" and e-mail address into the Connect dialog in the Options dialog box. The real name and e-mail address are visible to anyone else on the IRC network, so unless you crave spam or want to open yourself up to potential fraudsters or stalkers, don't use real information in either field. We recommend that you enter fake data in both places.

- **Limit the Identd server** Some IRC networks require the mIRC client to submit a little information about itself before they will allow the client to connect. These requests, called *Idents*, are not harmful, but the component of the IRC client that responds to them, the *Ident daemon* (or just Identd), can be abused by malicious hackers if you leave it running all the time. To avoid that, make sure this option is enabled in mIRC's settings: Open the Options dialog box in mIRC, expand the Connect category in the left pane, select Identd in the left pane, and in the right pane fill in the Enable Only When Connecting check box.
- **Stop mIRC from launching the browser** You may mean well, but sometimes accidents will happen, and you may click a link you didn't intend to. You can turn off mIRC's ability to launch the browser and load URLs by opening the Options dialog box, expanding the IRC category in the left pane, and clicking Catcher. Make sure the two check boxes labeled Open A New Window and Activate The Window under the Web Browser heading are unchecked.

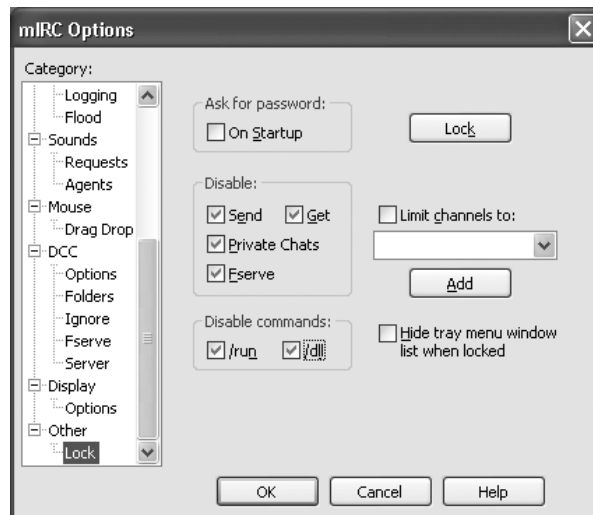


FIGURE 10-5 Turning off all the file sharing functions in mIRC is the safest way to chat.

Prevent Spim from Reaching Your IM Buddy List

With spam filters for e-mail clients improving, and some Internet providers (as well as the government) taking legal action against spammers, a growing number of junk mailers are turning to instant messaging to get the word out about their sleazy wares. Analysts at Ferris Research estimate that spim (spam over IM) messages will number about two billion by the end of 2004. According to David Ferris, the president of the research firm that bears his name, that volume is four times the previous year's total.

Many spim messages tout pornography or fast-money schemes and include a link to a web site. Following that link can trigger an avalanche of other privacy and security problems: You may get swamped with pop-up ads, or spyware and Trojan horse apps may install themselves on your PC. And spim can be even more intrusive than spam. Just like a regular IM message, spim can pop up in a chat window on top of whatever you're working on at the time.

Fortunately, all major instant messaging applications let you limit or eliminate spim, but the settings that block it require you to make some trade-offs. One-off messages from people not on your contact or buddy list—including messages from people you might want to talk to—will be blocked. You'll still be able to add users to your buddy list, but it'll take a few more mouse clicks.

The downside, however, is that many of the aggregator or multiprotocol clients, such as Trillian or Miranda, don't let you change the privacy settings you probably will want to modify for yourself. If you use Gaim, Miranda, Trillian, or another multiprotocol client, you'll probably have to install the first-party app, change the settings, and then uninstall the first-party app. The settings will remain as you changed them even without the first-party client installed. So we've given you the lowdown about where to find your privacy settings for each of the first-party clients described in the sections that follow.

One final note: It's a good idea to add everyone you think you may want to communicate with to your buddy/contact list before you implement the following tips. Otherwise, you might have a more difficult time adding people to your contact list, or you might miss messages set by people who you haven't added to your contact list yet.

Configure ICQ's Spam Control Settings

To block unwanted messages that come to you over the ICQ network, click the Main button and select Security And Privacy Permissions. Click Communication Events in the left pane, and then fill in the radio buttons under either the yellow check mark icon (which limits these actions to users on your contact list) or the red X icon

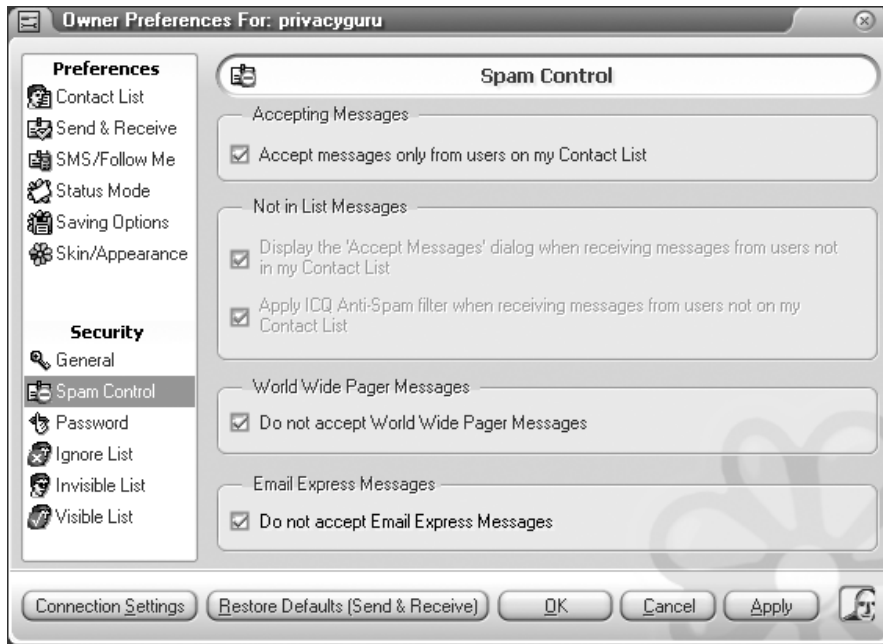


FIGURE 10-6 ICQ gives the user a lot of privacy choices, including the ability to block messages from people you don't know.

(which prevents anyone—including people you know—from sending you these things). Click Spam Control in the left pane, and fill in all the check boxes in the right pane (see Figure 10-6).

Configure MSN Messenger Privacy Settings

Once you're logged into MSN Messenger, click the Tools menu, select Options, and then select the Privacy tab. Fill in the "Only people on my Allow List can see my status and send me messages" check box. The Privacy tab also has controls for adding or removing people on the Allow List, as well as a button that lets you see which other MSN Messenger users have added you to their contact list.

Configure Yahoo Messenger Privacy Settings

Click the Login menu and choose Preferences. Select the Privacy item in the left pane of the Yahoo Messenger Preferences dialog box, and choose Ignore Anyone

Who Is Not On My Friend List. To prevent spim through Yahoo's web interface, choose "Do not allow users to see me online and contact me" in the When People See My ID On Yahoo Web Sites section.

Configure AIM Privacy Preferences

Press the F3 key (or click My AIM | Edit Options | Edit Preferences) to open the Preferences dialog box. Select Privacy in the left pane, and then choose the "Allow only users on my buddy list" option under the Who Can Contact Me header.

Update Your IM Client when New Software is Available

Updating your instant messaging client software is an important step to safeguard your computer. Updated versions prevent hackers from abusing weaknesses in the security of older, outdated IM clients. Invariably, companies release updates to their IM clients from several times a month to several times a year. A few companies automatically update the clients with new versions when they become available.

Update Primary Clients

Sometimes, the IM services make an effort to announce major upgrades to clients, but you can't always count on that happening every time a new version is released. In some cases, you'll need to head over to the web site for your preferred client(s) periodically and check if there's a new version. Here's what you need to do to make sure your client is up to date.

- **AIM** The AIM client automatically downloads updates for itself. There are two kinds of updates you can choose to get: final releases and *beta* releases. Beta releases are not-fully-baked new versions; they may add new features, but some might not work perfectly. Final releases are the most secure, fully functional copies of the software. While logged into AIM, press the F3 key, click Sign On/Off in the left pane, and make your choice (either Final Release, or Beta and Final Release) in the Auto Upgrade drop-down menu shown in Figure 10-7.
- **ICQ** Once you've downloaded and installed the ICQ client, the ICQ service will send you a special message when you can get updates to the client application. These messages will contain a link right to the update, so you won't have to go looking for it. When you get one of these update messages, you should download the update right away.

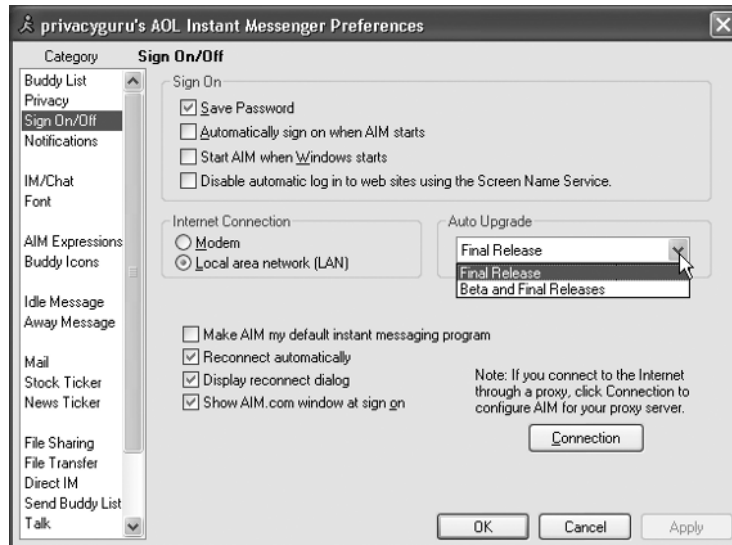


FIGURE 10-7 Choose Final Release if you want AIM to automatically update itself with the most stable version.

- **MSN** There isn't any obvious auto-update feature built into MSN Messenger, though you might get a system message when a new version is available to download. Check your current version (click the Help menu and select About MSN Messenger), and then head to the MSN Messenger download site (messenger.msn.com) to see if there's a newer version available.
- **Yahoo** The Yahoo Messenger client (which sometimes calls itself the Yahoo Pager) automatically updates itself, and there are no settings you can, or need to, change to make this happen. Once you've installed the client, it'll take care of the rest.

Update Aggregator Clients

Most third-party clients get updated more frequently than do first-party clients. These tools tend to add new features more often, and the developers often need to update these programs to ensure that they continue to work well with each of the

IM services they support. The only problem is that few third-party clients will automatically download updates. That means you need to periodically check the web site for the client you use to make sure you still have the latest version.

- **Gaim** While there aren't a huge number of updates to Gaim, you will need to check back with the Gaim web site from time to time. The client application doesn't offer any sort of automatic download of updates.
- **Miranda** The Miranda IM client doesn't have an automatic update feature, but the developers post announcements of new releases or updates on their message board (<http://find.pcworld.com/43048>).
- **Trillian** Trillian doesn't alert users of its free client that there are updates through the client, but you can expect to see them every two or three months posted on the front page of that company's web site. Head to <http://find.pcworld.com/43050> to check for updates about every three months.

Preserve Your IM Settings, Contact Lists, and Conversation Logs

Logging your instant messaging client helps you remember the details of past conversations—but they're only useful as long as you keep track of them. When you need to back up your computer, you'll want to keep a copy of your IM client's settings, your contact lists, and these conversation log files, so you can have a smooth transition and not need to set up everything the way you like it from scratch. The following sections describe how you can accomplish these tasks.

Back Up Your Contact List and Settings

Every instant messaging client (and mIRC for chat) stores its settings locally on your hard drive. IM clients also store your buddy list/contact list on the hard drive. Usually, you can find the location of these files in the C:\Documents and Settings*(your login name)*\Application Data\ folder, inside a folder named for your instant messaging client. A few programs, like mIRC, store settings in the folder where you installed the program (in mIRC's case, in a file called settings.ini).

Anytime you back up your critical files, you should back up these settings and contact list(s), in case you ever need to reinstall the client software or if there's a hard drive disaster and you lose your data. Backing up the contact list also can

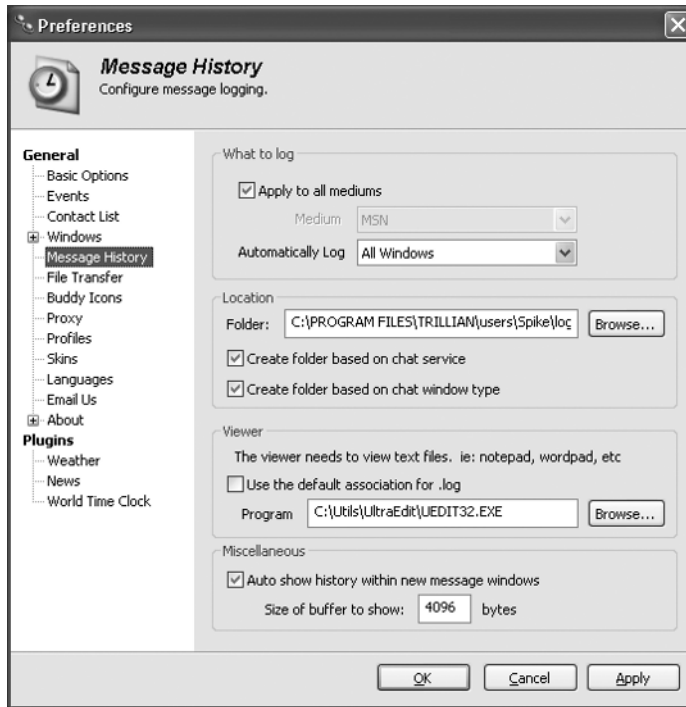


FIGURE 10-8 Trillian gives you a lot of options when it comes to logging chat sessions.

help if you want to use the same client software on another computer, or in case you delete a contact's name accidentally. Some programs, like Trillian, give you a lot of options for keeping logs (as shown in Figure 10-8).

Determine If You Need to Log Your Conversations

Most people find it handy to log the past 50 or so messages in an instant message conversation. If your boss sends you a link to an important work file, and you close the message window before you get the file, the message will stay in the *message history* or *message log* window for a while.

Some businesses require their employees to keep logs of all business-related conversations held in an IM client, in order to comply with laws governing certain kinds of financial transactions. In that case, you'll need to open the settings or preferences dialog for your specific client, find the log settings, and make sure the program keeps your logs indefinitely.

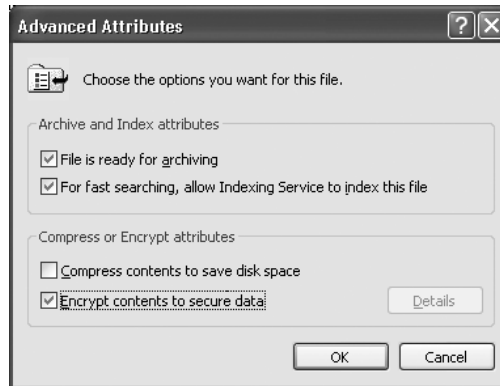


FIGURE 10-9 Compress folders containing IM or chat logs into Zip files, and then use Windows XP's encryption to protect those files from snoops.

Encrypt Archived Message Logs and Delete Old Logs

Periodically, you may find it useful to clear out some of your older chat logs, just to save a little space. But chat logs can contain sensitive information, so if you plan to archive those files, you'll want to compress and encrypt them, as well.

First, you'll start by compressing the files. Navigate to your logs (one of the windows in your client's preferences dialog will show you where that client stores its log files) in Windows Explorer, right-click the folder containing the logs, and choose Send To then Compressed (Zipped) Folder. The Zip file containing the logs will appear in the same directory as the original folder.

Next, right-click the Zip file, choose Properties, and then click the Advanced button. On the Advanced dialog, fill in the check box labeled Encrypt Contents To Secure Data (as shown in Figure 10-9), and then click OK twice. The encrypted file's filename and attributes will take on green lettering in Windows Explorer.

Defend Your Privacy in Chat and IM

Without question, when you use instant messaging or chat, you must defend your private information from virtually everyone. You can never truly know for certain whether someone who you chat with regularly, someone who might always seem cheerful and friendly, might be slightly unhinged. Online chat and IM attract a wide range of people, some of whom bring their real-life baggage with them into the online world.

You shouldn't think of chat and IM as a scary place where everyone is a pedophile or stalker. But just as in real life, you need to develop a form of street smarts online, that gut instinct that can help you judge a person's character. This is very difficult for some people, but it needn't be: You just need to follow some simple rules about protecting any information that can personally identify you to someone you meet online.

Who Wants Your Name?

Right now, as you read this book, many millions of people are online, chatting with one another. When you go online to chat, you place yourself not in a whirlwind of criminal activity, but into a frenzy of socializing, almost like a cocktail party with a zillion people, all talking at the same time.

But not all of these digital socialites are there for the fun. Among the hordes of people who love to chat you'll find a few lowlifes: criminals, creeps, nosy Nellies, weirdos, and a whole host of other people who—believe me—you don't want to get involved with. For some, it's all work: some want to separate you from your hard-earned money; others might want to infect your computer with spyware, which earns them a few cents.

Who are these folks? We can categorize them into a few general classes of shnooks:

- **Scammers and identity thieves** They will do whatever it takes to get you to click a link to their web site, where they can fool you into giving up a credit card number or bank account login name and password.
- **Spyware goons** They will tell you about some great new game, or cool tool, but the file they send you won't be either—it'll be a piece of spyware, which will infest your machine and cause you a lot of grief.
- **Spam zombies** They aren't real people but computers that have been infected with a worm or Trojan horse and want to send you a file that'll do the same to you.
- **Chatbots** They are software programs that respond to conversations as if they were real and ask probing questions you don't want to answer.
- **Screen scrapers** They don't care who you are, but if you type your e-mail address in a chat room, they'll pass it along to spammers within minutes.

They all want the same thing: your personal information. All you have to do is not give it to them—simple as that.

Apply Common Sense Liberally

Joining a chat room isn't necessarily an activity that's fraught with peril, if you know how to handle yourself. Here are some common sense guidelines to follow if you're interested in chatting or IMing:

- **Don't assume you "know" someone you chat with regularly** Even if you've talked to the same person for months on end, that person may not be who they make themselves out to be. Men pretend to be women, and vice versa; children pretend to be adults. Unless you know someone in the "real world," don't assume the other person is being completely honest with you.
- **Watch out for social engineering** Most people respond sympathetically when someone asks for help online. Unfortunately, the people asking for help might be trying to worm their way into your business, ingratiating themselves through flattery or deceit. Sometimes they pose as someone you know, or they might toss around the names of people you may have mentioned previously, and try to pass themselves off as a friend of your friend.
- **Never give anyone your passwords** Anyone who tells you they work for "the company" who runs your IM service or chat system, and then tells you they need your password for some sort of service call or to fix something, is shoveling a steaming pile of baloney in your face. Laugh it off, and then report them to the real company employees.
- **Think before you type** If you mention the name of your employer, or school, you might be giving the other folks in the chat too much information. When asked about what you do, where you live, or anything else that could let a potential weirdo find you and follow you around, just give a vague answer. You're not on a witness stand, you know.
- **You don't know who's reading over their shoulder** You might know every person in a chat room, but you don't know if they are alone in their rooms. Assume you're standing in a crowded bus station; don't say anything aloud you wouldn't want that sleazy guy who's standing in the corner staring at you to hear.
- **Hide your IP address** If a malicious chatter gets annoyed, they might decide to launch hack attacks against your computer as retaliation—but many chat and IM services hide your real IP address so hackers can't do that. Never tell people what your IP (Internet Protocol) address is, even if they tell you they need it. They don't.

- **When in doubt, don't give it out** If someone's being persistent about wanting to know your age, sex, or location, that should raise a red flag. Sometimes these people sleazily use the initial letter of each of those three pieces of vital data as a question, as in "A/S/L?" Tell 'em to take a cold shower.

Should You Create a Personal Profile in Your IM Client?

Most first-party IM client software allows you to create elaborate online profiles of yourself, most of which can be viewed, searched, and browsed by any other user of the service. Not only does this create a huge market for scammers and identity thieves, but pedophiles and other kinds of stalkers don't even have to exert any effort to build a dossier on you if you give them everything they need on a platter.

Among the items of information you could put into a profile, you can publish: your home and work mailing addresses; any number of e-mail addresses and phone numbers; your birthdate; details about your interests, hobbies, and educational background; your photograph; and links to your personal web site and the web sites you frequent. Many IM services (like ICQ, shown in Figure 10-10 below) also allow you to also create free-form bios of yourself and publish those along with all this other information.

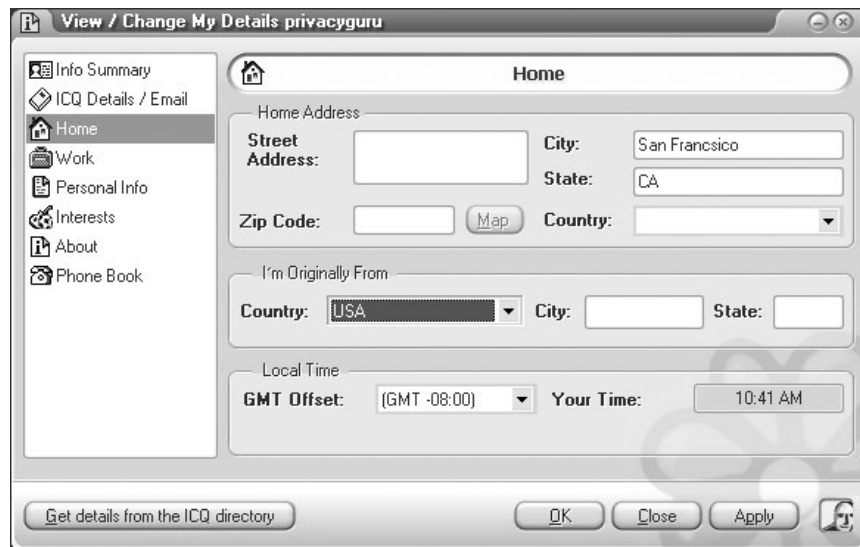


FIGURE 10-10 ICQ lets you create an entire dossier about yourself, all of which becomes publicly available as soon as you click OK.

You have to wonder what planet people are living on when they fill out questionnaires with all this unbelievably sensitive data and publish it all online. It's almost as if they've been living under a rock the past several years, while the crime of identity theft has turned into the number one white collar crime in the world. In general, creating a profile is a bad idea. Just don't do it.

Handle Chat and IM Security Issues

Chatting safely in IRC or IM takes just a little smarts. Knowing what you can and can't do isn't always obvious (though after you've finished this chapter, you should be a pro), but the steps aren't too hard to follow. The three things you need to be careful about are making sure to scan any files you download for viruses, not blindly clicking links people post in chat rooms or send you in IM messages, and not divulging information about yourself. See, I told you it was easy.

Avoid Chat- and IM-Borne Malware

Instant messaging and chat rooms sometimes can be vectors for *malware*—malicious software, such as viruses, worms, Trojan horses, spyware, or keystroke loggers (for more on what these things can do, see Chapter 8).

In addition, links in instant messages may take you to sites that could load spyware or worms onto your computer. But you don't have to stick your head in the sand, just take some simple precautions.

Download Files Safely over IM

When is it safe to have folks send you files? The answer is, it's usually pretty safe. The only time people get into trouble is when they haven't developed smart habits and practices that keep them safe. For instance, you should *never open a file immediately after someone sends it to you; always* run it through a virus scan. A ten-second scan could save you hours of hassle trying to rid your computer of a nasty bug. In the long run, it's gotta be worth it.

Another rule that's got to be set in stone is *never accept files from people you don't know or aren't on your Buddy List*. Sounds simple, right? It is, if you have your IM or chat client set up correctly. In fact, if you set this up right, you won't even see the file someone's attempting to send you, because your client will know better than to download it. And for those files you want to receive, set up your client to save them to a folder (as shown in Figure 10-11) where your antivirus program will always scan the incoming files.

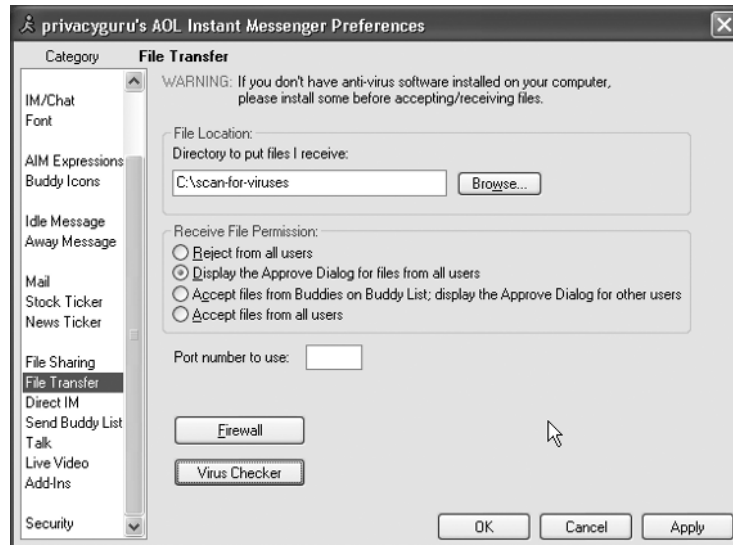


FIGURE 10-11 AIM lets you decide which incoming files you want to accept and where to save them.

Finally, and probably most importantly, you need to install a modern, up-to-date software firewall and antivirus package *before* you accept the first file from anyone (not to mention, you need to *keep current with your antivirus updates*). We can't stress this enough—these two programs are your computer's first (and sometimes only) line of defense against some pretty nasty malware.

Once you've done that, you can configure your IM client so it launches your antivirus program any time you download a file (as shown in Figure 10-12) and scans the newly downloaded file for viruses. It's not enough just to have antivirus software installed, you must set up this automatic scanning on each IM client you use.

Configure Antivirus for Chat and IM

Instant messages can spread viruses or worms as easily and quickly as they can send messages or files. Several IM clients have special settings within their overall program preferences that can launch your antivirus software to scan any files sent to you through the IM service. But even clients that can't launch your virus scanner can be set up more safely, by saving all downloaded files to the same place and then setting your virus software to scan that place on a regular basis.

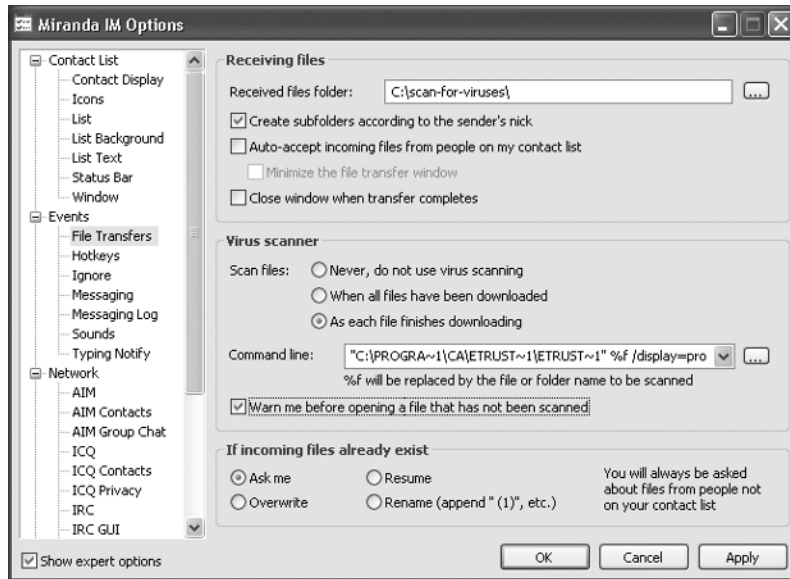


FIGURE 10-12 You can set up most IM clients, such as Miranda, to trigger your antivirus program to scan downloaded files for viruses as soon as you get them.

For instance, the AOL Instant Messenger software has a special Virus Checker setting (shown in Figure 10-13), which you can use to tell AIM where your antivirus software is located on your hard drive. (To find the setting, press the F3 key, click File Transfer in the left pane, and then click the Virus Checker button in the right pane. Use the Browse button in the Virus Checker dialog box to navigate to where your antivirus software is installed.) When you receive a file from someone else, AIM automatically launches the virus scanner, which then scans the file.

But not all IM clients have this functionality. To protect yourself, create a folder on your hard drive where you can store all the files people send you over IM. In the example shown in Figure 10-13, we've created a folder on the top level of the C: drive named *scan-for-viruses*. Every IM client lets you choose the folder where it will save downloaded files, so go into the settings dialog box for the IM client you use, and direct the client to save its files in C:\scan-for-viruses (or whatever folder you use).

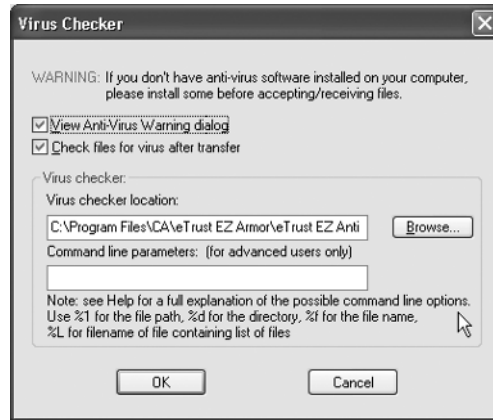


FIGURE 10-13 AIM's Virus Checker dialog lets you set up your antivirus application to scan downloaded files automatically.

Once you've got that set up, you'll want to set up a system to protect yourself. Most antivirus software can be configured to scan a predetermined folder on a schedule. Set your antivirus program to scan any files that appear inside this incoming files folder once a day or once an hour; at the very least, just scan the folder manually, whenever you get a file.

Play It Safe in mIRC

IRC has a reputation as an outlaw hub of malicious software (and the hangout of the hackers who write and use those programs). In reality, IRC is a lot more like a social club, though some unsavory types do occasionally crop up. Turning off file sharing features in your IRC client software is one way to prevent worms or Trojans from taking root on your PC. But not all infections start when an automated worm spreads itself around: Many more people accidentally infect themselves with viruses when they download and install *scripts* for their IRC client that, they think, are intended to serve some useful purpose.

An unsophisticated IRC user can get in a lot of trouble by downloading scripts, especially if that user doesn't have the foggiest idea how to check whether the script is just a Trojan horse. Scripts can help you do certain things in IRC, such as enter passwords (as shown in Figure 10-14), manage channels, play trivia games, listen to music, or mute annoying chatters.

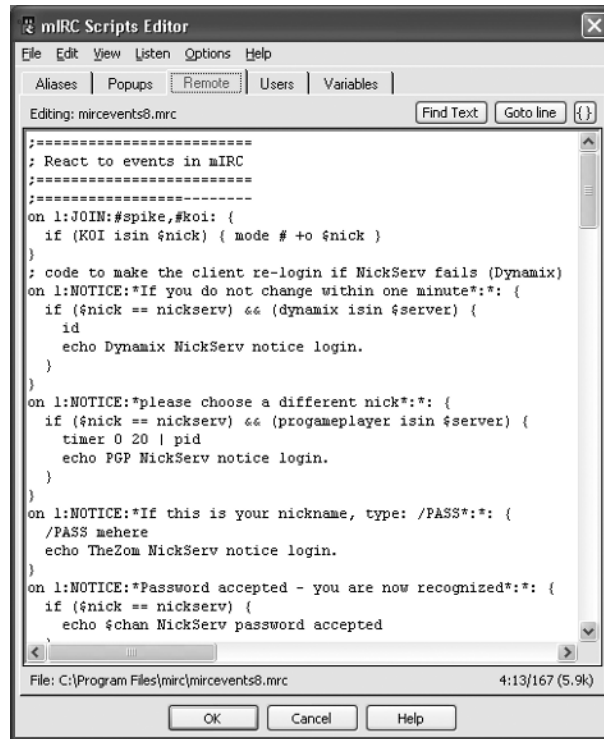


FIGURE 10-14 While most mIRC scripts are helpful tools (such as the one pictured, which enters a password automatically), some scripts can be dangerous.

There are a few common-sense rules you should follow. Don't download and install a script sent to you by another user; look first at reputable script download sites for software (<http://mircscripts.com>, <http://hawkee.com>, and <http://scripthaven.net> are three good starting points for users of mIRC); and for goodness' sake, run an antivirus scan on any script package you download *before* you install it.

In general, it's easy to spot the scripts just by looking at their names (I don't think *Virus Script* is one I'll be downloading any time soon). But you can't always count on the fact that a script with a safe-looking name is going to be safe. Stick to the add-ons and scripts on the legitimate sites, and you should do just fine.

Voices from the Community

WiredSafety's Parry Aftab: The Importance of Teaching Kids How to Chat Safely

Parry Aftab is no stranger to the risks people face when they chat or send instant messages. As the founder and director of WiredSafety.org, Aftab is an expert on the subject. Her book, *The Parent's Guide to Protecting Your Children in Cyberspace* (McGraw-Hill, 2000), is considered the authoritative tome on the subject of kids' online safety, and she's consulted with governments around the world about issues of Internet privacy and safety.

Aftab believes the paranoia parents feel over their children's online life—especially chat and instant messaging—isn't always justified, but that most parents do need to get more involved with their kids' computer use and teach their kids good cyber-street smarts.

"Parents are very, very concerned about chat. They've been frightened enough to believe that all the risks children on the Internet come from chat, and actually, that's not the case. In every case in the United States I'm aware of, instant messaging has been involved in cases where Internet sexual predators communicated and met children offline. In some cases, chat has been involved, but chat is not the bad guy some parents think it is.

"We always say we don't want kids to talk to strangers in real life," Aftab says. "When you apply that to the Internet, you lose a huge value of the Internet: allowing children to communicate with other kids or other people who can teach them things. That's what the World Wide Web's all about.

"So, instead of saying *don't talk to strangers*, we need to teach them *how* to talk to strangers. The example I use is that a child is sitting with her mother on a bus, and a lady sitting across from them tells the little girl, 'That's a lovely pair of shoes.'

"The child will look at the mother first to make sure that it's okay to talk, then say 'Thank you'—not 'Thank you *and here's my mom's credit card number she used to buy the shoes.*' And we need to teach our kids to do that online. We need to say, you can talk to people, but you don't give away personally identifiable information, and this is how it can sneak out without you realizing it, and that there are real people online who aren't everything that you think they are."

Protect AOL with Antivirus Users of America Online's Internet service are a particular target of worms and viruses, precisely because that company targets *its* services to neophyte users who may not understand the need for a software firewall or an antivirus application—or even have either of those things installed on their PCs. If you use or plan to use AOL as your Internet service provider (or even if you just use the free AIM service), you should take extra care to protect your computer.

Without exception, even if you use a dial-up AOL Internet connection, you need to use a software firewall. The free ZoneAlarm firewall (available from www.zonelabs.com) is just one of several free software firewalls you can download and install, and it will protect your computer from the minute it begins running. In addition, most suites of Internet security products, like Symantec's Norton Internet Security or Trend Micro's PC-cillin Security Suite, include a firewall with the package. Use it!

Prevent Stalking and Threats in Chat and IM

People do and say some crazy things online, things they never would do or say if you met them face to face in the supermarket, for instance. But in the world of relative anonymity that is the world of online chat, people can remake themselves in a hundred different ways.

Unfortunately, it's hard to tell when someone is merely blowing a lot of hot air, or if that threat they just made is the real deal. For a lot of people, the time they spend online is as valuable as time they'd spend socializing with people in the real world. When someone new upsets the social dynamic, it can result in disaster.

You may have heard all the stories: The 13-year-old girl who ran away from home to meet what she thought was a boy her age, only to discover the "boy" she had been chatting with online was a man in his late forties; the female author who rallied against a scam artist posing as an online book agent and was later tracked to her home by the scammer, who was arrested outside her house with a machete and a roll of duct tape. What's most important is, if you feel threatened or harassed online, take it seriously.

Who to Call If Someone Harasses or Stalks You Online

Several organizations can help you figure out your next step if someone has started harassing or stalking you online. Remember, online stalkers can quickly turn into

real-life stalkers, who could harass you at work, vandalize your property, or do much worse. If you're concerned, here are some places you can call.

- **The cops** Many police departments have detectives who work the cybercrime beat, and most U.S. states have laws that criminalize threats of physical violence, stalking (even online), or harassment. Don't be afraid to call in the fuzz. If your local department isn't giving you the help you think you need, head to www.wiredcops.org and file a report there.
- **WiredSafety (www.wiredsafety.org)** You'll find helpful advice for cases involving stalking or harassment on this site, as well as a form where you can report other serious cybercrimes, such as child abduction, child pornography, or identity theft.
- **The Justice Department's Cybercrime division (www.cybercrime.gov)** If you think you've been victimized by someone online, whether or not they live in this country, you'll find a rich volume of background research at this central repository of information about cybercrimes, and you can find out who to contact locally, if you think you're a victim.

Chapter 11

Shop and Socialize Securely



How to...

- Identify secure shopping sites
- Socialize and meet friends online safely
- Post your résumé with privacy in mind

Shop Online Safely

On the Web, you'll find some of the best bargains you've ever seen. Between mega-retailers like Amazon or travel sites like Priceline, shopping online can save you a ton of money. In fact, you can get so used to seeing (or hearing about) great bargains that, one day when your attention wavers for a moment, you could end up the victim of a bogus e-commerce site or auction fraud.

E-commerce experts often say, "If it looks too good to be true, it probably is too good to be true." It's good advice, because most victims of fraudulent sales and auctions get that way by being overcome by their own greed. They go into the deal thinking they've found a sucker who's willing to part with something for far less than it's worth, as all the while they themselves get suckered by the fraudster.

You don't have to end up like these people. Following a few safety rules (listed herein) will help keep you out of trouble as you navigate the great bazaar that is the Web.

Verify Security Before You Shop

Whether you buy something from the world's biggest retailer, or from some guy you know in Minnesota, the experience of shopping online should involve the same preliminary background checks before any money changes hands. Auctions deserve the most scrutiny, since that's where most of the trouble begins. Both eBay and Amazon auctions have a rating and user feedback system that lets buyers or sellers rate one another and leave comments. Ratings are the first place you should look. Can the other person explain away negative feedback satisfactorily? Does the person exhibit any negative behavior patterns, according to the people who gave feedback?

Auction issues are but a single concern. Many new frauds begin with so-called phishing e-mail messages, a form of spam that appears to come from an online bank or financial services business (see Chapter 9 for more about spam, or Chapter 12 for the lowdown on phishing). Following the URL in these messages can take you to a fake web site run by criminals, but one which looks like something your bank

would have created. Unsophisticated users get fooled by the appearance of the site matching their bank's page layout, but it's possible to check the security of web pages in a number of ways. Read on to learn how.

Check Out Your Auction Winner (or Seller)

According to an annual report published by the National Fraud Information Center (<http://fraud.org>), auction fraud accounts for 90 percent of Internet frauds reported in 2002, the latest year for which data is available. More than 75 percent of victims fall between the ages of 20 and 49, the average victim loses a little under \$500 in a typical auction fraud (though some people lose much more), and 13 percent (the largest) reside in the great state of California. About two-thirds of victims report they paid for a bogus or nonexistent product by any means other than credit cards, which would have offered them payment protection if only they'd used them.

Those sobering statistics (and more at <http://find.pcworld.com/43452>) make it pretty clear what you need to do—and I don't mean wait until you're over 50 years old to start using auctions. The higher the value of the item in the auction, the more you should scrutinize both the item and the other party. Check their feedback first, and try Googling their auction nickname as well. Keep in mind that some auctioneers shill their accounts—artificially raise their buyer/seller ratings by registering several user accounts at eBay, which they use to boost their “main” account's ratings—using fake auction transactions and fake feedback, so you can't always trust 'em.

Fraudsters don't just limit their activities to selling nonexistent items. Some perpetrators of auction fraud pose as buyers, “winning” auctions and then tricking you into believing that they've sent the money to your PayPal account so that you ship them the item you're selling. Always log directly into PayPal to check whether payments went through; e-mail alerts about payments are too easy to forge.

If the auction item costs more than you're willing to lose (a dollar amount that varies from person to person), look into using a legitimate auction escrow service. One such company is Escrow.com, which acts as an intermediary between the buyer and the seller in an Internet auction and takes a percentage of the sale price for its services (see Figure 11-1). Sellers send their products to the company, which records their arrival and stores them until payment arrives from the buyers. Then the escrow company forwards the sale price (less a commission) to the seller and drops the product in the mail to the buyer. If one side fails to live up to the deal, the escrow service returns the product or money to the other side.

If you're a buyer unwilling to take the hit of an escrow service's cost (and frankly, it's just not always necessary) but something in your gut tells you something about the sale isn't right, insist to the other party that you be allowed to pay by credit card

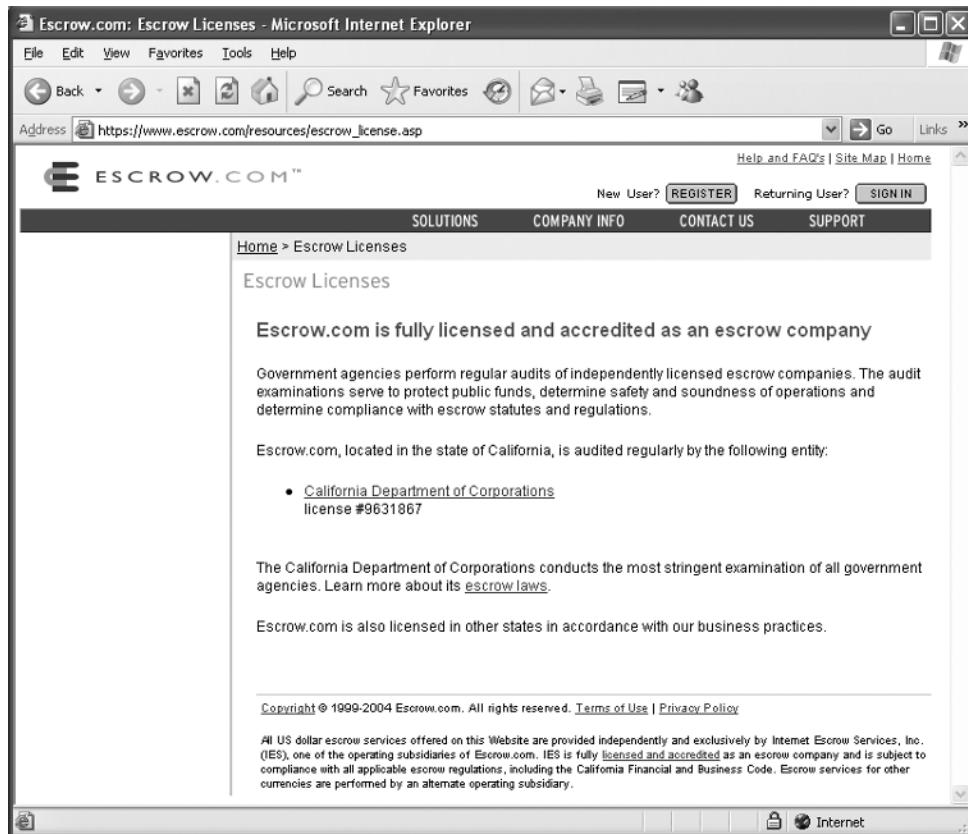


FIGURE 11-1 Escrow.com was the first Internet auction escrow service.

if the item costs more than \$50 to \$100. Most people who get victimized used a check, a money order, or PayPal to transfer funds to the seller.

For more information about preventing auction fraud, head to the Federal Trade Commission's web site (<http://find.pcworld.com/43450>), where you can find detailed advice about how to engage in safe auctioning.

Search the BBB Online for Complaints about Retailers

If you've never heard of the e-commerce site you're browsing for that great steal, be sure to give them a Better Business Bureau (www.bbb.org) search, just to see what someone else might have said about the company. Click the Check Out An

Organization link along the top of the BBB's web site, where you can look up a business or charity by name, address, phone number, or URL.

If you can't find a web site's mailing address anywhere on the site itself, run a WHOIS lookup on the domain name. (Sam Spade, the freeware tool mentioned in Chapter 9, can perform this task. Download it from <http://find.pcworld.com/43400>.) A WHOIS will give you the names and (hopefully) addresses of both the Administrative and Technical contacts for the web site, and you can then look up the address for the Administrative contact in the BBB database (see Figure 11-2).

Finding nothing in the BBB online database doesn't necessarily indicate the company's untrustworthy. But it doesn't affirm anything, either. If you can't find

BBB Information System (BIS) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://search.bbb.org/results.html> Go Links

Database Search Results

Special Note: Your search resulted in more than 50 matches. If the company you are looking for is not listed, then please narrow down your search by entering more specific information like the phone number or state and city.

The BBB logo will appear to the left of the company name if a company is a member of the BBB.

The HQ designation next to a report indicates the report is that of the company's headquarters location.

Is the company you are looking for not found in these results? Click [here](#) to search for close approximations.

1 to 50 of about 50 Matches.

COSTCO WHOLESALE #26
3801 Pelendale Ave
MODESTO, CA

COSTCO WHOLESALE #38
1616 E Hammer Ln
STOCKTON, CA

COSTCO
72800 Dinah Shore
PALM DESERT, CA

To find a BBB Reliability Report, please use the search form below to search by the business name and location; phone number; or URL.

☒ **Name:**
City:
State/Prov:
(Required if city entered)

☐ **Phone:**

☐ **Web Address:**

Done Internet

FIGURE 11-2 Use whatever information you have to search the BBB Online database.

anything at the BBB, you can Google the site's name or URL, or you could check consumer opinion sites; Epinions, at www.epinions.com, is a good place to start. Just pick Online Stores And Services from the drop-down menu next to the search bar at the top of the Epinions front page, and you can search for your company by name or URL. Sites like MySimon (www.mysimon.com) or PriceGrabber (<http://pcworld.pricegrabber.com/>) also allow customers to rate retailers and comment about their service and support.

Verify That You're Using a Secure and Trustworthy Site

There are a few key things you need to look for on any web page where you might spend money. These features should always be present; if they're not, it should raise a red flag.

- **SSL encryption** Web sites that take orders online should always present you with an *encrypted* ordering page, so thieves can't swipe your credit card number when you click that Buy button. Virtually all legit sites already support this feature, but you should always check the little padlock icon that usually appears in the bottom-right corner of your web browser to make sure. You might also see the <http://> temporarily change to <https://> in the address bar when you take your virtual shopping cart to the register. If you see that change, or if the padlock icon is closed, the page is encrypted, and you can transact business safely. If the padlock icon looks open, you run a risk if you submit a card number.
- **Published sales, return, and privacy policies** If you're dealing with a legit site, you'll find all of these things, as well as the business' postal mailing address and/or telephone number. You can use these two pieces of information to do a little digging about the company, if you're unsure whether to trust it.
- **Certified by private "seal" programs** Many (though not all) legitimate commerce sites are also members of one or more "certificate" programs with companies like BBBOnLine, TRUSTe, WebTrust, or VeriSign. These organizations certify that the business operates according to principles of fairness, and some also offer a dispute resolution service for consumers who have a problem with a member company. However, don't just accept the seal itself as proof the site is a member; clicking the seal often takes you to a page that verifies the site's business information. If you're using an unfamiliar online store, take that extra step and click the icon to make sure everything's on the up-and-up. Also, be wary if you see a profusion of these seals; some seal programs aren't worth the pixels their icon takes up on a page (you can depend on the companies just listed).

Verify a Shopping Site's Security Certificates

When legitimate shopping sites want to build a secure order form (one that can *encrypt*, or scramble, the data you enter into the form), they buy something called an *SSL security certificate* from one of a few companies known as *certificate authorities* (or just *CAs*). These certificates work with your browser to scramble your data to protect it from hackers, and they also *authenticate* the retailer (which proves that the company running the web site is who they say they are). The most obvious sign that a site is using encryption is the little padlock icon that typically appears at the bottom-right corner of your browser window, which looks like it's locked when the site is encrypting the page, and looks unlocked when it's not, as shown here:



But security certificates aren't flawless. Some fraudsters have made their own certificates, which means that when your browser is on their web site, the little padlock might give you the mistaken impression that everything's alright. If you're shopping on a site you're not familiar with, and you see the little closed padlock icon, you can check the site's security certificate and make sure it's not a fake (see Figure 11-3).

In most browsers, you can just click the little closed-padlock icon to bring up a dialog box with the details about the security certificate. But unless you're an expert, you probably won't be able to tell if the certificate is legit just by looking at it. Fortunately, one of the most well-known certificate authorities, VeriSign, issues most of the SSL certificates used by big online retailers, banks, and other large web-based businesses—and you can check the validity of the certificate on their web site. To do that, you just need to copy the certificate's *serial number* from your browser and paste it into a web form on VeriSign's web site (located at <http://find.pcworld.com/43458>). Here are the steps for IE and Mozilla/Netscape:

- **Internet Explorer** Bring up the certificate dialog box in your browser (double-click the padlock icon), and select the Details tab (see Figure 11-4). In the upper pane of that dialog box, select the Serial Number item, and then highlight and copy the string of numbers and letters (32 characters, arranged in eight groups of four characters) from the lower pane by holding down the CTRL key and hitting the C key. Go to the VeriSign page and paste the serial number into the Search By Serial Number field, but before you click the Search button, carefully delete the spaces between each group of four characters.



FIGURE 11-3 SSL certificates help browsers make secure connections, but they're not easy for non-experts to figure out.

- **Mozilla/Netscape** As with Internet Explorer, bring up the security certificate dialog in the browser (right-click the padlock icon). Click View and then the Details tab (see Figure 11-5). Highlight the words Serial Number under the Certificate Fields pane, and then select and copy the serial numbers from the bottom pane. In these browsers, the serial number appears as 16 pairs of digits, with each pair separated by a colon. As with IE, you'll have to delete anything that isn't a letter or number before you can hit the Search button on VeriSign's site, so get rid of the colons before you submit the search.



FIGURE 11-4 The serial number, as displayed in IE, has spaces between groups of four characters. Delete those spaces before you search.

Once you've submitted the check, it takes the VeriSign site only a few seconds to look up the serial number from its database. The most important parts of the certificate details that appear are the site's URL (does the URL on the certificate match that of the shopping site?) and the Status, which should always read Valid.

It's unfortunate that the browser companies have made checking the validity of security certificates such a hassle. But if you're unfamiliar with the shopping site you want to spend money at, the small amount of time spent doing this little check is well worth the effort.

Read and Understand Web Site Privacy Policy Legalese

Privacy policies, which used to be a relatively rare breed of web page, are now a standard part of almost every legitimate business' web site. The teensy link to the privacy policy (usually located at the bottom of the browser page) belies what's commonly an unfortunate mishmash of legal contract language and descriptions of various forms of technology. Most privacy policies were written by engineers and lawyers, more often because of legal requirements than a deep desire to be honest

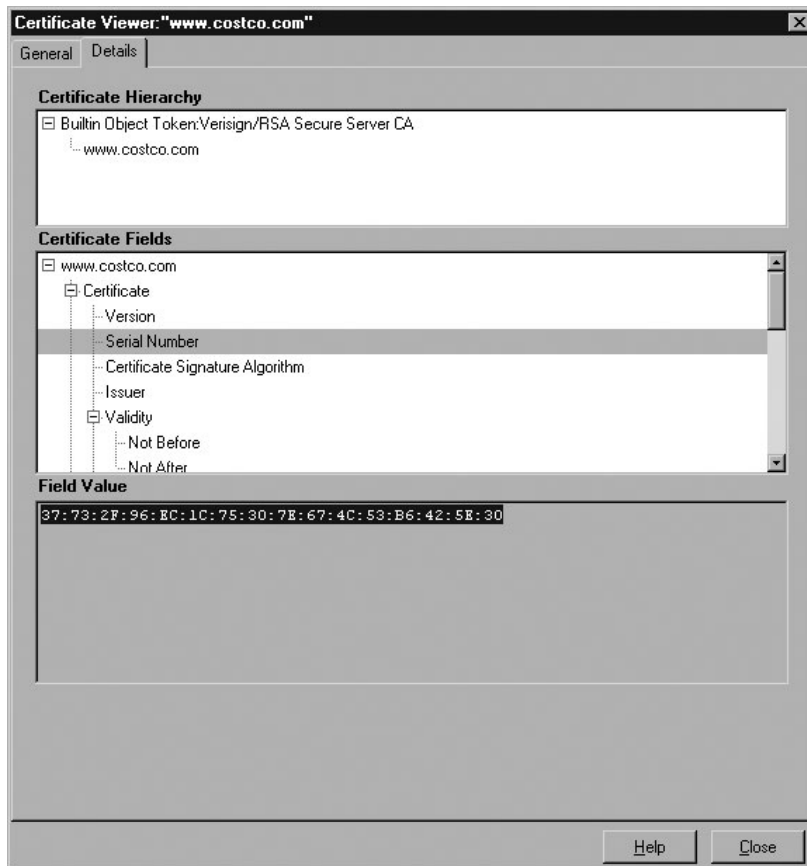


FIGURE 11-5 Mozilla displays the SSL serial number with colons between pairs of characters. Delete each colon in the search field before you submit it, or the search won't go through.

with customers; many policies read as if the company took those two groups and locked them inside a shipping container to fight it out until this was all that was left.

But it's not really safe to ignore privacy policies either. With a profusion of web sites now requiring some form of registration to browse or read the site, it's important for you to understand what the company will do with the information you provide them, and what steps you can take to protect your privacy. And just because a policy exists, that doesn't mean the policy will protect you. After all, a company could make a privacy policy (albeit a really nasty one) that says they will sell your name and personal information to anyone who wants it.

Learn the Lingo of Privacy Policies

Sure, your favorite web site might post a privacy policy, but that doesn't do you any good unless you actually read it. Here are a few things to look for as you're slogging through the legalese:

- **What's collected** You can always assume that sites that require registration also archive all the information you enter in a registration form. If a site uses cookies to track you as you move through its pages, those cookies could tell the company exactly what you're reading, how long you stay on a page, where you came from before visiting their site, where you went afterward, and other statistics. If a site's privacy policy admits that the company sells data collected through cookies, user registration, and other kinds of tracking such as web bugs, make sure it also says that the company uses the data in the aggregate (stuff like statistics, that doesn't include your personal information), which means marketers don't ever get data about you personally.
- **Business relationships** If a site you use frequently is a division of a larger company, it's safe to assume the two divisions share data. Sometimes two or more otherwise unrelated companies make business deals to share some or all of the information users give when they register. Again, it's important to note whether they share data in the aggregate or if they transmit personally identifiable information about you, such as your user name or e-mail address. Sites may also sell your e-mail address to spammers, though they sometimes do this unintentionally. Usually you can check (or uncheck) a box indicating you don't want to receive offers from partner companies. Or you could use a free e-mail address (that you don't use for anything else) just to register at web sites.
- **Security of stored data** If a shopping site lets you keep a credit card number on file, it's not enough to have the information encrypted as it travels from your computer to theirs. Electronic-commerce companies also need procedures in place to protect sensitive financial data stored on the servers. If you shop online, look at how the online retailers you deal with protect your stored information. If they don't mention it, e-mail the webmaster to find out. If you don't get a satisfactory response, take your business elsewhere.

Use Tools to Help You Match Policies to Your Preferences

More than two-thirds of Internet users, in a July 2003 *PC World* survey (<http://find.pcworld.com/42124>), said they read or skim the privacy policy of a web site at

least some of the time. The majority of those who didn't read the policy complained that the policies are too long or complex, or that they didn't understand what the terms in the policies meant. If your eyes glaze over after the second paragraph of a privacy policy, you're not alone. But reading those policies is still pretty important. Fortunately you can use browser settings or small software programs to help you sort through the legal mumbo-jumbo of privacy policies and make sure sites adhere to your preferences.

A couple of years back, some very smart people crafted a way to turn these complex legal policy documents into a code that software could read and interpret. The code, called the Platform for Privacy Preferences (or P3P), allows the companies that make web browsers to build tools into the browsers that can control how much information a site can get about you.

Internet Explorer, starting in version 6, integrated a Privacy tab into the Internet Options dialog box (click Tools | Internet Options), which gives you some control over cookies (see Figure 11-6). Mozilla and Netscape (click Edit | Preferences) let

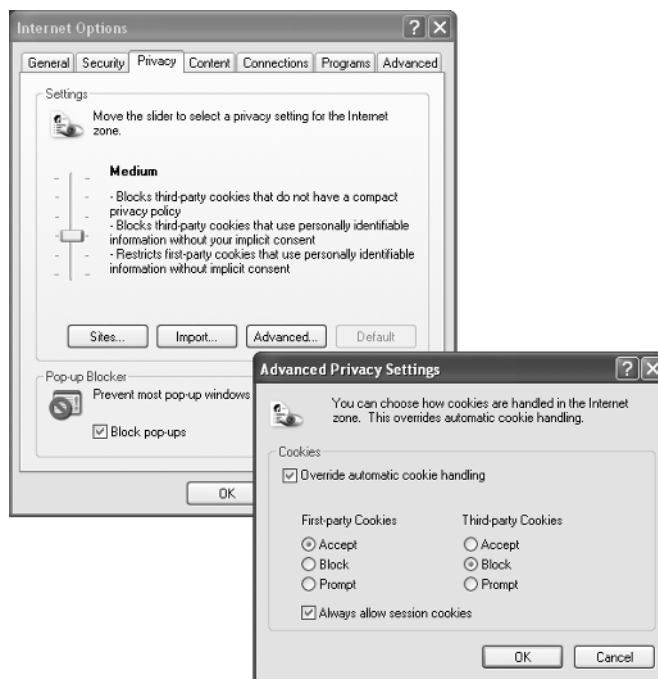


FIGURE 11-6 Internet Explorer's Privacy settings let you block some kinds of cookies while allowing others.

you control not only cookies but also pop-up windows and images that come from advertisers.

But you get real awareness over every aspect of a site's privacy policies by using software called *user agents* to keep tabs on the policies, and make sure they mesh with your own preferences. Two great, free user agents to try out are AT&T's Privacy Bird (<http://privacybird.com>) and IDcide's Privacy Companion (<http://find.pcworld.com/43460>). These tools (both for Internet Explorer only) put tiny, easy-to-understand icons into the IE window that let you know how privacy-invasive the site is on any given page.

For example, when you install Privacy Bird, you'll notice a rectangle about an inch wide that occupies the right side of the browser's title bar. The rectangle turns red and the bird icon flaps angrily when a site's privacy preferences don't match your own (you enter your preferences into Privacy Bird first), but it chirps cheerfully and the bar turns green when the site you're visiting doesn't take more information than you might want it to do.

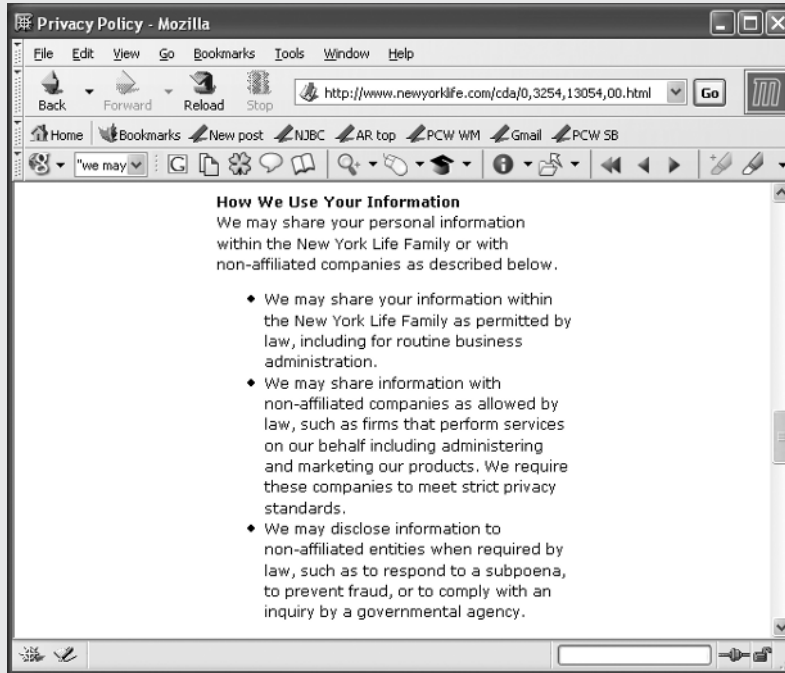
Did you
know?

Most Sites Don't Know When You're Unhappy with Their Privacy Policies

In the July 2003 *PC World* privacy survey we mentioned earlier in this chapter, 72 percent of those surveyed indicated that, if they didn't approve of or agree with the privacy policies of a web site, they wouldn't use that site. Bravo for those people, because they really *grok* the purpose of a privacy policy. But to the operators of a web business, it's impossible to know why someone would visit their site and leave. Maybe the prices weren't good enough, they might surmise. Perhaps the selection was better elsewhere, or the web visitor might have been just doing research, but wasn't ready to buy.

But those visitors also might have left the site without buying anything as a result of the visitors' objection to the site's privacy policies, and the site's owners wouldn't have a clue. In the survey, only four percent of the participants said they'd decline to use a site *and* complain to the site's operators if they didn't agree with their privacy policies. The operators of some web sites tend to cry ignorance when customers challenge some invasive change to the site's privacy policy. We haven't received many (or any) complaints, they almost always say.

Most people who object to a privacy policy don't complain, because it's just so easy to close the browser window and go somewhere else. But unlike walking out of a brick-and-mortar store in a huff, the act of leaving a web site gives the site's owner no useful information. The solution: let the operators of a web site know *why* you didn't choose to buy something there.



Most web sites have a general feedback link, a Contact Us page, or some other form of a virtual suggestion box where you can express your objections to their privacy policy. While it's easier just to surf somewhere else to shop, if enough people let web shopping sites know about their privacy concerns, those complaints can convince the proprietors of a web business to change their privacy policies—and that could benefit everyone who uses that site (you included), in the long run.

Compose an Effective Privacy Policy Complaint

If you're feeling bummed out about the privacy policy at a shopping site, let the operators of the site know how you feel. Here are a few tips that will help you craft a successful and effective complaint about a privacy policy:

- **Keep it short and to the point** Many web feedback forms let you enter only about 1,000 characters, which means you can write about 200 words, on average. Just get right to the point.
- **Be polite** How would you feel if you were the guy or gal reading the suggestion box e-mail, and came across a rude or profane message? Your message is more likely to be taken seriously if you clearly explain what you don't like, and leave out the part where you tell them their privacy policy makes you so angry you could pull someone's head off. Follow the golden rule, and remember Grandma Bubby's advice: You'll catch more flies with honey than with vinegar.
- **Be specific** Do you object to the part where the company says they'll share your information with their partners, without naming either the information they'll share or the names of the partners? Say so! If the policy has numbered paragraphs, cite the specific number of the portion of the policy you object to. Otherwise, quote the exact line(s) of the policy you object to (keeping it really short) in the complaint.
- **If you were writing the policy, how would you write it?** Let the folks at the company know how you'd do things differently, if you were in charge. Do you think the company shouldn't share data with partners? Say so. Leave out the part about how, if you were in charge, the company would give a million dollars and a pony to people who write really good complaints about their privacy policy.

Protect Your Credit Cards Online

Virtually all online merchants accept credit cards for payment, making your card number the linchpin of your ability to shop online. While we go into the topic of preventing identity theft (which includes the theft of your card number) in greater depth in Chapter 12, it's worth noting in this chapter about shopping that there are a few online services that can help you protect your credit card number when you shop online, and card-issuing banks also take steps to prevent someone else from using your card number without your permission.

Credit Card Fraud Prevention Services

All four of the major credit card companies offer some form of fraud prevention service to their customers, though not all companies offer all (or exactly the same)

services to all their customers. Sometimes you need to have a specific card, or (in the case of Visa and MasterCard) the card-issuing bank needs to be signed up for the service in order to offer it to cardholders. Here are some of the services the major companies offer.

- **American Express** If you have one of American Express' new(ish) Blue cards, the company sends you software and a special card reader you can plug into your PC to shop online. The card's embedded Smart Chip can also store URLs and login usernames and passwords to e-commerce sites, using the free ID Keeper software you get with the card.
- **Discover** With the Discover Deskshop you can generate a *single-use card number* every time you want to purchase something online (see Figure 11-7). You would enter one of these special numbers in an online order form just as you would your regular card number, except they can be used only for the exact amount you specify, and (duh!) only once. You can use Deskshop by means of a stand-alone Windows application (you can download it free from www.discovercard.com/deskshop) or by using an online version hosted on the Discover card web site.
- **MasterCard** Besides offering zero liability for online purchases, MasterCard has SecureCode (www.mastercard.com/secured), which lets you create a password that you have to enter (in addition to the card number) when you fill in the order form at a participating merchant's web site. The only problem: At press time, fewer than twenty companies are participating in the program.

**FIGURE 11-7**

Discover's Deskshop application automatically fills in order forms with your name, address, and card information.

- **Visa** The Verified By Visa program works just like MasterCard's SecureCode; once you create a password through the program, you'll be prompted for the password every time you submit an order form on a participating online shop. The differences: You can sign up for the Verified By Visa program from any participating site as you're doing the checkout portion of your online purchase (MasterCard requires you to sign up on their web site), and at press time about 240 companies support the Verified By Visa program.

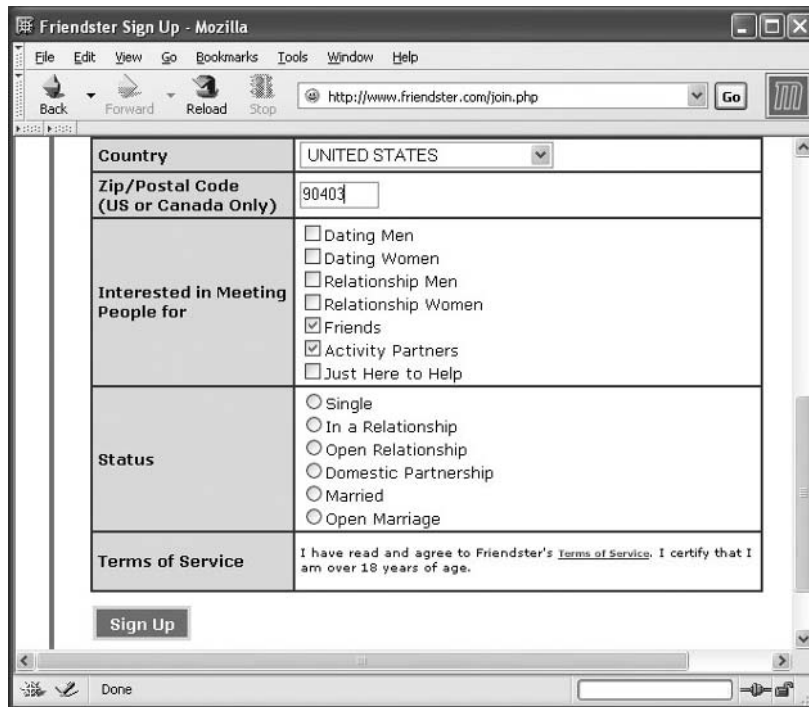
Safely Socialize Online

Back in Chapter 10, we told you about the applications you can use to chat and send instant messages. But being social with other folks over the Internet doesn't just involve specialized software: web sites where people find others with similar interests are all the rage. Some of these are just online versions of personals ads (which you can find almost anywhere, even on fake-news megasite TheOnion.com, tech guru mecca Slashdot.org, or weird-headline portal Fark.com), while others offer sophisticated services to match two or more people.

The mission of any given social networking site is always to bring people together, but each site tries to reach a slightly different group of people. People in this business call this type of site a *social networking* site. But the term "social" can be defined pretty loosely. For example, Friendster.com uses relationships between people who already know one another to help you find an interesting "friend of a friend" to socialize with (see Figure 11-8), while LinkedIn.com helps business people network with people in the same line of work.

If you're not into planning ahead, ISawYou.com helps strangers who passed in the night (or the subway, the club, the restaurant, the museum) find one another. On the other end of the spectrum, Meetup.com (which got a lot of press for its Howard Dean events) helps highly organized folks who share a common interest or attribute set up a regular time and public place to meet, chat, drink coffee, play games, cross-stitch, or do whatever it is that "teen vampires" do (I kid you not; if you don't believe me, take a look at <http://teenvampire.meetup.com>).

Frequent travelers might find that friends they meet through CouchSurfing.com will let them have a free place to stay on their journeys. Indie music fans have been finding one another on MakeOutClub.com since 1999, which, despite the name, isn't a sexually oriented social networking site.



The screenshot shows a Mozilla browser window titled "Friendster Sign Up - Mozilla". The address bar displays "http://www.friendster.com/join.php". The form contains the following fields and options:

Country	UNITED STATES
Zip/Postal Code (US or Canada Only)	90403
Interested in Meeting People for	<input type="checkbox"/> Dating Men <input type="checkbox"/> Dating Women <input type="checkbox"/> Relationship Men <input type="checkbox"/> Relationship Women <input checked="" type="checkbox"/> Friends <input checked="" type="checkbox"/> Activity Partners <input type="checkbox"/> Just Here to Help
Status	<input type="radio"/> Single <input type="radio"/> In a Relationship <input type="radio"/> Open Relationship <input type="radio"/> Domestic Partnership <input type="radio"/> Married <input type="radio"/> Open Marriage
Terms of Service	I have read and agree to Friendster's Terms of Service . I certify that I am over 18 years of age.

A "Sign Up" button is located at the bottom of the form.

FIGURE 11-8 You'll have to state your intentions when you register for Friendster.com.

Rules of the Road for Social Networks

Sure, social networking can be a fun way to make new friends, but there are a few rules you should always follow when you sign up for one (or more) of these services. You don't want to set your e-mail inbox up as a vortex for spam, and you might not like everyone who sends you a message through the service, so look for sites that mask or otherwise hide your real e-mail address. If they can't hide e-mail addresses from the whole world, then use a free web mail address just for your social networking.

Once Posted, Personal Data Goes Out of Your Control Forever

Anything that you post about yourself on the Web will never disappear. Thanks to sites like the Way Back Machine (www.archive.org) and Google's cache of web sites and Usenet newsgroups, we can research the history of the Web. But there's

a potential dark side to the whole Web archiving thing: someone will be able to find out stuff about you years into the future.

Posting something about yourself that you might later regret could adversely affect your relationships or your ability to get employed, because even today, employers are Googling people who apply for jobs and folks who might want to date people they meet online can search for dirt on you just as easily.

As long as you're aware of the ramifications of your actions, post away.

Maintain Your Privacy While Job Hunting

The Web is a fantastic place to look for a job. As far as we're concerned, the want ads in the newspaper (you know, that bundle of dead trees someone throws at your porch in the morning) are history. Online, you can refine your search a hundred different ways, browsing the results and picking only the most interesting prospects.

Most job sites don't only host job listings but also let job hunters post their résumés online. Potential employers (or recruiters) can search through these résumés and find the most qualified candidates. But there are privacy implications of posting a résumé online: Résumés often contain the very same kinds of personally identifiable information that identity thieves and scam artists thrive on, so you normally provide somewhat less information—for example, not your street address or phone number—when you post a résumé online or e-mail it than you would if you were just sending it on paper in the postal mail directly to the human resources manager at a company.

And one additional word of caution for the go-getting job hunter: You'll see job listings for what look like amazing jobs—salary of \$80,000 or more, no experience necessary, high school education the only prerequisite, and (best of all) you get to work from home. As mentioned previously, if it sounds too good to be true, it is (see Figure 11-9). You'll see a bunch of these kinds of jobs all through your job searches. Just steer clear of them, unless you seek a mentally stimulating career in the envelope-stuffing or multilevel marketing industry. It's just silly to step on a land mine you can see from a distance.

Know Your Résumé Site

Ready to begin your job search? If you're going to be sending personal details about your job history to a web site, it's important to make sure you're dealing with a legitimate job hunt site. A typical search for "job search" turns up a lot of junk. These are a few job sites you can have a little more faith in.

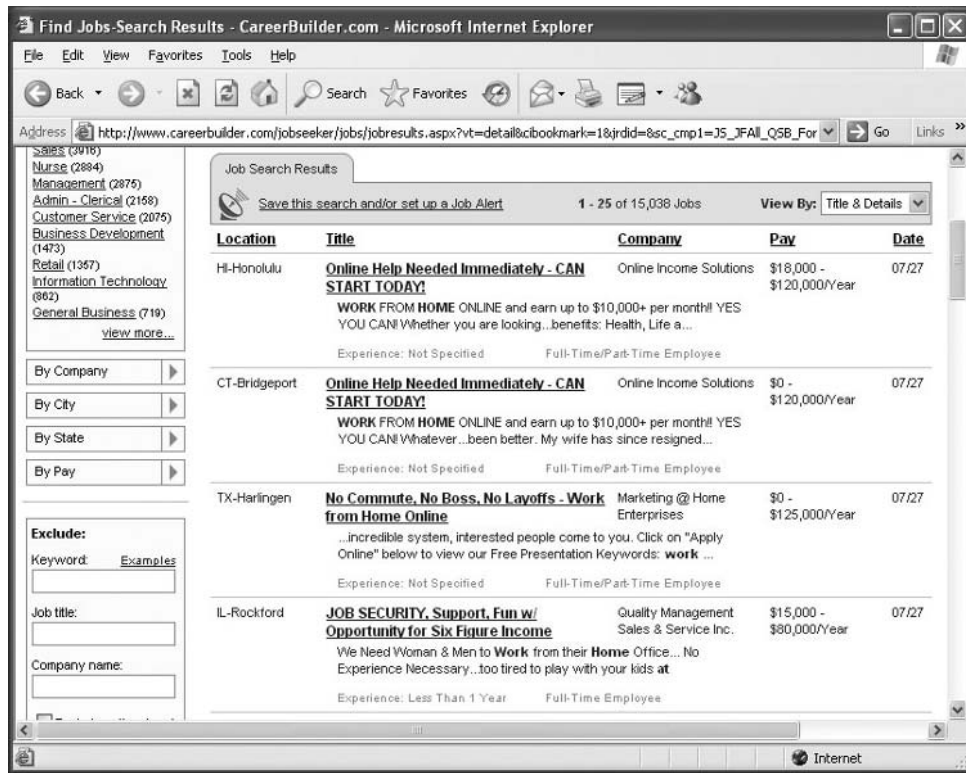


FIGURE 11-9 If you see the kinds of want ads that read like what you might see on a flyer posted to a telephone pole, just move along.

- **Monster.com** Don't let the silly name fool you: Monster.com is one serious career search site. Far more than a job search or résumé posting site, Monster.com also offers a social networking component to help get your foot in the door, a salary calculator that determines what you should be earning in terms of your geographic location, and tips about writing a better résumé, interviewing, and even advice about how to relocate to a different city for a new job.
- **Yahoo! HotJobs (hotjobs.yahoo.com)** The front page of Yahoo's site for job seekers is busy but full of good information. HotJobs gives you a place to post a résumé online, quick searches for jobs and training centers, and career self-assessment tests. Before you start padding that résumé with outrageous claims, take a look at the link where you can run a background check on yourself (it costs anywhere from \$10 to \$50, depending on the level of detail) to find out what employers can find out about you.

- **CareerBuilder.com** Twice a month, CareerBuilder hosts a Career Fair in a different city. At the fairs, you can meet local employers face to face, but if you don't want to wait for the Career Fair train to pull into your station, you can post a résumé and search for jobs here, too. And because CareerBuilder lets you post as many as five résumés, you can experiment with putting different information into your résumé, with the goal of improving your chances of landing your dream job. If that job's out of state, you can get free quotes from moving companies, too.

Dos and Don'ts for Self-Hosted Résumés

If you've got your own web site and want to host your résumé online there, you'll want to create a custom version of that résumé to protect yourself. Here are some of the dos and don'ts of posting your own résumé online yourself.

Do:

- **Include an e-mail address**, but use a free web mail account, to keep spammers at bay.
- **Say what city and state/province you live in**, but give out no additional location information until you're signing the job contract.
- **Give your relevant job history**, but keep it short and lightly formatted. Flashy or verbose résumés won't get you hired, your work experience will.

Don't:

- **Include a phone number.** If they want to talk to you before the interview, they can drop you an e-mail message with *their* phone number, so you can call them. Google the phone number they give you, to make sure you're really calling a potential employer.
- **Give out salary history over the phone.** Some con artists call the phone numbers of people listed in résumé sites or on their own sites, pretend to be HR managers, and ask people for their financial history. In general, if you feel like you're getting the third degree from a stranger that called you, try to get as much information as you can about the caller. If they resist answering your questions, politely thank them, excuse yourself from the conversation, and hang up.

- **Make your résumé graphically rich**, unless you're going after a graphic design job. Plain text is much easier to read than a visually complex résumé on screen. Think about the person reading your résumé on the other end: Will a heavily formatted page break on their web browser? Will they want to load a 30-second Flash movie before being able to view your résumé? Keep it simple.

Chapter 12

Prevent Identity Theft and Protect Yourself



How to...

- Evade credit card fraudsters and identity thieves
- Deal with identity theft, if you're a victim
- Identify and avoid phishing scams and spyware apps

Keep Identity Thieves Away from Your Data

The formerly obscure crime of identity theft, where someone electronically impersonates someone else for financial gain, is now the most common white collar crime in the world. According to research studies by Harris Interactive and Gartner, roughly seven million people became identity theft victims between July 2002 and July 2003 (the latest statistics available at press time). Even more shocking, in 2003 statistics compiled by the Federal Trade Commission, the victim never even reported the crime to police in more than half the cases.

Law enforcement agencies that deal with financial crime, such as the Secret Service and FBI, estimate it can cost government from \$15,000 to \$20,000 to prosecute just one identity theft criminal. Many identity thieves are repeat offenders, who strike again and again because the “classic” act of identity theft—stealing a credit card number, ordering expensive goods online to a *dead drop* (a secret delivery location), and then fencing the illicit goods for cash—is far more lucrative (and much safer) than robbing banks or knocking over liquor stores.

But to an identity theft victim, a stolen credit card number is just the beginning of what seems like an endless nightmare. According to data compiled by the Identity Theft Resource Center (www.idtheftcenter.org), the average victim spends 600 hours and more than \$1,400, over the course of several years, dealing just with the immediate aftermath of the theft. This includes the restoration of their credit history and recovery of any funds stolen from bank accounts. Beyond that, some victims have had to suffer the indignity of rejected loan, job, or home rental applications, and a few have even experienced the ultimate Kafkaesque nightmare of being arrested for crimes they didn't commit.

Identity theft may be the biggest crime of the century, but you're not powerless to defend yourself, whether or not you've become an ID theft victim. Taking some of the steps we outline in this chapter may help keep you from becoming a victim yourself.

Safeguard Your Information Before Thieves Strike

If you've never had your personal data stolen and used by a criminal, you're pretty lucky. About 85 percent of people who become ID theft victims find out after the damage is done. But don't think it can't ever happen to you, just because it hasn't happened to you yet. Sticking your head in the sand won't protect yourself from ID theft in the future. There are a lot of steps you can take to make it harder for ID thieves to get a foothold into your financial information.

Sign the Back of Your Credit Card

This one might seem like a no-brainer, and for some people, it is. But a surprisingly high number of people still fail to sign the backs of their credit cards.

In order for the signature to work as a way to authenticate yourself, the person who takes the card must take a moment to check the signature against the card slip. But if you use credit cards regularly, you know that the people who take credit cards rarely notice the signature, let alone check it carefully. More frequently, they check the name on your ID against the name imprinted on the card. Signing the card should add a modicum of additional verifiability to a transaction, but it almost never does.

However, once you notice this, you can pull some amazing practical jokes on clerks. To illustrate how little attention anyone pays to the signature on a credit slip, humorist John Hargrave (www.zug.com/pranks/credit/) signed his credit card slips with a squiggle, then a scribble, then a grid, an X, a stick figure, Egyptian hieroglyphics, the names of famous people, and finally, "Please Check ID." At no time did a clerk or cashier so much as bat an eyelid at the bizarre signatures he used (see Figure 12-1).

12

Shred Your Paper Records

Yeah, it's not high tech, but it works. An inexpensive paper shredder can turn reams of sensitive financial and other records into something you can use to line your kid's hamster cage. You could also use old records to light a fireplace or start the barbecue, or mulch them in your compost heap. Identity thieves don't need to resort to technology to steal your data when a little dumpster diving will do. Don't make it easy for them.

Wipe Old Hard Drives and Destroy Removable Media

When MIT students Simson Garfinkel and Abhi Shelat bought 158 old hard drives in late 2002, they discovered a treasure trove of sensitive personal information.

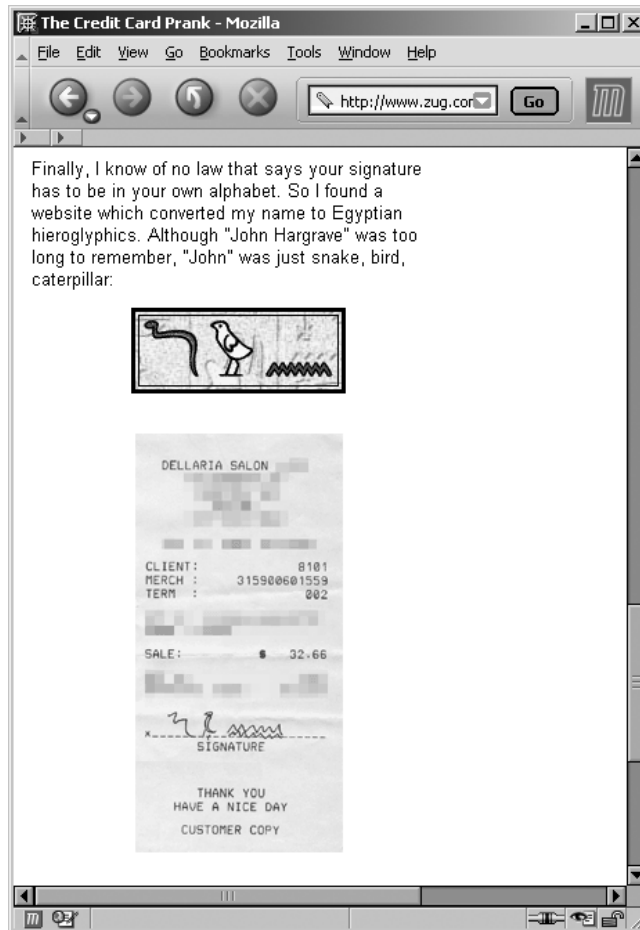


FIGURE 12-1 Nobody seems to notice even if you sign your credit card slip with your name in hieroglyphics.

For less than \$1,000, the pair obtained 129 working hard drives. Using commonly available data recovery software, they were able to undelete most of the files that had been placed in the My Documents directory. On 28 of the drives, no attempt whatsoever had been made to delete any of the data.

What were they able to find? Even though 60 percent of the drives had been formatted or had part of the data deleted, the pair recovered a file containing more

than 5,000 credit card numbers, personal e-mail, and some detailed medical information, internal corporate documents—and let’s not forget: gigabytes of porn.

How many computers have you owned over the years? Can you, right at this very minute, account for the hard drives, floppy disks, recordable CDs, and other kinds of removable media you used on all of these computers? Simply dropping files in the Recycle Bin won’t get rid of documents. Even a standard format rewrites only a small portion of the hard drive, deleting just the map, or file table, that it used to locate the files that are still present on the drive.

The scope of the problem is enormous, but fortunately, you can do something about it: have a scorched-earth policy about old data media.

Software like the free Eraser utility (www.heidi.ie/eraser/) can wipe your entire hard drive (or just parts of it) clean. And you can buy shredders (like the one in Figure 12-2; see <http://find.pcworld.com/43464>) designed to pulverize CDs, DVDs, and floppy disks into plastic confetti. These tools exist for one reason: Data lives a lot longer than most people realize, and it can be used to commit identity fraud crimes. Unless you plan to melt your old disks down in a modern art display at Burning Man, get rid of them safely—don’t just chuck ’em in the trash.

Make a Boot and Nuke Floppy Using Eraser Eraser is a small applet that can wipe portions of the hard drive (such as the browser cache, the swap file, and unallocated space on the hard drive—the so-called “empty” space that is actually full of “deleted” files) or the entire drive in one go, including the operating system (see Figure 12-3). For the purposes of this chapter, we’re assuming you plan to get rid of an old computer or hard drive, and you want to blow away any data on it.

For the purposes of erasing an entire hard drive, you’ll need to create a special bootable floppy disk with a data destruction program on it. Once you’ve done that, all you need to do is boot the computer with the special floppy in the drive, and the software will scour the hard drive clean of any trace of data. One word of caution, before you wipe your drive: physically disconnect the power and data cable from any hard disk in your PC that contains data you want to keep before you boot up the special floppy disk.

Download and unzip Eraser’s installer (www.heidi.ie/eraser/), and run the EraserSetup.exe file. The program runs through a standard installation procedure. When it’s done, click Start | Programs | Eraser | Create Nuke Boot Disk. Insert a floppy in the drive, click the OK button in the dialog box, and in a few minutes



FIGURE 12-2 Alera's CD/DVD Shredder makes optical discs unreadable.

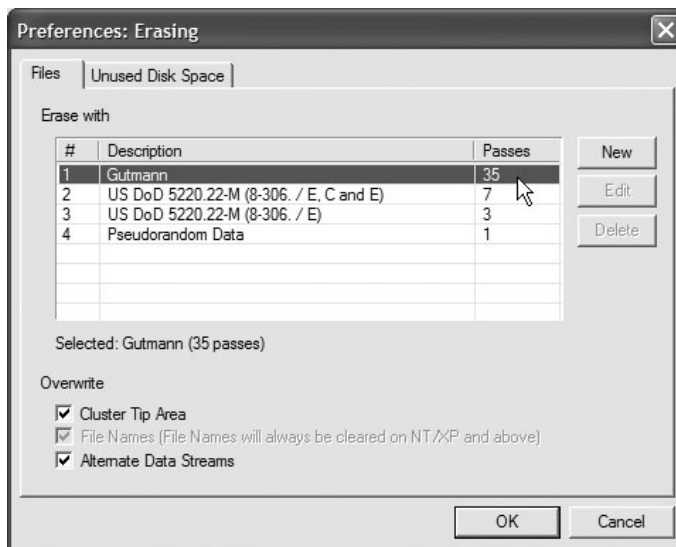


FIGURE 12-3 Eraser can overwrite files or empty space on a hard drive once, three times, seven times, or thirty-five times, depending on how paranoid you are.

you will have your instrument of destruction, known as a DBAN disk (named Darik's Boot and Nuke after its creator, shown in Figure 12-4).

To wipe a drive clean, just make sure it's installed in a computer, insert the DBAN disk, and turn the computer on. It can take anywhere from 20 minutes to an hour for the DBAN disk to do its job, but when it's done, not one byte of data should be recoverable from the drive. You can donate or sell the old drive assured that your secrets will remain secret.

Opt Out of “Credit Card Checks” and Similar Services

Many banks that issue credit cards periodically send their customers special pre-printed checks. These checks work just like those you get for your checking account, only when you spend them, the charges go onto your credit card bill. Because banks send these checks out all the time, often without warning, you're unlikely to notice when thieves steal them out of your mailbox. If you get checks like these and don't plan to use them immediately, or ever, shred them. (After all, they're just as steal-able from your trash can.) If you never use these kinds of checks, head to your bank's web site (or call them) and ask them to stop sending these checks to you.



FIGURE 12-4 Once you've installed Eraser, you can create a Boot and Nuke disk from the Start menu.

Get Your Credit Report and Check It Out

If you've never gotten a credit report, or if it's been more than a year since you last got one, order one today. Under the terms of a law passed at the end of 2003 called the Fair and Accurate Credit Transactions (FACT) Act, every American is entitled to a free copy of his or her credit report once a year. (If you've been a victim of identity theft, you're entitled to free reports from all the major credit reporting bureaus right now—go to the next section in this chapter for more information.) The Federal Trade Commission (FTC) will begin administration of the forms you'll need to fill out beginning in January 2005.

Until then, if you're anxious to get started checking out your credit history, you can visit the web sites of each of the three major credit reporting bureaus—Experian, Equifax, and TransUnion—and order a report today. Each bureau offers two kinds of credit reports: one that contains the information they have about you, and a “three bureau” report that (theoretically) contains information from all three bureaus. Prices for the single reports cost around \$9; the three-bureau report costs from \$30 to \$40, depending on which bureau's site you order the report from (see Figure 12-5).

Examine your credit report for discrepancies, such as account numbers or references that you don't recognize or that are clearly wrong. If you find anything out of the ordinary, report it to the bureau(s) that listed the incorrect information on your report. Each bureau includes specific instructions on how to do this with the credit report.

Here's how to get a copy of your credit report and what it costs (for non-fraud victims) for a single and three-bureau report:

- **Contact the FTC** Beginning in January 2005, the FTC web site (www.ftc.gov) will have information about how you can get a free copy of your credit report once a year.
- **Experian** Reports cost \$9 (single) or \$35 (three-bureau) and can be ordered through the web site (<http://find.pcworld.com/43466>) or by calling (866) 200-6020.
- **Equifax** Reports cost \$9 (single) or \$30 (three-bureau). Order from their web site (<http://find.pcworld.com/43468>) or by calling (800) 685-1111.
- **TransUnion** Reports cost from \$1 to \$9 (single), depending on what state you live in, or \$30 (three-bureau). Order reports from the web site (<http://find.pcworld.com/43470>) or by calling (800) 888-4213.

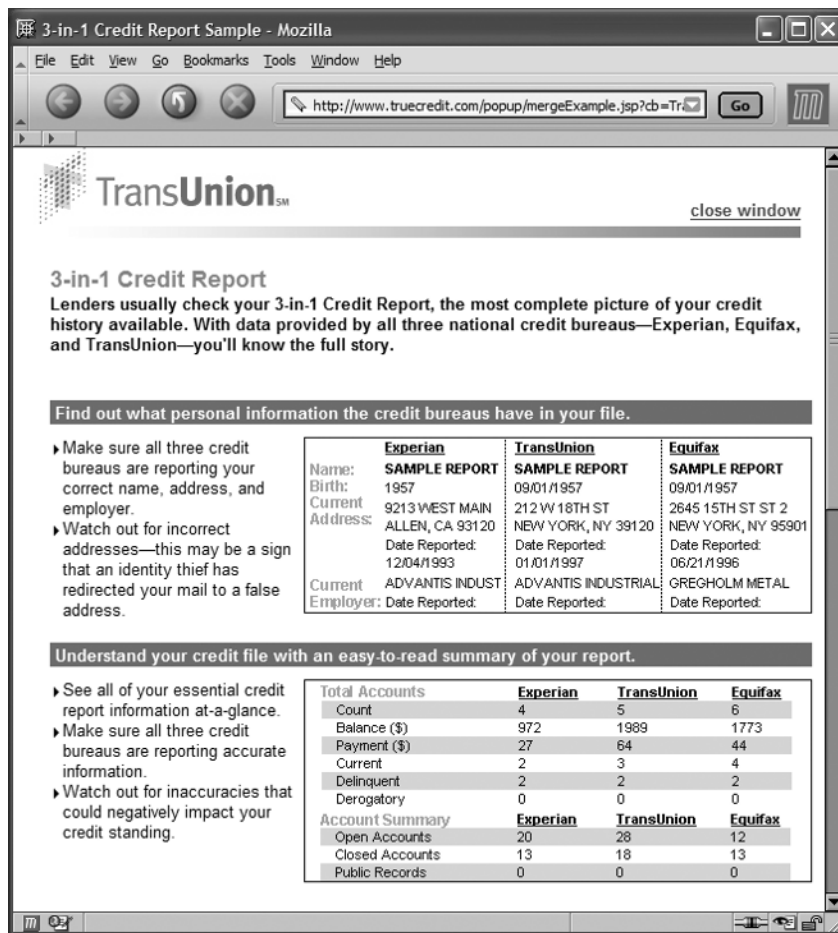


FIGURE 12-5 The information in a 3-in-1 credit report is the same, no matter which bureau you order it from.

NOTE

When ordering a credit report to check for fraud, don't tack on extras like a personal credit score or credit monitoring. These additional services won't help you determine whether you've been victimized prior to ordering the services, so they aren't worth the extra charges.

Did you
know?

E-Mail Messages with Dire Warnings about Your Credit Report Are Bogus

Some people started receiving e-mail messages in 2001 from friends and family, alerting them to a terrible danger—anyone would be able to get a copy of your credit report unless you call a special toll-free number and ask to be removed from some sort of list. The e-mail messages are still floating around today, despite the fact that the entire message is wrong. No strangers can legally get a copy of your credit report.

The telephone number listed in the e-mail is the same number as the prescreening opt-out line, (888) 5-OPT-OUT, which only prevents credit issuers from giving you “instant” credit or pre-approved credit card applications. But don’t worry: Credit reporting agencies are prohibited from giving out your credit history to just anyone—only financial institutions, insurance companies, landlords, and other businesses who need to know your financial history are allowed to get that information.

So even if you don’t call the prescreening opt-out phone line, your credit records are still safe. If someone forwards a similar e-mail to you, send them to <http://find.pcworld.com/43462> so that they can learn the truth about this annoyingly persistent urban legend.

In addition, the three credit reporting bureaus operate a service where you can request that your credit information not be released for the purposes of offering you pre-approved credit, loans, those “credit card checks” just mentioned, or other marketing of financial services. Companies engage in this practice, known as *prescreening*, so that they can send you applications for credit in the mail where you’re guaranteed to get the card.

Unfortunately, thieves love to steal these envelopes and sign up for the credit in your name, but sent to another address (usually an apartment building, where they can pull the envelope out of the bin where the postal carriers or apartment dwellers dump all the junk mail). This is one way identity thieves get a foothold into your credit. Fortunately, you can contact the “opt-out line” at (888) 567-8688 or (888) 5-OPT-OUT and prevent companies from sending you pre-approved credit offers in the mail. As a side benefit, you get less junk mail, too. You can’t beat that!

Terminate an Identity Theft Case

Identity theft can happen to anyone, and you don't even need to do something "wrong," like losing a wallet, to become a victim. If you discover someone else dragging your good name (and your financial history) through the dirt, step up to the plate and take action to stop the thief and restore your honorable reputation.

Protect Your Identity if Fraud Hits Your Accounts

The more evidence you collect as you trace the steps of the identity crook who sullied your financial history, the better. As you obtain records, file reports, and discover new information, take notes recording the details, as well as the date and

Did you
know?

Fraud Alerts in Your Credit Report Can Be a Blessing and a Curse

Victims of identity theft quickly learn that the credit reporting bureaus can put a *fraud alert* or *security alert* in their records pertaining to you. This notice permits you to freeze new credit applications in your name—even the legitimate ones—for a short period of time (usually 90 to 120 days), until you can sort out a situation where someone has spoofed your identity and used it to run up huge bills somewhere. The bureaus each have a process to take a report about identity theft and put the fraud alert in your records. If you suspect or have evidence that you've been victimized, contacting the bureaus about a fraud alert should be one of your first steps.

You can, however, still put a fraud alert in the bureau records, even if you haven't been a victim of identity theft. The alert prevents the bureaus from releasing your credit report without your explicit approval, which usually can be given in a phone call. While this may seem like an inconvenience, it also prevents credit card companies from sending you pre-approved credit applications (the same ones identity thieves love to steal out of mailboxes).

But you should never take the decision to set up a fraud alert lightly. Having a fraud alert on your credit record can also affect your ability to get a home or car loan, obtain insurance, rent an apartment, and possibly even get a job. Fortunately, these expire in a few months.

time you learn new things. Collect the information into an archive, where you can add to it as necessary, and keep copies of your records that you can provide to police or other investigators. The steps here are listed roughly in order of priority.

Alert All Your Banks and Any Other Financial Institutions You Do Business With

First things first: Protect your savings. Contact your bank(s) where you have checking and/or savings accounts, and apprise them of the situation, even if the bank isn't involved in the initial fraud (see Figure 12-6). They can help you set up procedures (such as verbal passwords or replacement PIN numbers you will use to identify yourself) that will ensure your deposits aren't raided by the identity thief.

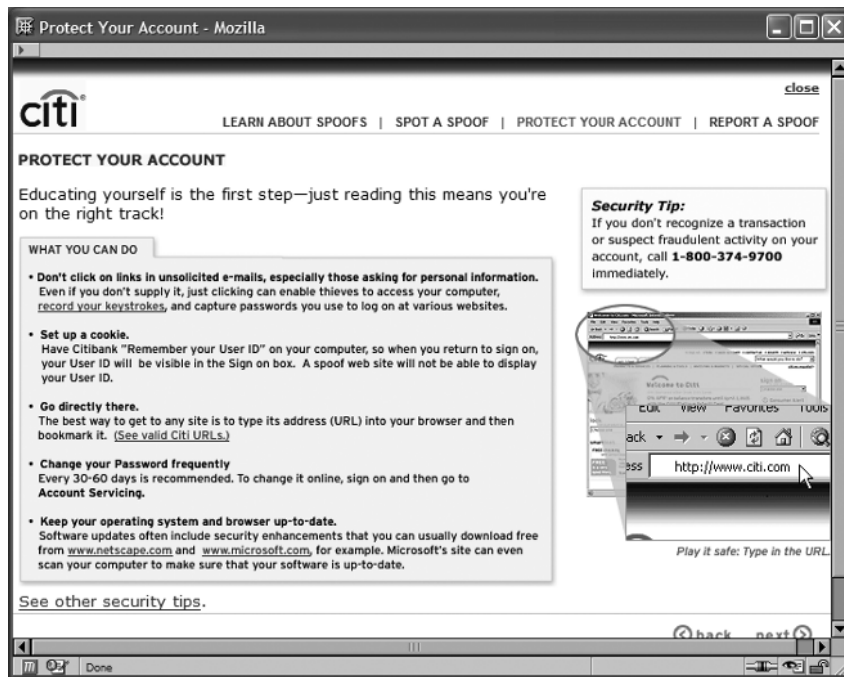


FIGURE 12-6 Citibank has a special hotline—(800) 374-9700—you can call if you suspect you're a fraud victim.

Put a Fraud Alert in Place with the Credit Reporting Bureaus

If you're sure that an account in your name on your credit record does not belong to you, first contact the credit reporting agency on whose record the account is listed, and ask them to begin a fraud investigation and to set up a fraud alert on your records in their database. Then call the other bureaus and do the same thing. Here are the credit reporting bureau phone numbers to call to set up a fraud alert.

- **Experian** (888) 397-3742
- **Equifax** (800) 525-6285
- **TransUnion** (800) 680-7289

When you set up the fraud alert, one or more of the credit reporting agencies will fax and/or call the bank where the fraudulent account was opened.

Once you've positively determined that someone has opened accounts in your name, you'll want to contact the bureaus and ask them to put a seven-year victim statement in your credit record file. These statements, which can include details of the identity theft incident, help ensure that the case does as little damage as possible to your credit rating and financial history.

Close Any Accounts That Were Opened in Your Name by Someone Else

If you find a strange card number associated with your name in your credit report, contact the customer service department from the bank or financial services company that issued the card, let them know who you are, and explain that you need them to *dispute* the account pending an investigation into an identity theft case. If they can close the accounts, ask them to do so. If they can't do that while you're on the phone with them, ask them to contact the credit reporting bureaus immediately. Use the FTC's standard identity theft affidavit form (<http://find.pcworld.com/43472>) to provide the necessary information to the bank or other business where you are disputing a new, unauthorized account.

Report the Identity Theft to the Police, the Social Security Administration, and the FTC

Once you've got your money protection set up, call your local police department and ask them to take a report about the identity theft case. You will need this police record (and case number) as part of your documentation to clean up your credit record.

If you believe the identity thief was able to get your social security number (and let's face it, this isn't hard), you should also contact the Social Security Administration (www.ssa.gov or telephone (800) 772-1213, 7 A.M. to 7 P.M., Monday through Friday). In some cases, you'll get a new social security number (if the identity thief continues to open new credit in your name). The SSA won't issue you a new number if the identity theft happens just once, if you've ever declared bankruptcy, or if you lose your social security card and nobody else appears to be using the number.

Finally, you should always report a case of identity theft or fraud to the Federal Trade Commission. Their web site (www.consumer.gov/idtheft) has an automated complaint form (you can find it at <http://find.pcworld.com/43474>) that you can fill out if you're a victim (see Figure 12-7). Financial crimes such as these are added to a database, which can help law enforcement track down and prosecute identity criminals.

The screenshot shows a web browser window displaying the FTC's identity theft questionnaire. The browser's address bar shows the URL <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>. The form is titled "How the Fraud Occurred" and includes a section for checking all that apply for items 11-17. The form is displayed in a Mozilla browser window with a toolbar and a sidebar on the left showing "Bookmarks", "Signatures", "Layers", and "Pages". The form content includes the following questions:

How the Fraud Occurred

Check all that apply for items 11 - 17:

- (1) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.
- (12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.
- (13) ☐ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ☐ stolen ☐ lost on or about _____ (day/month/year).
- (14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Below the questions, there are two lines for "Name (if known)".

FIGURE 12-7

The FTC's identity theft questionnaire asks some very detailed questions about the fraud incident.

Protect Your Sensitive Data Online and on Your PC

Identity thieves are using increasingly more sophisticated tools to steal information from your PC that will enable them to commit identity fraud types of crimes. From keystroke logging software to so-called *social engineering* attacks, ID thieves increasingly are turning to technology to steal the data they need to rip you off.

Keep Private Information about Yourself to Yourself

Almost everywhere you go on the web, you're asked to tell the world about yourself. Newspaper web sites commonly ask their online readers to *register* with the site. You might participate in message board discussions, but as part of the signup process, the board may have asked for your birth date, what you do for a living, your annual income, your favorite hobbies, or any of a dozen other bits of information an identity thief could use against you. Instant messaging programs (which we covered in Chapter 10) also provide a venue for you to spill the beans to ID criminals in their "personal profiles" sections.

When asked for sensitive data—your mother's maiden name, your SSN, your birthday, where you live or work, your phone number, or any other personally identifiable information—don't be a pushover. You can, and should, vigorously question anyone who asks you for this kind of very sensitive information. Even the social security administration advises people who are asked for their social security number to ask why it's needed, what it'll be used for, what happens if you refuse to turn it over, and what law requires that company to ask you for it.

It's not easy for some people to say no to these kinds of requests. In fact, when asked by the folks who run cash registers in stores, people give up details like their address so often that the clerks who ask for this kind of information are usually surprised when you just say no. Frankly, when this happens, I find the puzzled look on a cashier's face hilarious. But if you find it irresistible to tell the world about every detail of your life, resist that urge; it's going to get you in a lot of trouble in the long run. Except in very specific circumstances (such as when the store is going to deliver something to your house), no business needs to know that much about you.

And if you've already posted some or all of this stuff online somewhere, it's not too late to take it down. Delete your profile details today. Get that stuff off the Web!

Perform “Vanity Searches” and Unlist Yourself

Ever Google yourself, just for fun? Sometimes you can find some pretty interesting stuff about yourself (see Figure 12-8). While it may seem cool at the time, there’s a catch: identity thieves can and do use this kind of information for nefarious purposes, too.

Maybe your employer lists the company directory online, and that photo of you at a charity event that ended up in the local paper is cached somewhere, too. If you attend college or graduated since 1990, there might be a lot more information about you than you realize, including your social security number, your name, and

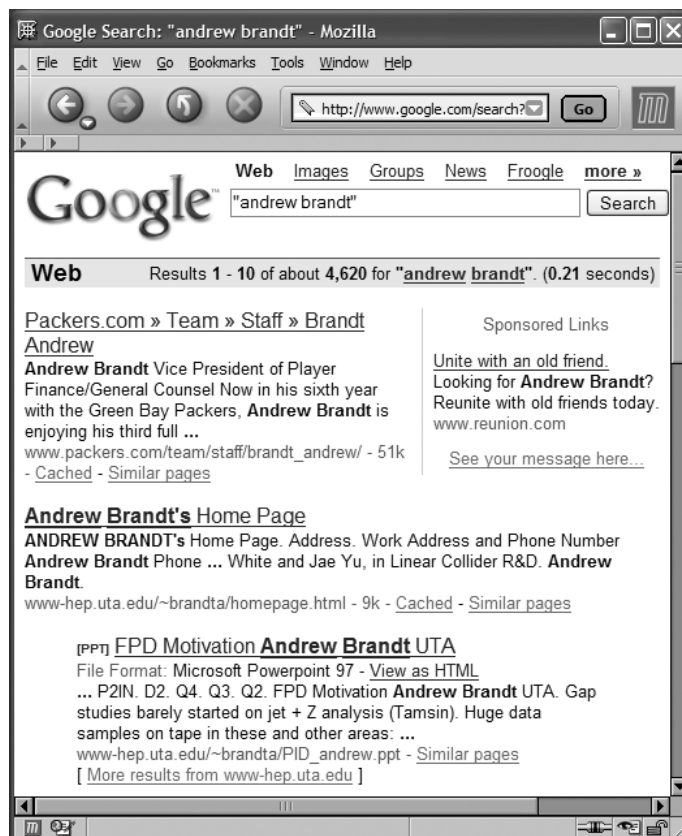


FIGURE 12-8 Vanity searches typically turn up lots of odd results.

a photograph. Some military officers’ promotion notices, for example, are published in the Federal Register—which is also mirrored to the Web—and include those officers’ social security numbers.

It’s worth the effort to try to get the most damaging information taken offline. What kinds of things should you search for? Court records, especially those from civil courts, are increasingly published online. If you’ve sued someone, or if you’ve been sued, contact the courthouse to find out if their records are online. Buying real estate also puts your personal information in a public record that might be searchable from the Web. (See Figure 12-9.)

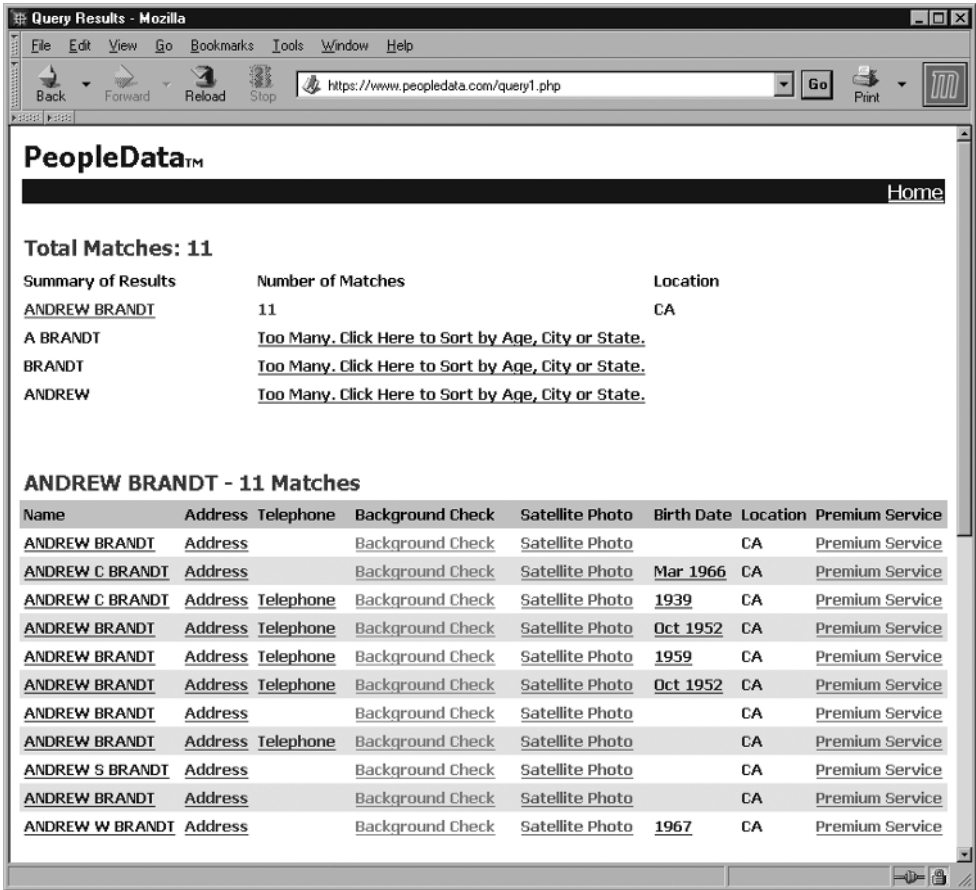


FIGURE 12-9 For just \$50, peopledata.com lets you run background checks.

Start by entering your vital details into search engines: your full name, street addresses where you've lived, your birth date and social security number, and your phone number. And don't just Google this stuff (see Figure 12-10); look on Yahoo.com, Altavista.com, Alltheweb.com, lycos.com, metacrawler.com, and excite.com as well. Sites like anywho.com, whowhere.com, and whitepages.com specialize in searching for people, and peopledata.com lets you run complete background checks, for a fee of course, on yourself (or people with the same name).

Combine searches of your name with the company you work for, or your e-mail address, home address, or work address. Most importantly, when you find sensitive personal information, contact the site and get them to take it down. Google's own PhoneBook search tool lets you unlist yourself from the directory. Head to www.google.com/help/pbremoval.html to get yourself out of their white pages.

The screenshot shows a Mozilla browser window titled "Google PhoneBook Name Removal - Mozilla". The address bar displays "http://www.google.com/help/pbremoval.html". The main content area features an "IMPORTANT NOTE" stating that removing a phonebook listing does not remove personal information from other pages. Below this, a list of reverse phone lookup services is provided, including Anywho, Switchboard.com, Whitepages.com, Reverse Phone Directory, Phonenumber.com, and Smartpages.com. A link to a Google search for a comprehensive list of reverse phone lookup services is also present. The form itself is titled "Please enter all information exactly as it appears in your phonebook entry:" and contains three text input fields: "Enter your name", "Enter your city and state (e.g. Mountain View, California)", and "Enter the phone number to be removed" (with a format of () -). Below these fields are three radio button options for the "Reason for removal": "My phone number is incorrect", "Privacy concerns", and "Other". A "Submit Form" button is located at the bottom right of the form area. The footer of the browser window shows "©2004 Google - Home - All About Google - We're Hiring - Site Map".

FIGURE 12-10 Google's PhoneBook Name Removal form takes your home address and phone number offline.

Steer Clear of Phishing Scams

Starting in 2003, some of the spam e-mail that flows into our inboxes began to take on sinister overtones. Our accounts were on the verge of being shut down, said the messages. Some of them included the official corporate logos of our banks, of the auction sites we visit most, of online payment services like PayPal. They warned you, you need to log into our site and “confirm” your account, lest it be closed for good.

Thousands of people, fearing the loss of money, e-mail, or auctions-in-progress in online accounts, rushed to click the links in these messages, entered their usernames and passwords into official-looking pages on what they thought was the real web site.

Then, blammo. Nothing happened. Or did it?

In reality, those folks just handed their most sensitive information—logins and passwords to online banks, investment web sites, and payment services—right over to the identity thieves. This kind of scam, now given the unfortunate name of *phishing*, was so effective that the victims didn’t even know they’d been robbed for days or weeks, until one day, their accounts had been emptied, or the password changed. That was when the grim reality began to set in. They’d been swindled, suckered by a twenty-first century P.T. Barnum.

But to sophisticated users, these forgeries were pretty obvious. Misspelled words dotted the windows. Graphics didn’t line up correctly with other elements on the page. And if you hovered your mouse pointer over the links in the messages, the URLs just didn’t look right. In the beginning, you could spot one of these scams a mile off, if you knew what to look for.

Then the crooks behind the phishing scams began to get wise. They corrected the obvious dumb grammar and spelling mistakes. They cleaned up the graphics. And most deviously, they exploited weaknesses in how Outlook Express or Internet Explorer displays a URL on a page, to obscure the real URL where the link in the e-mail message would take you. Thousands more got scammed.

What to Do If You Get a Phishing E-Mail

According to the Anti-Phishing Working Group (www.antiphishing.org, see Figure 12-11), phishing attacks are growing exponentially and getting more sophisticated. There are a few basic rules you can follow to avoid getting suckered by a phishing expedition. For one thing, your bank won’t ever close your online account simply because you haven’t logged in for a while, so don’t believe any e-mail that warns about this kind of outcome. Banks, payment services, and auction sites never need you to e-mail them your passwords—they run the site, after all, so they know them already!

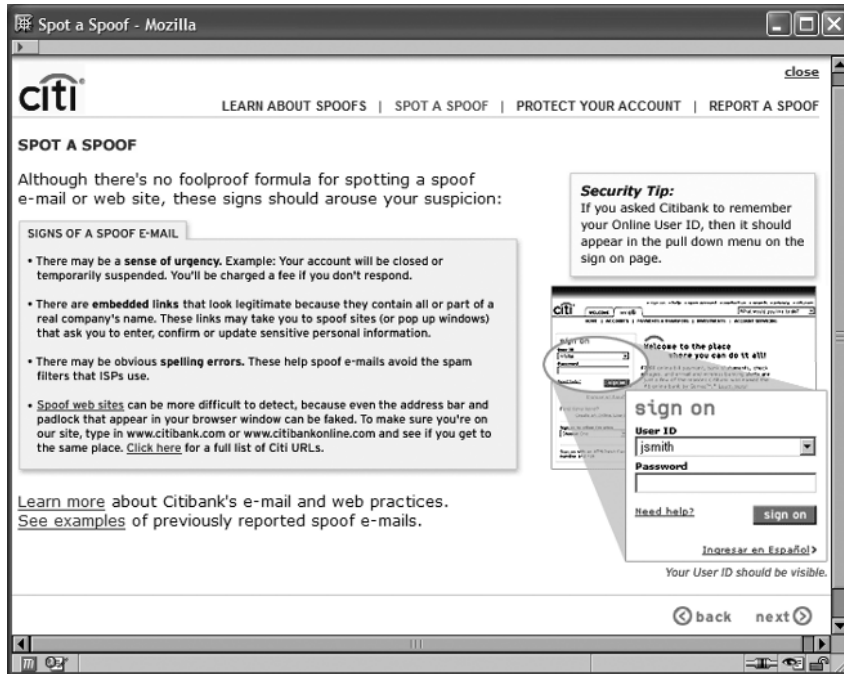


FIGURE 12-11 Phishing messages often share some characteristics.

If you think, even for a moment, that a message might be legit, don't click the link in the message. Instead, open your browser and type in each letter of your bank's (or payment service's, or credit card company's) URL yourself, and hit the ENTER key. Look for their secure login page, which will have a URL that begins with "https://" (look for the extra *s*, instead of the "http://" you're used to), and use that link.

Spread the word to your more gullible (or less net-savvy) friends and family about phishing scams. If you're reading this book, you're duty-bound to make sure the people you care about don't fall for this kind of stuff.

And the Anti-Phishing Working Group wants copies of any phishing e-mail you get. For details and instructions about how to send the messages, click the Report Phishing link on their front page.

Better Browsing with Alternatives

One of the easiest ways you can avoid many of the pitfalls of modern web browsing is to use an alternative browser. Attacks against Internet Explorer, using rogue

ActiveX controls or exploiting scripting vulnerabilities, are the most common ways bad guys get into your PC. Here are a few options you can choose from:

- **Netscape (<http://find.pcworld.com/43476>)** Tied in with AOL's broadband service, Netscape includes AIM and a streaming music service, Radio@Netscape (see Figure 12-12). Netscape's mail application features a Palm Sync function for owners of that PDA, and both the mail client and browser claim to be able to easily import your settings from other browsers.



FIGURE 12-12 Netscape is the senior graphical web browser.

- **Mozilla (www.mozilla.org)** This is the core of the Netscape browser, without the AOL additions (see Figure 12-13). Tabbed browsing lets you keep many pages open at once, and a built-in pop-up blocker prevents unsightly ad exposure. The mail client provides only rudimentary spam filtering.
- **Opera (www.opera.com)** Opera shares many of Mozilla's features and includes a spam-filtering mail reader, an IRC client, and an RSS reading application (see Figure 12-14). The one downside: Opera's free version is ad-supported and displays a banner ad, embedded in its window, at all times. However, its paid version is ad-free.

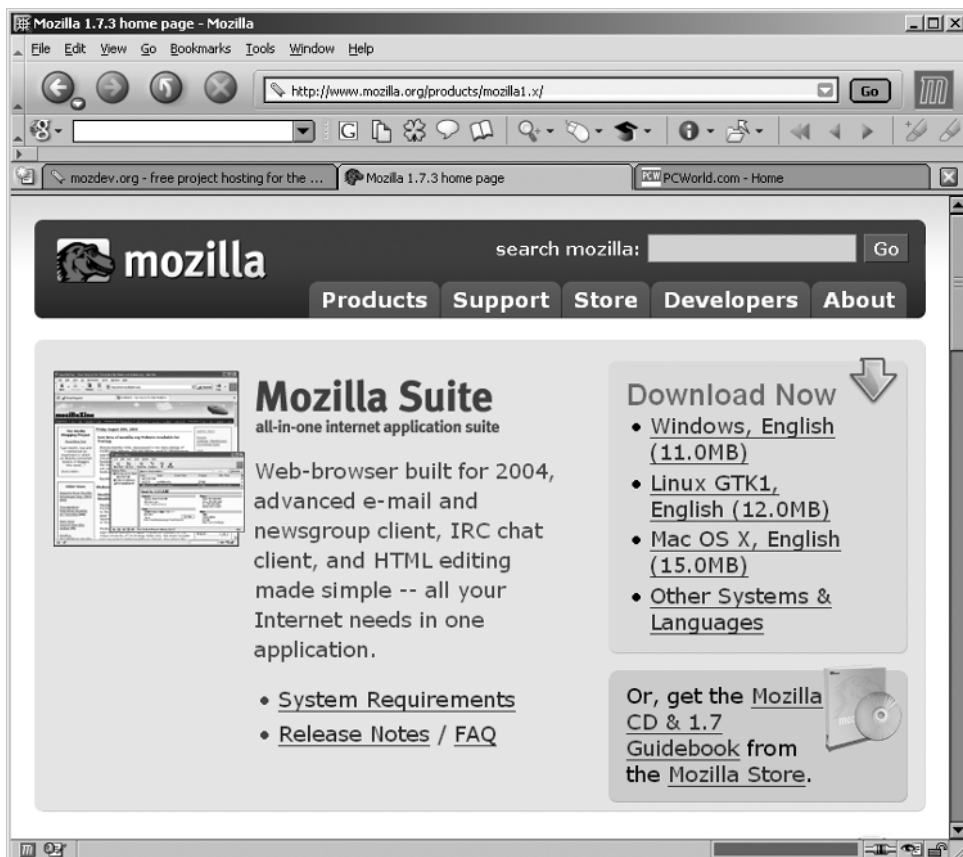


FIGURE 12-13 Mozilla extracts all the best of Netscape's features and engine.



FIGURE 12-14 Opera's settings are always within easy reach.

- **Firefox (www.mozilla.org/products/firefox/)** Mozilla's younger cousin is speedy and slick (see Figure 12-15). Downloads all go to the desktop automatically to reduce the number of dialog boxes you encounter. At 4.7MB, it's one of the slimmest browsers anywhere. Like the others, it has its own pop-up blocker, and its UI is fully customizable, with a substantial theme library.
- **Lynx (<http://find.pcworld.com/44394>)** For the ultimate experience in retro-web browsing, you have to try Lynx, the original text-based web browser (see Figure 12-16). Web pages display in an 80 × 32 command-line window, and you use arrow keys to move your selection from link to link. The SPACEBAR turns the page. It's got no pop-ups, but also no graphics to speak of.



FIGURE 12-15 Firefox is made for speed.

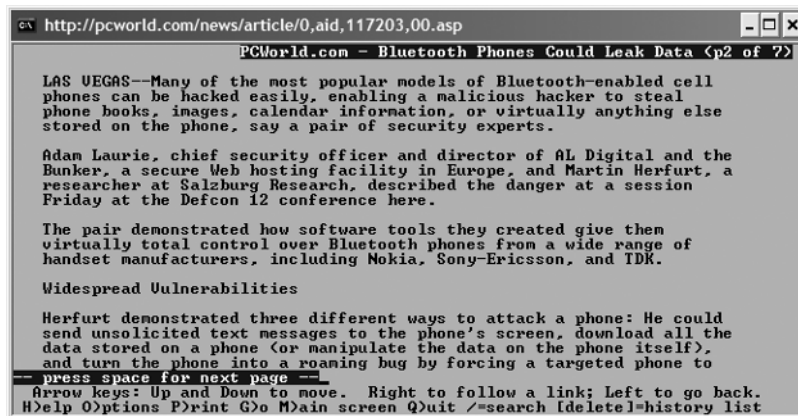


FIGURE 12-16 Lynx, the first text-only web browser, brightens up DOS.

Index

Numbers

- 10 Gigabit Ethernet, features of, 39
- 802.11* standards
 - using with WAPs, 18, 83–84
 - for wireless networks, 142
- (888) 5-OPT-OUT, significance of, 324

A

- access points, adding to networks, 82. *See also* gateways
- access, preventing with MAC filtering, 166
- accounts, closing to prevent identity theft, 327
- Active Content, relationship to spam, 253
- ActiveX controls
 - installing with Windows Update, 177
 - relationship to Windows Update, 175
 - using with Office Update, 186–187
- ad blocking
 - in antivirus applications, 200–201
 - managing spyware with, 130
- Add a Port dialog box, displaying in Windows Firewall, 120
- address ranges
 - selecting for wired networks, 64–65
 - selecting for wireless networks, 94–95
- Adelphia ISP, spam filters provided by, 250
- ad-hoc mode versus infrastructure mode, 149
- administration console, explanation of, 146–147
- ADSL (Asynchronous DSL), features of, 15
- AES (Advanced Encryption Standard), relationship to wireless networks, 142
- Aftab, Parry and chat safety for kids, 290
- aggregator clients
 - obtaining for IM, 270
 - updating, 278–279
 - using with IM and chat applications, 267, 269
- AIM (AOL Instant Messenger)
 - configuring privacy preferences in, 277
 - downloading, 268
 - managing incoming files with, 286
 - updating, 277–278
 - Virus Checker in, 287–288
- air ducts, pulling cable through, 59
- alerts, configuring in Security Center, 115–116
- American Express Smart Chip, features of, 308
- antennas
 - extending signal range with, 86
 - installing to remote locations, 45
- Anti-Phishing Working Group
 - reporting phishing e-mail to, 334
 - web address for, 333
- antispam efforts, example of, 257
- antispam legislation, significance of, 256–257.
See also spam
- antispyware applications. *See also* spyware
 - configuring, 131–132
 - maintaining with updates, 132
 - selecting, 130–131
- antivirus applications. *See also* viruses
 - ad blocking with, 200–201
 - advisory about installation of, 207
 - alternatives to, 207–208
 - analyzing communication protocols with, 200
 - configuring for chat and IM, 286–288
 - configuring Norton Internet Security Suite, 217–225
 - e-mail scanning with, 200
 - features of, 199
 - file scanning with, 199–200
 - finding trial offers for, 205–206
 - installing Norton Internet Security Suite, 209–217
 - operating and maintaining, 225–227
 - protecting AOL with, 291

- antivirus applications (*cont.*)
 - rating, 202
 - removing, 204
 - selecting appropriate features of, 202–203
 - stopping viruses with, 128–129
 - trial versions of, 203–206
- antivirus suites, features of, 203
- AOL (America Online)
 - protecting with antivirus applications, 291
 - spam filters provided by, 250
- application exceptions, enabling in Windows Firewall, 121
- applications. *See also* Microsoft applications
 - applying updates for, 194
 - locating updates for, 190–191
 - updating, 117
- attachments, examining in IM, 272
- attacks from Internet sources.
 - See also* blended threats; security
 - brute force attacks, 112
 - buffer overflows, 111
 - DDoS attacks, 113
 - DoS (denial of service), 113
 - logon attacks, 111–112
 - man-in-the-middle attacks, 112–113
 - port scans, 110
- auction fraud, preventing, 296
- auction winners and sellers, checking out when shopping online, 295–296
- auditing tools, evaluating security with, 135–136.
 - See also* security tools
- Automatic Updates. *See also* patches; updates
 - configuring, 180–182
 - features of, 116
 - functionality of, 180
 - settings available in, 181–182
 - turning off, 182
 - verifying application of, 182–183
 - viewing System Log in, 182–183
- Automatically Connect To Non-Preferred Networks box, significance of, 150

B

- background checks, running, 331
- banks
 - notifying about identify fraud, 326
 - receiving suspicious e-mail from, 259
- baseboards, pulling cable through, 59
- Bayesian filters
 - defeating spam filters with, 252–253
 - significance of, 260–261

- BBB (Better Business Bureau), searching online for complaints about retailers, 296–298
- best-of-breed antivirus applications, features of, 203
- BHOs (Browser Helper Objects), effect of, 130
- binary numbers, converting octets into, 64
- BITS (Background Intelligent Transfer Service), relationship to Automatic Updates, 180
- blackhole lists, relationship to spammers, 258
- blacklists
 - using with iHateSpam, 247–248
 - using with spam filters, 241
- blended threats, explanation of, 198.
 - See also* attacks from Internet sources; security
- bots
 - characteristics of, 110
 - identifying activity of, 198
- BPL (Broadband over Power Line), relationship to HomePlug, 61
- bridge card game, participation in, 12
- bridges, using in wireless networks, 82
- Brightmail
 - features of, 252
 - using with Adelphia ISP, 250
- broadcasts, address range associated with, 65, 95
- browsers
 - examples of, 131
 - using alternatives to, 334–338
- brute force attacks, effect of, 112
- buffer overflows
 - dangers of, 172
 - effect of, 111
- Bugtraq service, using, 193
- building materials, importance of, 37–38

C

- cable cutters, features of, 26
- cable ends, connecting, 60–61
- cable installation tools, types of, 25–27.
 - See also* Cat5 cable
- cable modems, features of, 14–15
- cable pulling techniques. *See also* pulling cable
 - for completed houses, 57–59
 - in new construction, 54–57
- cable routes
 - in frame wall, diagram of, 56
 - measuring, 42–43
 - planning, 36
- cable strippers, features of, 26
- cable testers, using with Cat5 cable, 27
- cables. *See also* wires
 - Cat5 cable, 20–27
 - fishing through walls, 59

- keeping from getting twisted, 56
 - roughing in, 55–56
 - stapling, 55
 - tools for connection of, 52–54
 - tools for pulling of, 51–52
- cablings
- selecting installation tools for, 50–54
 - using for data, 27–29
- CAN-SPAM Act, significance of, 256–257
- “cantennas,” building for wireless networks, 86
- career search sites, examples of, 312–313
- Cat5 cable. *See also* cable installation tools
- alternatives to, 61–62
 - characteristics of, 20
 - color codes used with, 20–21
 - connectors used with, 24–27
 - cross-section of, 53
 - inline couplers for, 25
 - installing without special tools, 28
 - keeping from getting twisted, 56
 - overview of, 19–20
 - preparing for termination, 53
 - tips for installation of, 21–24
 - using cable testers with, 27
- ceilings, pulling cable through, 59
- “certificate” programs, importance to online shopping, 298
- Change Scope dialog box, displaying in Windows Firewall, 120
- channel bonding
- advisory about, 84
 - explanation of, 39
 - of wireless networks, 160
- character sets, using with iHateSpam, 245
- chat. *See also* IRC (Internet Relay Chat)
- configuring antivirus applications for, 286–288
 - defending privacy in, 281–285
 - explanation of, 10–11
 - guidelines for children, 290
 - and IM (instant messaging), 264
 - obtaining first-party clients for, 268–269
 - preventing stalking and threats in, 291–292
 - risks associated with, 265–266
 - using common sense in, 283–284
- chat client applications, overview of, 266–267
- chat sessions, logging in Trillian, 280
- chatbots, guarding against in chat and IM, 282
- Checkmark antivirus product, obtaining, 202
- child protection, providing with antivirus applications, 201
- Citibank, fraud hotline for, 326
- clear channels, finding for wireless networks, 87
- clickstreams, definition of, 129
- clients, configuring for dynamic IP address allocation, 90–92
- color code standards, using with Cat5 cable, 20
- Comcast ISP, spam filters provided by, 250
- Commtouch, relationship to CAN-SPAM Act, 257
- communications protocols. *See also* multiprotocol devices; protocols
- analyzing with antivirus applications, 200
 - errors related to, 172–173
- Computer Management console, functionality of, 151
- computer systems, using Windows Update with, 176–179
- computer-program flaws
- buffer overflows, 171–172
 - communications protocol errors, 172–173
 - discovery by users or security researches, 174
 - exploitation of, 174–175
 - finding and patching, 174
 - in program design, 174
 - programming errors, 173–174
- computers
- configuring for wired networks, 63–70
 - listing when planning home networks, 32–35
 - naming for workgroup networking, 70–71, 100
 - renaming, 34
 - role in networks, 6–7
 - scanning with MBSA (Microsoft Baseline Security Analyzer), 126–127
- concentrators
- determining placement of, 45–46
 - examples of, 6
 - overview of, 16–18
 - purpose of, 5–6
- connections, finding in Network Connections folder, 77, 92
- contact lists, backing up in IM clients, 279–280
- Control Panel, selecting Network And Internet Connections area of, 65–66
- cookies
- effect of, 129
 - managing, 130
- cops
- contacting wiredcops.org, 292
 - reporting identity theft to, 327–328
- CouchSurfing.com, focus of, 309
- court records, availability of, 331
- crackers, definition of, 112
- credit card checks, identity-theft concerns related to, 321

- credit cards
 - protecting from identity theft, 317
 - protecting online, 307–309
- credit reporting bureaus
 - examples of, 322
 - placing fraud alerts with, 327
 - prescreening performed by, 324
- credit reports
 - fraud alerts in, 325
 - obtaining and examining, 322–324
 - receiving e-mail related to, 324
- crimes, contacting Cybercrime about, 292
- crimes of opportunity, WiFi hacking as, 163
- crimpers, features of, 54
- crosstalk, relationship to Cat5 cable, 20
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection), relationship to Ethernet, 16
- CVE (Common Vulnerabilities and Exposures) list, using, 191–192
- Cybercrime, web address for, 292

D

- data, transmitting with microwaves, 43
- DBAN disks, creating with Eraser utility, 321
- DCC (Direct Client-to-Client) functions, disabling in IRC, 273
- DDoS attacks
 - on blackhole lists, 258
 - effect of, 113
- defense in depth, protecting systems with, 137
- desktop antivirus applications, features of, 128
- devices. *See also* network device list; wireless network devices
 - adding to physical maps of home networks, 40–42
 - listing when planning home networks, 35
 - using wired Ethernet with, 46–47
 - using wireless networking technology with, 46
- DHCP (Dynamic Host Configuration Protocol)
 - assigning IP addresses with, 69
 - enabling to control IP addresses, 90
- dial-up modems, features of, 15–16
- dictionary attacks, effect of, 111–112
- digital signatures, monitoring executables for, 210
- directory networks, explanation of, 48
- Discover Desktop, features of, 308
- distance criteria
 - including on network maps, 42–43
 - relationship to network selection, 38
- DOCSIS (Data Over Cable Service Interface Specification) certification, explanation of, 14–15

- domain networks, explanation of, 48
- DoS (denial of service) attacks
 - effect of, 113
 - exploiting bugs for, 172
 - occurrence of, 172
- dots, using in IP addresses, 64
- downloads of Microsoft updates, web address for, 183
- drawings of home networks, creating, 40–42
- drill bits, pulling cable with, 51–52
- drivers, using with WiFi cards, 152–153
- DShield.org, enrolling logs in, 123, 135–136
- DSL modems, features of, 15
- ductwork, using plenum-rated cable in, 24
- dynamic addresses
 - configuring wireless networks for, 90–92
 - using in wired networks, 70
 - using in wireless networks, 98

E

- Earthlink, SpamBlocker utility provided by, 250
- egress filtering, relationship to firewalls, 134
- EIA/TIA color codes for Cat5 cable, explanation of, 20–21
- EICAR (European Institute for Computer Antivirus Research), downloading antivirus test files from, 204
- electrical cabling
 - disadvantages of, 55
 - using for data, 27–29
- Elk Cloner virus, origin of, 197
- e-mail. *See also* harvesting e-mail
 - costs associated with, 10
 - phishing of, 259
- e-mail addresses
 - protecting from spam, 233–236
 - protecting in IRC, 273
- e-mail antivirus scanning services, using, 207–208
- e-mail attachments, examining in IM, 272
- e-mail scanning, implementing with antivirus programs, 200
- encryption
 - enabling for wireless networks, 88–89, 156–163
 - and online shopping, 299
- encryption keys, using with WEP, 89
- Epinions, web address for, 298
- Equifax credit reporting bureau
 - placing fraud alerts with, 327
 - web address for, 322
- Eraser utility, downloading and using, 319–321

escrow services, using when shopping
 online, 295–296

Ethernet. *See also* high-speed Ethernet; wired Ethernet installations

- and CSMA/CD signaling technology, 16
- over power wiring, 61–62
- over telephone lines, 29
- over telephone wiring, 62
- using Homeplug standard with, 27–28

Ethernet device connectivity, verifying, 63

Ethernet hubs, features of, 16

Eudora, using iHateSpam with, 248

Excel spreadsheets, detecting viruses in, 227

exceptions, enabling in Windows Firewall, 119–121

Experian credit reporting bureau

- placing fraud alerts with, 327
- web address for, 322

external versus internal wireless adapters, 80–81

F

FACT (Fair and Accurate Credit Transactions) Act, significance of, 322

false negatives and positives, generating with spam filters in Outlook, 240

fiberglass, disadvantage of, 37–38

FightBack abuse monitoring system, features of, 135–136

File and Print Sharing, turning off on notebooks, 150–152

file attachments, examining in IM, 272

file scanning, implementing with antivirus programs, 199–200

file sharing, enabling, 71–74

files

- downloading safely over IM, 285–286
- sharing in wireless networks, 100–103
- sharing in workgroup networking, 71–74

financial institutions

- notifying about identify fraud, 326
- receiving suspicious e-mail from, 259

finish cabling, explanation of, 57

Firefox browser, features of, 337–338

firewall logs

- auditing, 135–136
- deciphering in Windows Firewall, 122–123
- managing in IM clients, 281

firewalls. *See also* Windows Firewall

- configuring, 134
- functionality of, 119
- installing, 134

- maintaining, 135
- selecting, 133
- using at home, 138
- versus Windows Firewall, 133

first-party clients

- obtaining for chat and IM, 268–269
- relationship to chat and IM, 266

fish bits, pulling cable with, 52

fish drills, installing cabling in existing walls with, 59

fish rods

- installing cabling in existing walls with, 57
- using with baseboards and raceways, 59

fish tapes and rods, pulling cable with, 51–52, 57, 59

floor plans, examples of, 40–41

folders

- sharing in wired networks, 72–74
- sharing in wireless networks, 100–103

fraud alerts

- appearance in credit reports, 325
- placing with credit reporting bureaus, 327

fraud information center, web address for, 295, 296

FreeScan antivirus scanner, using, 207–208

Friendster.com, focus of, 309–310

FTC (Federal Trade Commission)

- and fraud prevention, 296
- involvement in spam investigations, 256
- obtaining credit reports from, 322
- obtaining identity theft affidavit from, 327
- reporting identity theft to, 327–328

G

Gadu-Gadu aggregator client, web address for, 269

Gaim aggregator client

- downloading, 270–271
- updating, 279

games, participation in, 12

gateways. *See also* access points

- versus access points, 82
- changing SSIDs for, 147–149
- configuring for wireless networks, 90–92
- configuring WPA on, 158–159
- functionality of, 6
- overview of, 18
- password-protecting administration console of, 146–147

Gigabit Ethernet, features of, 39

Google's PhoneBook, removing contact information with, 332

H

hacker terminology, origin of, 112

hackers

- blocking with third-party Internet firewalls, 132–135

- blocking with Windows Firewall, 118–123

harassment or stalking online, getting help with, 291–292

hard drives, protecting from identity theft, 317–321

hardware firewalls, features of, 133

harvesting e-mail, effect of, 252.

See also e-mail

headers of spam, grabbing in Outlook Express, 253

heuristic analysis, implementing with antivirus programs, 199–200

hexadecimal, entering WEP keys with, 161–162

high-speed Ethernet, features of, 39. *See also*

Ethernet; wired Ethernet installations

Hill, Zachary Keith as phisher, 259

Hillery, Bob on firewalls for home use, 138

home address, taking offline, 332

home networks

- challenges to, 12–14

- connecting to Internet, 76–78

- constructing from pre-made patch cables, 28

- creating physical maps of, 39–44

- determining requirements for, 32–36

- planning for future expansions of, 35–36

- using firewalls in, 138

home runs, using with wired networks, 46

HomePlug standard

- significance of, 27–28

- speeds of, 61–62

- using with Ethernet, 61–62

HotJobs site, features of, 312

hubs, purpose of, 16

I

IANA (Internet Assigned Numbers Authority), web address for, 111

ICQ first-party client

- configuring spam control settings in, 275–276

- creating personal profile in, 284

- downloading, 268

- updating, 277

ICS (Internet Connection Sharing), protecting addresses with, 117–118

ICSA Labs, testing of antivirus products by, 202

Identd servers, limiting in IRC, 274

identity theft

- protecting against, 325–328

- reporting to agencies, 327–328

- safeguarding information against, 317–326

- statistics related to, 316

identity thieves, guarding against in chat and IM, 282

IDSs (intrusion detection systems)

- in antivirus applications, 201

- features of, 136

IE (Internet Explorer). *See* Internet Explorer

IEEE standards for wireless networks, overview of, 142–143

iHateSpam

- downloading and installing, 245–246

- features of, 244–245

- filtering spam with, 246–249

- reporting spam with, 251

IM automation, avoiding, 272

IM buddy lists, protecting from spim, 275–277

IM habits, improving, 271–272

IM (instant messaging) applications

- backing up contact lists and settings in, 279–280

- and chat, 264

- configuring antivirus applications for, 286–288

- creating personal profiles for, 284–285

- defending privacy in, 281–285

- downloading files safely for, 285–286

- examples of, 10

- logging conversations in, 280

- managing message logs in, 281

- obtaining first-party clients for, 268–269

- overview of, 266–267

- preventing stalking and threats in, 291–292

- protecting against viruses, Trojans, and

- worms, 270–272

- risks associated with, 265

- updating, 277–279

- using, 269

- using common sense in, 283–284

- vulnerability to spammers, 262

“In the Wild” viruses, explanation of, 202

InfoSec News, web address for, 159

infrastructure mode, keeping laptops in, 149–150

inline couplers, using with Cat5 cable, 25, 28

installation files, unpacking and downloading for

Norton Internet Security Suite, 210–211

internal versus external wireless adapters, 80–81

Internet

- connecting wireless networks to, 89–94

- significance of, 8–12

Internet chat. *See* chat; IRC (Internet Relay Chat)

Internet Connection Firewall. *See* Windows Firewall

Internet connections

- configuring and sharing in wired networks, 76–78

- configuring and sharing in wireless networks, 92–94

Internet Explorer
 accessing Windows Update with, 175
 alternatives to, 131
 downloading Office updates with, 185–190
 Privacy settings in, 304
 verifying security certificates with, 299

Internet firewalls. *See* firewalls

Internet gateways. *See* gateways

Internet Protocol (TCP/IP) Properties dialog box,
 displaying, 68

Internet Security. *See* Norton Internet Security Suite

IP addresses
 assigning with DHCP, 68
 changing when enabling Internet Connection
 Sharing, 78, 94
 configuring, 68
 controlling with DHCP, 90
 explanation of, 64
 hiding in chat and IM, 283
 versus MAC addresses, 166
 protecting with ICS, 117–118

IP fragment attacks, dynamics of, 172–173

IP (Internet Protocol), relationship of ports to, 111

IP packet attacks, dynamics of, 173

IRC (Internet Relay Chat). *See also* chat
 explanation of, 10–11
 risks associated with, 265
 security of, 272–274

ISawYou.com, focus of, 309

ISP lawsuits, filing against spammers, 258

ISP spam filtering services, using, 249–251

J

Jabber aggregator client, web address for, 269

jacks, inserting wires into, 60

job hunting, maintaining privacy in process of, 311–314

junk mail. *See* spam

Justice Department's Cybercrime, web address
 for, 292

K

key provisioning, relationship to WEP keys, 162

L

LANs (local area networks), definition of, 6

laptops
 configuring WPA on, 158–159
 keeping in infrastructure mode, 149–150
 turning off File and Print Sharing in, 150–152

layered defenses, establishing, 137

LinkedIn.com, focus of, 309

Linksys Internet gateways, configuring, 90–92

LiveUpdate
 checking for updates with, 223–224
 configuring setting sin, 214
 launching in Norton Internet Security
 Suite, 219–220

Local Area Connection icon, displaying, 67

log files
 auditing, 135–136
 deciphering in Windows Firewall, 122–123
 managing in IM clients, 281

logging, enabling in Windows Firewall, 122–123

logical maps, creating for networks, 45–47

logon attacks, effect of, 111–112

Lynx browser, features of, 337–338

M

MAC addresses
 character pairs in, 165
 identifying, 165

MAC (Media Access Control) filtering
 capabilities and limitations of, 166
 overview of, 163–166

macros, appearance as indicators of viruses, 227

Mailinator service, web address for, 233, 235

mailing lists, explanation of, 9

MakeOutClub.com, focus of, 309

malware
 definition of, 109
 examples of, 198
 protecting chat and IM from, 285

man-in-the-middle attacks, effect of, 112–113

maps
 accounting for distances on, 42–43
 creating, 39–44
 logical maps, 45–47
 physical maps, 39–44

MasterCard SecureCode, features of, 308

Matterform Media's Spamfire, significance of, 251

MBSA (Microsoft Baseline Security Analyzer)
 downloading, 123
 installing, 124–125
 using, 125–127

message logs, managing in IM clients, 281

metallic materials, signal attenuation by, 37

Microsoft applications, locating and downloading
 updates for, 183–185. *See also* applications

Microsoft Downloads, web address for, 183

microwaves, transmitting data with, 43

Miranda IM aggregator client
 downloading, 270
 updating, 279

mIRC

- securing, 288–289, 291
- stopping from launching browsers, 274
- web address for, 273

MIT (Massachusetts Institute of Technology),

- relationship of hacker term to, 112

modems

- functionality of, 6
- types of, 14–16

Monster.com site, features of, 312**Mozilla browser**

- downloading, 271
- features of, 336
- privacy preferences in, 304–305
- verifying security certificates with, 300, 302

MSN Hotmail and MSN Premium/Plus, spam filters

- provided by, 250

MSN Messenger first-party client

- configuring privacy settings in, 276
- downloading, 269
- updating, 278

multiprotocol clients

- obtaining for IM, 270
- updating, 278–279
- using with IM and chat applications, 267, 269

multiprotocol devices, advantages of, 84. *See also*

- communications protocols; protocols

multiservice clients

- obtaining for IM, 270
- updating, 278–279
- using with IM and chat applications, 267, 269

MySimon, web address for, 298

N**NAS (Network Attached Storage), significance of, 33****NAT (Network Address Translation)**

- features of, 117–118
- significance of, 18

National Fraud Information Center, web address for, 295**Netscape browser**

- features of, 335
- privacy preferences in, 304–305
- verifying security certificates with, 300

NetStumbler, surveying wireless networks with, 154–155**network addresses. *See* IP addresses****Network And Internet Connections area of Control Panel, choosing, 65–66****network antivirus applications, features of, 129****network cabling**

- selecting installation tools for, 50–54
- using for data, 27–29

network cards, finding MAC addresses of, 165**network collisions, limiting with switches, 17****Network Connections folder, finding connections**

- in, 77

network costs, cutting, 12–13**network device list, example of, 35. *See also* devices;**

- wireless network devices

network ID, address range associated with, 65, 95**network maps**

- accounting for distances on, 42–43
- creating, 39–44
- logical maps, 45–47
- physical maps, 39–44

network selection

- distance criteria in, 38
- security implications for, 38

network technologies, factors related to, 36**network utilization plans, creating, 47****networking equipment, connecting, 62****networks**

- components of, 5
- creating logical maps of, 45–47
- functionality of, 8
- protecting with, 119
- reducing complexity of, 13–14
- role of computers and PDAs in, 6–7

new construction cabling, pulling, 54–57**newsgroups, explanation of, 9****NeWT vulnerability scanner, web address for, 135****NEXT (near-end crosstalk), avoiding, 60****Norton Internet Security Suite**

- configuring, 217–225
- configuring real-time protection in, 223–224
- installing, 209–217
- launching after configuration of, 221
- obtaining updates for, 222–223
- performing scheduled scans with, 224–225
- unpacking and downloading installation files for, 209–212

notebooks. *See* laptops**NtServicePack events, searching in Automatic Updates, 183**

O**octet, definition of, 64, 95****“off by default,” significance to firewalls, 119****Office Update**

- downloading with Internet Explorer, 185–190
- using, 186–190
- web address for, 186

“old work” boxes, using for existing walls, 58–59**online antivirus scanners, using, 207****online harassment or stalking, getting help**

- with, 291–292

- online shopping security
 - checking out auction winners and sellers, 295–296
 - overview of, 294–295
 - and privacy policy complaints, 306–307
 - protecting credit cards, 306–307
 - reading web-site privacy policies, 301–303
 - searching BBB online for complaints about retailers, 296–298
 - for trustworthy sites, 298
 - verifying security certificates, 299–301
- Opera browser, features of, 336–337
- operating systems
 - keeping up to date, 137
 - maintaining security of, 175–183
 - relationship to networks, 7
 - using Automatic Updates with, 179–183
- opinion sites, consulting when shopping online, 298
- “opt-out” line, contacting, 324
- outbound ports, blocking, 134
- Outlook
 - using iHateSpam with, 248
 - using SpamNet with, 241–242, 244
- Outlook Express
 - grabbing spam headers in, 253
 - using iHateSpam with, 248
 - using spam filters in, 237–240
 - using SpamNet with, 241–242, 244

P

- P2P networking
 - benefits of, 48
 - setting up in wired networks, 70
 - setting up in wireless networks, 99–100
 - sharing files in, 71–74
- P3P (Platform for Privacy Preferences), significance of, 304
- paper records, shredding to prevent identity theft, 317
- passwords
 - changing in gateways, 146–148
 - protecting in chat and IM, 283
- patches. *See also* Automatic Updates; updates
 - advisory about, 176
 - downloading, 183–185
 - importance of, 170–171
 - preventing receipt of spam with, 234
 - using Automatic Updates with, 179–183
- pattern detection, implementing with antivirus programs, 199
- PC Card adapters, using with wireless networks, 81
- PDAs (personal digital assistants), role in networks, 6–7
- peer-to-peer networking
 - benefits of, 48
 - setting up in wired networks, 70
 - setting up in wireless networks, 99–100
 - sharing files in, 71–74
- penetration testing tools, testing defenses with, 135
- peopledata.com, running background checks with, 331
- personal information, protecting in chat and IM, 282
- personal profiles, creating for IM clients, 284–285
- Pervade virus, origin of, 197
- phishing
 - avoiding, 333
 - dealing with, 333–334
 - origin of, 259
 - relationship to spam, 253
- phone numbers, taking offline, 332
- PhoneBook in Google, removing contact information with, 332
- physical maps, creating for networks, 39–44
- plenum-rated cable, using in ductwork, 24
- police
 - contacting wiredcops.org, 292
 - reporting identity theft to, 327–328
- pop-up blockers
 - in antivirus applications, 200–201
 - managing spyware with, 130
- port exceptions, configuring with Windows Firewall, 119–121
- port scans and ports, explanation of, 110–111
- ports, blocking for outbound traffic, 134
- power wiring, Ethernet over, 61–62
- pre-authentication, relationship to WPA2 encryption scheme, 142–143
- PriceGrabber, web address for, 298
- printers
 - sharing in wired networks, 75–76
 - sharing in wireless networks, 103–104
- Privacy Bird, web address for, 305
- Privacy Companion, web address for, 305
- privacy, defending in chat and IM, 281–285
- Privacy Guard, using with Norton Internet Security Suite, 219
- privacy, maintaining while job hunting, 311–314
- privacy policies
 - composing complaints about, 306–307
 - importance to online shopping, 298
 - matching to personal preferences, 303–305
 - for online shopping, 301–307
 - relationship to spam, 234
 - statistic related to, 303–304
 - voicing objections to, 305–306
- privacy protection, providing with antivirus applications, 201

privacy settings

- configuring in AIM, 277
- configuring in MSN Messenger, 276
- configuring in Yahoo Messenger, 276–277

private address ranges, examples of, 65

private information, protecting, 329

program failure states, occurrence of, 172

program flaws. *See* computer-program flaws

programming errors, occurrence of, 173–174

programs. *See* applications

promiscuous mode, switching WiFi cards into, 154

protocols, role in networks, 7–8. *See also*

- communications protocols; multiprotocol devices

public WiFi networks, security risks associated with, 157

pulling cable, tools for, 51–52. *See also* cable pulling techniques

punch-down connectors, using with Cat5 wall jacks, 24

punch-down tools, using with cable, 27, 54

Q

quarantine, accessing in iHateSpam, 246–247

R

raceways, pulling cable through, 59

radio interference, sources of, 85

radio signal strength

- checking, 143–144
- listing with NetStumbler, 155

RADIUS (Remote Authentication Dial-In User Service), using with wireless networks, 89

RBLs (real-time blackhole lists), blocking spam with, 250–251

read me notes, locating for Norton Internet Security Suite, 217

real-time scanning, configuring in Norton Internet Security Suite, 223–224

receive lines, relationship to Cat5 cable, 20

Registry, protecting from spyware, 131

remote locations, installing antennas to, 45

removable media, destroying to prevent identity theft, 317–321

repeaters, extending coverage of wireless networks with, 86

résumé sites

- dos and don'ts for, 313–314
- examples of, 312–313

retailers, rating when shopping online, 298

RJ-45 connectors, using with Cat5 cable, 19–20, 24

RJ-45 jacks, using with Cat5 cable, 24–25

RJ-45 crimp tools, features of, 25–26

RJ-45 plugs, terminating, 61

roughing in cabling, 54–56

routers. *See* gateways

rules, creating for spam filters in Outlook Express, 237–240

rules-based scoring filters, relationship to spam, 260

Rx lines, relationship to Cat5 cable, 20

S

Salem, Enrique on Brightmail, 252–253

Sam Spade, investigating spam with, 254–255

Sandvine, statistics on source of spam, 260–261

savings, protecting from identity fraud, 326

SBC Yahoo, spam filters provided by, 251

scammers, threats posed to chat and IM by, 282

Scan for Viruses screen, displaying in Norton Internet Security, 224–225

Scob worm, effect of, 198–199

screen scrapers, guarding against in chat and IM, 282

scripts

- identifying, 289
- protecting when using mIRC, 289

SDKS (Synchronous DSL), features of, 15

“seal” programs, importance to online shopping, 298

security. *See also* attacks from Internet sources;

- blended threats
 - analyzing with MBSA, 123–127
 - of chat and IM, 285–292
 - configuring wireless hardware for, 146–155
 - configuring wireless networks for, 142
 - of data over wireless connections, 156–168
 - evaluating with third-party auditing tools, 135–136
 - implications for network selection, 38
 - of IRC, 272–274
 - of non-Microsoft applications, 190–194
 - of online shopping, 294–301
 - of operating systems, 175–183
 - of public WiFi networks, 157
 - and socializing online, 309–311
 - of wireless networks, 140–141

Security Center

- auditing system security with, 114–115
- configuring alerts and warnings in, 115–116
- overview of, 113–114

security certificates

- importance to online shopping, 299
- verifying with Internet Explorer, 299

Security Focus, features of, 192–193

security patches. *See* patches

- security risks. *See also* attacks from Internet sources
 - overview of, 108
 - spyware, 110
 - Trojan horses, 109–110
 - viruses, 109
 - worms, 109
 - zombies and bots, 110
- security suites, features of, 203
- security tools. *See also* auditing tools
 - antispyware applications, 129–132
 - antivirus applications, 128–129
 - overview of, 113
 - Security Center, 113–116
- security updates. *See* updates
- sensitive data, protecting, 329–338
- Serial Number item, verifying with Internet Explorer, 299, 301
- Server service, disabling, 151–152
- services, listing, 151
- ShareDemo Properties dialog box, displaying, 72, 100
- “sharing hand”
 - appearance under folders, 74, 102
 - appearance under printers, 76, 104
- shopping. *See* online shopping security
- shredders, using to prevent identity theft, 317, 319–320
- signal attenuation
 - causes and minimization of, 85
 - significance of, 37
- signal range, extending in wireless networks, 86
- signal strength
 - checking, 143–144
 - listing with NetStumbler, 155
- signals, visualizing, 43–44
- Simple File Sharing, enabling, 71–74, 100–103
- site surveys, performing for wireless network devices, 87
- SMS spam, significance of, 262
- SneakEmail service, web address for, 233, 235
- social engineering, guarding against in chat and IM, 283
- social networking
 - goals of, 309
 - rules for, 310–311
- Social Security Administration, reporting identity theft to, 327–328
- software firewalls, features of, 133
- software, lifecycle of, 174–175
- SP2 (Service Pack 2), downloading, 144
- spam. *See also* antispam legislation
 - and Active Content, 253
 - avoiding receipt of, 233–236
 - fighting, 233, 256–262
 - investigating with Sam Spade, 254–255
 - occurrence in foreign languages, 252
 - origin of, 232
 - protecting e-mail addresses from, 233
 - relationship to viruses, 261–262
 - reporting to authorities, 251, 253–256
 - source of, 260–261
 - statistics related to, 232
 - tracking by organizations, 251
- spam control settings, configuring in ICQ, 275–276
- spam filters
 - future of, 260–261
 - iHateSpam, 244–249
 - overview of, 236
 - shopping around for, 240–241
 - SpamNet, 241–244
 - using free or available types of, 237–240
 - using ISPs as, 249–251
- spam headers
 - and Bayesian filters, 261
 - grabbing in Outlook Express, 253
- Spam Zombies
 - significance of, 260–261
 - as threats to chat and IM, 282
- SpamBlocker filter, features of, 250
- Spamcop, features of, 254
- SpamCrime, web address for, 251
- Spamfire, significance of, 251
- spammers
 - activities of, 232–233, 255, 262
 - backlash by, 258–261
 - preventing exploits by, 258
- Spamming Bureau, advisory about, 255
- SpamNet
 - downloading and installing, 241–242
 - filtering spam with, 242–244
- Speakeasy ISP, spam filters provided by, 251
- speed, considering requirements for, 38–39
- speed limit, breaking in wireless networks, 84
- spim (spam over IM)
 - protecting IM buddy lists from, 275–277
 - significance of, 262
- Spitzer, Eliot and antispam efforts, 257
- spybots, effect of, 198
- spyware. *See also* antispyware applications
 - effect of, 129, 198
 - explanation of, 110
- spyware goons, guarding against in chat and IM, 282
- spyware risk level, determining, 129–130
- SSIDs (server set IDs)
 - changing for gateways, 147–149
 - configuring for wireless networks, 88
- SSL encryption, importance to online shopping, 298
- SSL security certificates, importance to online shopping, 299

stalking and threats, preventing in chat and IM, 291–292

stand-alone antivirus applications, features of, 203

staple guns, obtaining, 55

static addresses

- using with wired networks, 65–69
- using with wireless networks, 95–98

streaming media, explanation of, 11

strippers, connecting cables with, 52–54

Super G, speed of, 84

Survival Time statistic in DSHeild, explanation of, 136

switches, using to limit network collisions, 17

Symantec's Norton Internet Security Suite.

- See* Norton Internet Security Suite

System Log, viewing in Automatic Updates, 182

System Properties dialog box

- displaying computer names in, 33
- displaying for Automatic Updates, 180

System Restore utility, using with antivirus applications, 204

T

T568A standard, relationship to Cat5 cable, 20–21

TCP/IP addressing, managing, 63–70

telephone cabling

- Ethernet over, 62
- using for data, 29

termination, preparing end of Cat5 cables for, 53

third-party firewalls. *See* firewalls

threats and stalking, preventing in chat and IM, 291–292

tools

- for connecting cables, 52–54
- for installing cabling, 25–27, 50–54
- for pulling cable, 51–52
- punch-down tools, 27, 54
- RJ-45 crimp tools, 25–26

transmission distances, examples of, 38

transmit lines, relationship to Cat5 cable, 20

TransUnion credit reporting bureau

- placing fraud alerts with, 327
- web address for, 322

trial offers, finding for antivirus applications, 205–206

Trillian aggregator client

- downloading, 270
- logging chat sessions in, 280
- updating, 279

Trojan horses

- explanation of, 109–110
- identifying activity of, 198

troubleshooting

- WEP connection problems, 162–163
- WPA connection problems, 159–160

Turbo, speed of, 84

Tx lines, relationship to Cat5 cable, 20

Type 110 punch-down terminals, relationship to RJ-45 jacks, 27

U

UNIVAC virus, origin of, 197

updates. *See also* Automatic Updates; patches

- of aggregator clients, 278–279
- applying for non-Microsoft software, 194
- controlling virus outbreaks with, 226
- downloading for Office applications, 185–190
- for first-party clients, 277–278
- locating and downloading for Microsoft applications, 183–185
- obtaining for Norton Internet Security, 222–223
- types of, 116–117

USB ports, conserving, 81

Usenet groups, using free Web mail addresses with, 236

user agents, relationship to privacy policies, 305

V

vanity searches, unlisting oneself from, 330–332

VeriSign, web address for, 299

Virus Checker in AIM, using, 287–288

viruses. *See also* antivirus applications

- acting on detection of, 226–227
- acting on suspicion of, 225, 227
- detecting in spreadsheets, 227
- explanation of, 109
- first occurrence of, 196–197
- identifying activity of, 197
- “In the Wild;” 202
- and spam, 261–262
- using manual updates with, 226

Visa Verified By program, features of, 309

Voices from the Community

- The Importance of Teaching Kids How to Chat Safely, 290
- A Spam-warrior's Look at Trends in Spam, 252–253
- Why Do I Need a Firewall at Home?, 138

VoIP (Voice over Internet Protocol), significance of, 11

vulnerability scanners, example of, 135

W

Walker, John and Pervade virus, 197

wall jacks, connecting, 60

- walls, fishing cable through, 57, 59
- WANs (wide area networks), 6
- WAPs (wireless access points)
 - centering, 44
 - standards for, 17–18
- warnings, configuring in Security Center, 115–116
- Way Back Machine, web address for, 310
- web beacons, relationship to spam, 252
- web pages, description of, 8
- web, researching history of, 310–311
- web servers, purpose of, 8
- web sites
 - AIM (AOL Instant Messenger), 268
 - Anti-Phishing Working Group, 333
 - BBB (Better Business Bureau), 296
 - credit reporting bureaus, 322
 - Cybercrime, 292
 - Discover Desktop, 308
 - EICAR (European Institute for Computer Antivirus Research), 204
 - Epinions, 298
 - Eraser utility, 319
 - finding information on, 8–9
 - Firefox browser, 337
 - FTC (Federal Trade Commission), 296, 328
 - FTC spam collection, 256
 - Gadu-Gadu aggregator client, 269
 - Gaim aggregator client, 270
 - IANA (Internet Assigned Numbers Authority), 111
 - ICQ first-party client, 268
 - Identity Theft Resource Center, 316
 - iHateSpam, 245
 - InfoSec News, 159
 - Jabber aggregator client, 269
 - Lynx browser, 337
 - Mailinator, 233, 235
 - MasterCard SecureCode, 308
 - Microsoft Downloads, 183
 - Miranda IM aggregator client, 270
 - mIRC, 273
 - Mozilla browser, 271, 336
 - MSN Messenger first-party client, 269
 - MySimon, 298
 - National Fraud Information Center, 295
 - Netscape browser, 335
 - NetStumbler, 154
 - NeWT vulnerability scanner, 135
 - Office Update, 186
 - Opera browser, 336
 - PriceGrabber, 298
 - Privacy Bird, 305
 - Privacy Companion, 305
 - Sam Spade, 254
 - script download sites, 289
 - Security Focus, 192
 - SneakEmail, 233, 235
 - for social networking, 309
 - Social Security Administration, 328
 - SpamCrime, 251
 - Spamming Bureau, 255
 - SpamNet, 241
 - Trillian aggregator client, 270
 - VeriSign, 299
 - Way Back Machine, 310
 - West Coast Labs, 202
 - WildList organization, 202
 - Windows Update, 175
 - Windows XP Wireless Rollup patch, 159, 162
 - wiredcops.org, 292
 - WiredSafety, 292
 - wireless networking troubleshooting page, 162
 - Yahoo Messenger first-party client, 269
 - ZoneAlarm, 261
 - ZoneAlarm firewall, 291
- well-known ports, examples of, 111
- WEP connection problems, troubleshooting, 162–163
- WEP keys, entering in hexadecimal, 161–162
- WEP (Wired Equivalent Protection) standard
 - configuring, 161–162
 - overview of, 89, 160
- West Coast Labs, Checkmark antivirus product
 - offered by, 202
- whitelists
 - using with iHateSpam, 247–248
 - using with spam filters, 240
 - using with SpamNet, 244
- WHOIS lookups, finding web addresses with, 297
- WHQL-certified drivers, using with WiFi cards, 152–153
- WiFi cards
 - switching into promiscuous mode, 154
 - using WHQL-certified drivers for, 152–153
- WiFi channels, number of, 155
- WiFi hacking, considering as crime of opportunity, 163
- WiFi networks. *See* wireless networks
- WildList organization, web address for, 202
- Windows Firewall
 - configuring, 119–121
 - enabling logging in, 122–123
 - overview of, 118–119

- Windows Update
 - accessing with Internet Explorer, 175
 - advisory about web site for, 176
 - features of, 116
 - functionality of, 175
 - updating systems with, 176–179
 - web address for, 175
- Windows XP
 - and DHCP (Dynamic Host Configuration Protocol), 69
 - enabling Simple File Sharing in, 71–74, 100–103
 - setting up workgroup networking in, 70–71
 - using dynamic addresses in, 70
 - using static addresses in, 65–69
- Windows XP Wireless Rollup patch, installing, 159, 162
- wired Ethernet installations. *See also* Ethernet; high-speed Ethernet
 - applications for, 37
 - devices used with, 46–47
 - planning cable routes for, 36
- wired networks
 - cable pulling techniques for, 54–59
 - configuring computers for, 63–70
 - connecting cable ends in, 60–61
 - connecting to Internet, 76–78
 - installing cabling for, 50–54
 - managing TCP/IP addressing in, 63–70
 - naming computers in, 70
 - naming workgroups in, 70
 - selecting address ranges for, 64–65
 - setting up workgroup networking in, 70–71
 - sharing files and folders in, 71–74
 - sharing printers in, 75–76
 - using dynamic addresses in, 70
 - using Ethernet over HomePlug with, 61
 - using Ethernet over telephone wiring with, 62
 - using home runs with, 46
 - using static addresses in, 65–69
- WiredSafety, web address for, 292
- wireless card drivers, using with WiFi cards, 152–153
- wireless Ethernet
 - choosing, 83–84
 - using microwaves with, 43
- wireless Ethernet equipment
 - access points versus gateways, 82–83
 - bridges, 82
 - internal versus external wireless adapters, 80–81
 - wireless Ethernet signals, getting to network devices, 43–44
- wireless hardware
 - configuring for security, 146–155
 - security considerations related to, 143–145
- Wireless Network Connections profile, entering WPA paraphrases into, 158–159
- wireless network devices. *See also* devices; network device list
 - configuring, 86–89
 - performing site surveys for, 87
 - placing for best reception, 85–86
- wireless network tool, changes made to, 144–145
- wireless networks
 - configuring computers for, 94–98
 - configuring for security, 142
 - configuring routers for, 90–92
 - configuring SSIDs for, 88
 - connecting to Internet, 89–94
 - cutting through traffic jams in, 155
 - devices used with, 46
 - enabling encryption in, 88–89
 - extending signal range in, 86
 - finding clear channels for, 87
 - IEEE standards for, 142–143
 - managing TCP/IP addressing in, 94–98
 - naming computers in, 99
 - naming workgroups in, 99
 - security overview of, 140–141
 - setting up workgroup networking in, 99–100
 - sharing, 167–168
 - sharing printers in, 103–104
 - surveying with NetStumbler, 154–155
 - troubleshooting, 162
 - using dynamic addresses in, 98
 - using in public places, 157
 - using static addresses in, 95–98
- wires, inserting into jacks, 60. *See also* cables
- WLAN Utility, displaying signal strength with, 144–145
- workgroup networking
 - benefits of, 48
 - setting up in wired networks, 70
 - setting up in wireless networks, 99–100
 - sharing files in, 71–74
- workgroups
 - naming, 70–71
 - naming in wired networks, 99
 - naming in wireless networks, 99

worms

- explanation of, 109
- identifying activity of, 198
- WPA connection problems, troubleshooting, 159–160
- WPA passphrases, entering into Wireless Network Connections profile, 158–159
- WPA versus WEP gateway security settings, 161
- WPA (Wi-Fi Protected Access) standard
 - configuring on gateways and laptops, 158–159
 - overview of, 89, 156
 - requirements for, 156–158
- WPA2 (WiFi Protected Access 2), relationship to wireless networks, 142
- WPA-PSK (Pre-Shared Key), significance of, 158

X

- Xtreme G, speed of, 84

Y

- Yahoo! HotJobs site, features of, 312
- Yahoo Messenger first-party client
 - configuring privacy settings in, 276–277
 - downloading, 269
 - updates, 278

Z

- zombies
 - explanation of, 110
 - identifying activity of, 198
- ZoneAlarm firewall
 - using with AOL, 291
 - web address for, 261
- ZoneLog Analyser, using, 135

INTERNATIONAL CONTACT INFORMATION

AUSTRALIA

McGraw-Hill Book Company
Australia Pty. Ltd.
TEL +61-2-9900-1800
FAX +61-2-9878-8881
<http://www.mcgraw-hill.com.au>
books-it_sydney@mcgraw-hill.com

CANADA

McGraw-Hill Ryerson Ltd.
TEL +905-430-5000
FAX +905-430-5020
<http://www.mcgraw-hill.ca>

GREECE, MIDDLE EAST, & AFRICA (Excluding South Africa)

McGraw-Hill Hellas
TEL +30-210-6560-990
TEL +30-210-6560-993
TEL +30-210-6560-994
FAX +30-210-6545-525

MEXICO (Also serving Latin America)

McGraw-Hill Interamericana Editores
S.A. de C.V.
TEL +525-1500-5108
FAX +525-117-1589
<http://www.mcgraw-hill.com.mx>
carlos_ruiz@mcgraw-hill.com

SINGAPORE (Serving Asia)

McGraw-Hill Book Company
TEL +65-6863-1580
FAX +65-6862-3354
<http://www.mcgraw-hill.com.sg>
mghasia@mcgraw-hill.com

SOUTH AFRICA

McGraw-Hill South Africa
TEL +27-11-622-7512
FAX +27-11-622-9045
robyn_swanepoel@mcgraw-hill.com

SPAIN

McGraw-Hill/
Interamericana de España, S.A.U.
TEL +34-91-180-3000
FAX +34-91-372-8513
<http://www.mcgraw-hill.es>
professional@mcgraw-hill.es

UNITED KINGDOM, NORTHERN, EASTERN, & CENTRAL EUROPE

McGraw-Hill Education Europe
TEL +44-1-628-502500
FAX +44-1-628-770224
<http://www.mcgraw-hill.co.uk>
emea_queries@mcgraw-hill.com

ALL OTHER INQUIRIES Contact:

McGraw-Hill/Osborne
TEL +1-510-420-7700
FAX +1-510-420-7703
<http://www.osborne.com>
omg_international@mcgraw-hill.com

Sound Off!

Visit us at **www.osborne.com/bookregistration** and let us know what you thought of this book. While you're online you'll have the opportunity to register for newsletters and special offers from McGraw-Hill/Osborne.

We want to hear from you!

Sneak Peek

Visit us today at **www.betabooks.com** and see what's coming from McGraw-Hill/Osborne tomorrow!

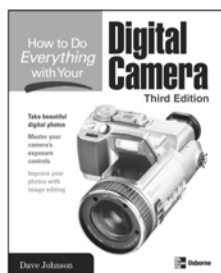
Based on the successful software paradigm, Bet@Books™ allows computing professionals to view partial and sometimes complete text versions of selected titles online. Bet@Books™ viewing is free, invites comments and feedback, and allows you to "test drive" books in progress on the subjects that interest you the most.

OSBORNE DELIVERS RESULTS!

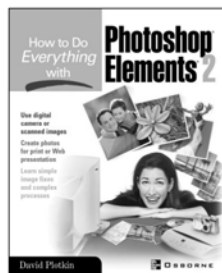


OSBORNE
www.osborne.com

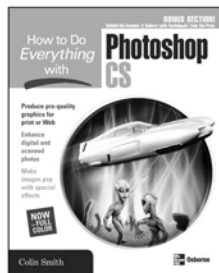
Know How



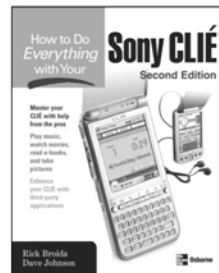
How to Do Everything with Your Digital Camera
Third Edition
ISBN: 0-07-223081-9



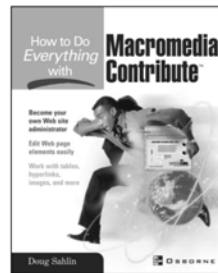
How to Do Everything with Photoshop Elements 2
ISBN: 0-07-222638-2



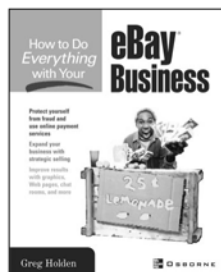
How to Do Everything with Photoshop CS
ISBN: 0-07-223143-2
4-color



How to Do Everything with Your Sony CLIE
Second Edition
ISBN: 0-07-223074-6



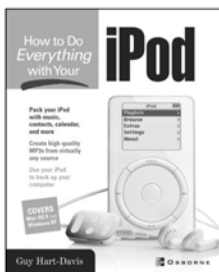
How to Do Everything with Macromedia Contribute
0-07-222892-X



How to Do Everything with Your eBay Business
0-07-222948-9



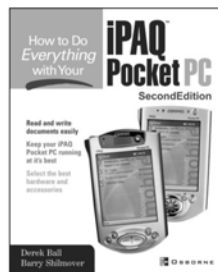
How to Do Everything with Illustrator CS
ISBN: 0-07-223092-4
4-color



How to Do Everything with Your iPod
ISBN: 0-07-222700-1



How to Do Everything with Your iMac,
Third Edition
ISBN: 0-07-213172-1



How to Do Everything with Your iPAQ Pocket PC
Second Edition
ISBN: 0-07-222950-0

OSBORNE DELIVERS RESULTS!

**Mc
Graw
Hill** **Osborne**
www.osborne.com

Create, Protect, and Manage Your Passwords

Passwords, like death, taxes, and Elvis impersonators at Vegas weddings, are an inescapable fact of life in the twenty-first century. If you're like most people, you have no trouble coming up with passwords for all the web sites, programs, and computers you need to access. The challenge, for you and many other people, is to come up with passwords that are hard for the bad guys to simply guess or easily figure out, and to keep track of them. We'll teach you how to do just that in this spotlight section, in addition to showing you some cool products you can use to help you along the way, so get out your #2 pencils and some scrap paper, and get ready to start making up ingenious passwords.

Who Needs a Tough Password, Anyway?

Chances are, if I know a little bit about you, I can guess the password you use most frequently within three guesses. If you think you're being stealthy using your child's name, your wedding anniversary, your pet's name, or some equally mundane piece of personal data as a password, think again. In a *PC World* survey of 1,500 Internet-using adults, 30 percent of people use a date that's important to them as their password, and 26.8 percent use the name of a person or pet they know as their password. That means, if I know a few of your personal details, I can guess your password correctly more than half the time.

Even if I don't know anything about you, I know the first place I'm going to look for a password: that yellow sticky note taped under your keyboard (or worse, right onto the front of your monitor). Really, what's the point of having a password at all if you're going to make it so easy for me to find it?

In reality, we all use passwords for a multitude of purposes throughout the day. Your ATM card's PIN is a password, as is the string of text you have to enter to log into your PC, read an online news story, view your e-mail messages, pay bills at your bank's web site, or even add movies to your Netflix queue. Virtually everything you do online requires you to use a password at one time or another, and most of us use the same password (or a small number of them) for everything.

That's a bad idea, because if the bad guys crack the password you use at Netflix, for example, they won't only be able to rearrange the order of the movies you'll get, they could try it out on all your other accounts, and statistically speaking, they're likely to hit gold if they try. Some of these passwords protect really critical stuff, like your bank account (or your Netflix movie queue), so making lots of different, tough passwords is the safest way to go.

If you haven't figured it out yet, the answer to the question posed by the name of this section is this: Everyone needs tough passwords, and a good way to keep track of them.

Organize and Store Your Passwords

Before we get into the details of making up new passwords, you should get your house in order with the passwords you already use. A number of tools can help you accomplish this task (some are free, some cost a little money), so we'll go over the options for keeping track of passwords, and their relative merits, in this section.

Store Passwords Using Windows XP

You need look no further than Windows XP itself if you want a bare-bones, simplistic password keeper. While Windows won't help you come up with hard-to-guess passwords, it can automatically remember and enter the passwords into certain forms in web pages through Internet Explorer, or when you log into home or business networks. Click Start | Settings | Control Panel, and then open the User Accounts applet, as shown in Figure 1.

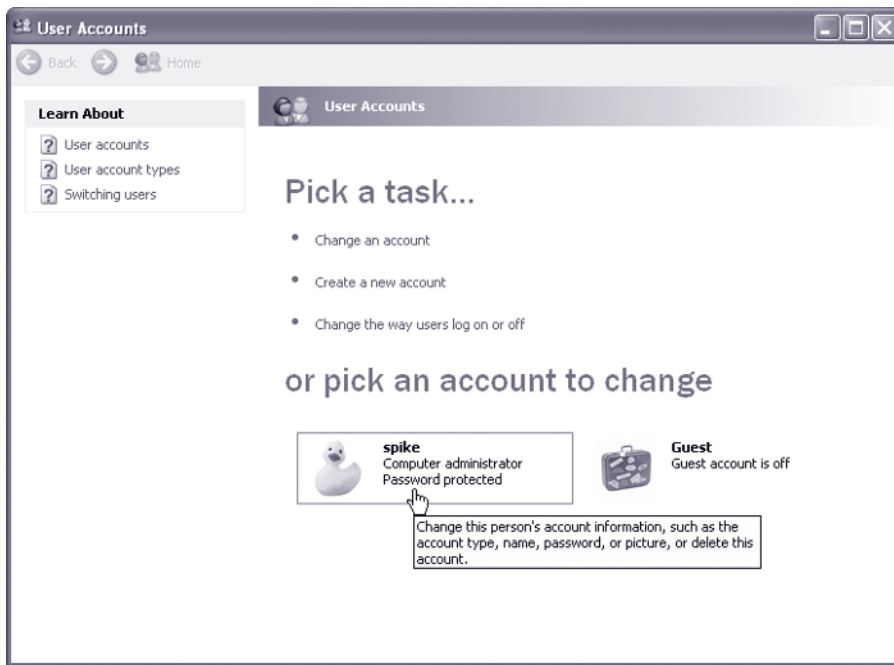


Figure 1.

Usually, you'll see two accounts, one labeled Administrator, and one labeled Guest. Unless you've already changed these settings, Windows XP logs you on as Administrator (in Figure 1, you'll note I've changed my user name to Spike). Click the Administrator icon to access the details of your user account.

First and foremost, you should always create a password for the Administrator account. Not having a password for this account leaves your system wide open to intrusions. Since you're following along and are already in the place where you can do this, click Create A Password on the User Accounts page, and then enter your password (into both fields at the top of the screen) and a password hint into the bottom field (as shown in Figure 2).

The password hint will be readable by anyone who uses the computer, so don't enter your actual password as the hint. Click the Create Password button and you're done.

NOTE

After you reboot the computer, you'll need to enter the password you created here to use your computer. So, at least until you've read the part of this spotlight section about making memorable yet tough passwords, use a password that you won't forget.

Your Windows logon password protects the rest of your system. But don't go to the trouble of creating a password if you're not going to use it. One feature in Tweak UI, a Windows XP Power Toy (<http://find.pcworld.com/44094>) from Microsoft, lets

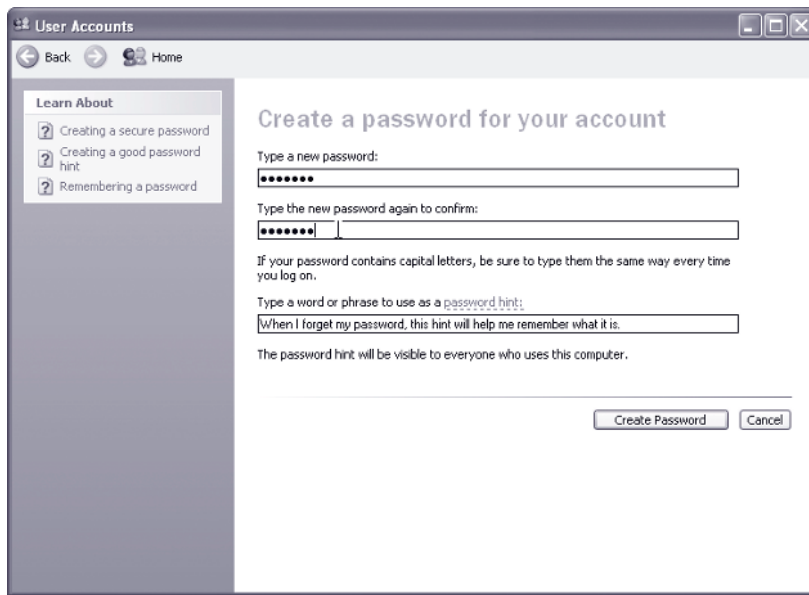


Figure 2.

Windows XP automatically enter your password for you at logon, so when you boot the PC it goes right to the desktop. For the sake of your PC's security, don't use this feature.

Web Password Management in Windows

Once you've created a password for your user account, you can safely use Windows' own password management tools to automatically enter passwords when you log into certain web sites, or when you connect to password-protected networks. Click the Manage My Network Passwords link in the upper-left corner of the User Accounts applet to see the Stored User Names And Passwords dialog box. This is where Windows keeps track of passwords for other computers you might connect to.

Whenever you successfully connect to a password-protected shared folder on another computer, checking the Remember My Password

box will create an entry in this list of stored usernames and passwords. Thereafter, any time you try to connect to the same computer, Windows presents you with a dialog box with the username and password already filled in.

You can also change the password you use for these other computers through this interface. While you've got the Stored User Names And Passwords dialog box open, select one of the shared machines from the list, and click the Properties button. You can enter your new password into the Logon Information Properties dialog box.

Internet Explorer also has some rudimentary password-remembering features. If you fill in the Sign Me In Automatically check box (shown in Figure 3) when you log into Hotmail.com, for example, IE adds the username and password to its list of AutoComplete entries. Afterward, when you



Figure 3.

go to the Hotmail login screen, the username and password are already entered into the fields, so you only have to hit the Sign In button to get to your mail.

What's the problem with this? Well, it means anyone who can sit down at your keyboard can surf over to Hotmail and read your messages (or even send mail "from you") without needing to know your Hotmail username and password.

Fortunately, there's something you can do about this: Don't use IE's password manager feature. Other browsers have similar features, but (with the notable exception of Mozilla Firefox) they're protected with a "master password" of their own, so you still need to enter a password before the browser will auto-fill your username and password into web forms. (We'll talk more about this later.)

If you've already used IE to save your passwords, you can easily clear out the stored information. Open IE, click Tools | Internet Options, select the Content tab, and then click the AutoComplete button on that tab. By default, IE is set up to remember the usernames and passwords, and to prompt you before it stores them (with the little check box). To get rid of this feature altogether, deselect the check box labeled User Names And Passwords In Forms. To dump any passwords it's already got, click the Clear Passwords button (as shown in Figure 4).

Some web sites that offer a similar "remember me for next time" option on their login screens store the username and password in a cookie on your hard drive. Typically, low-security web sites, like message boards or online news services, store passwords in a cookie, if they offer this feature. That means, even if you aren't using Windows' own password storage system, your passwords may be inadvertently stored in the browser's cache and can be used by anyone who can use your computer. To get rid of these

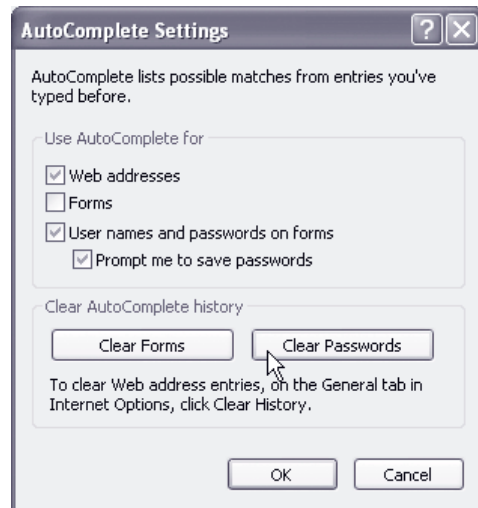


Figure 4.

cookies, try a good cookie remover, like Cookie Crusher (<http://find.pcworld.com/30608>), to blow away all your cookies and start fresh. Once you do that, you'll have to re-enter passwords on web sites where you might have previously checked a "remember me" box.

And when presented with the dialog box that asks if you want the browser to remember you for next time, don't check that little check box. We'll talk about some tools you can use to save your passwords in the next section.

Use Your Browser's Password Manager

Rather than using Windows' or Internet Explorer's password management tools, you can try third-party applications that do the same thing, only they store the passwords more securely. Alternative browsers, for example, can store passwords for web sites in their own password storage mechanism. Password manager software can create, store, and remind you of passwords used for a variety of purposes, including passwords to log into applications, passwords for other computers, or web site logins.

Alternative Browsers Keep Tabs of Web Site Passwords for You

Virtually all of the alternative browsers we mention at the end of Chapter 12 have their own form of password manager built right into the application. These tools record the passwords you use when you log into secure web sites in an encrypted file that makes it hard for snoops to read. Each browser's

tools are slightly different, so just for an example, let's take a look at the password manager in Mozilla (available from www.mozilla.org). Mozilla is the core browser inside of Netscape, so if you use Netscape, you'll find that the menus and commands work for you, too.

The Mozilla Password Manager pops up a dialog box every time you enter your password on a web page (as shown in Figure 5). Clicking Yes to this dialog box adds the username and password to Mozilla's password store, and the browser will auto-fill that information every time you visit the site again. Clicking Never For This Site adds a reference to the Password Manager that excludes this site from any password management features, while clicking No will result in Mozilla asking you the same question the next time you log into the same site.

Mozilla lets you look at which passwords it has stored in its Password Manager through its preferences page (click Edit | Preferences, then expand the Privacy & Security item in the left pane, and select Passwords). Click the Manage Stored Passwords button; any passwords to sites where you clicked Yes in the Password Manager dialog box will appear in the tab labeled Passwords Saved, while the URLs of sites where you clicked Never For This Site will show up in the Passwords Never Saved tab (as shown in Figure 6).

Mozilla has another feature, called the Master Password, that protects the rest of the username/password combinations it has stored. Once you create a master password and save your login information at the web sites you normally visit,

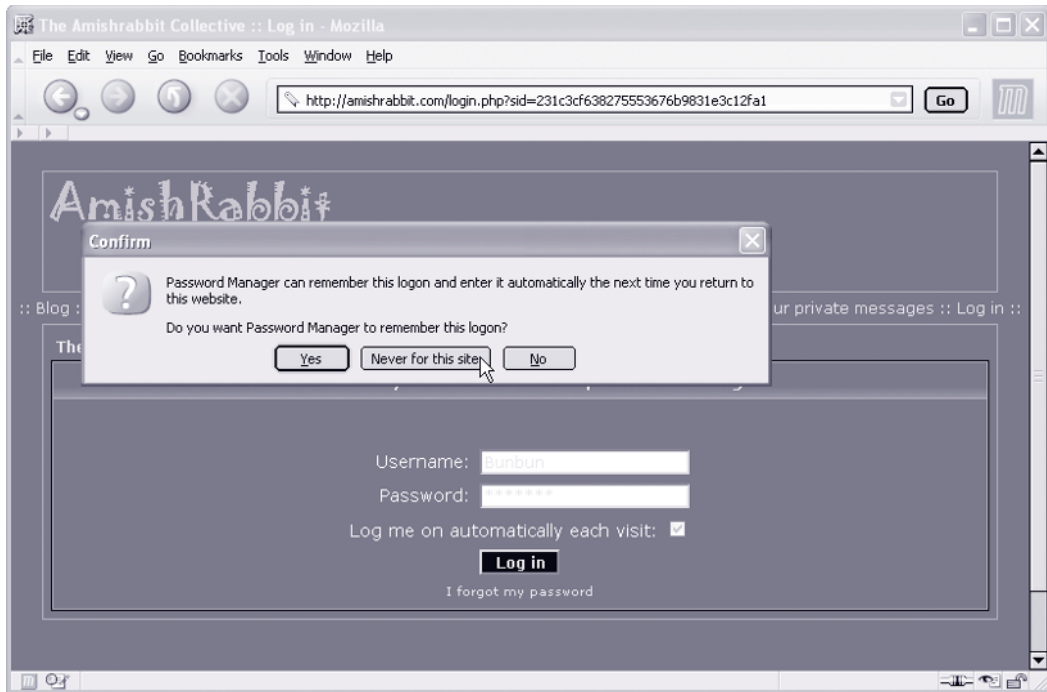


Figure 5.

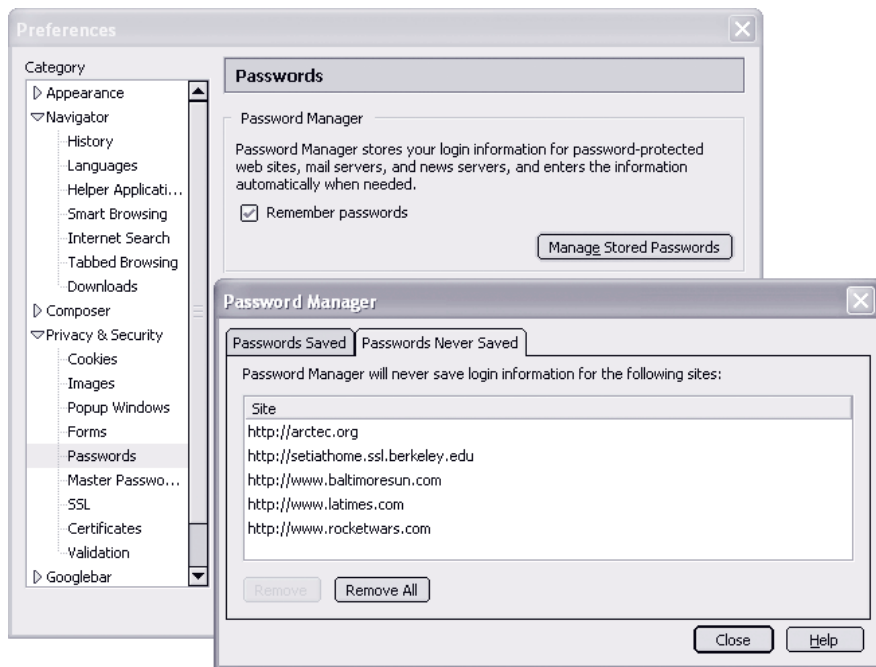


Figure 6.

you'll only have to enter that master password to log into the web sites. Thereafter, when you have to log in somewhere, the browser will automatically fill in the username and password for you.

Using the master password not only simplifies your login experience, but it puts a layer of protection around the list of stored passwords in Mozilla.

Without a master password in place, anyone could skim the saved passwords right out of Mozilla's own list just by clicking Edit | Preferences, expanding the Privacy & Security category, and selecting Passwords. Mozilla stores passwords behind the Manage Stored Passwords button on this settings page, and it's wide open until you create a master password.

Depending on your paranoia level, you could set Mozilla to require you to enter the master password every time you visit a web site that requires a login (really paranoid), or after you don't change the browser page for a set number of minutes (moderately

paranoid), or once per browser session (a normal level that offers the most basic protection, maintaining essential security over the password list).

As you can imagine, it's really important to create a master password if you're going to use the browser's Password Manager. In Mozilla (or Netscape), click Edit | Preferences, then expand the Privacy & Security item in the left pane, and select Master Password below it. Click the Change Password button, then enter your master password twice, and click OK. Mozilla also gives you an idea of the relative strength of your master password in the Password Quality Meter on this page; the longer the dark bar extends to the right (see Figure 7), the more difficult Mozilla surmises it will be for someone to guess or crack the Master Password. You can use it as a gauge to see how tough Mozilla thinks your password is.

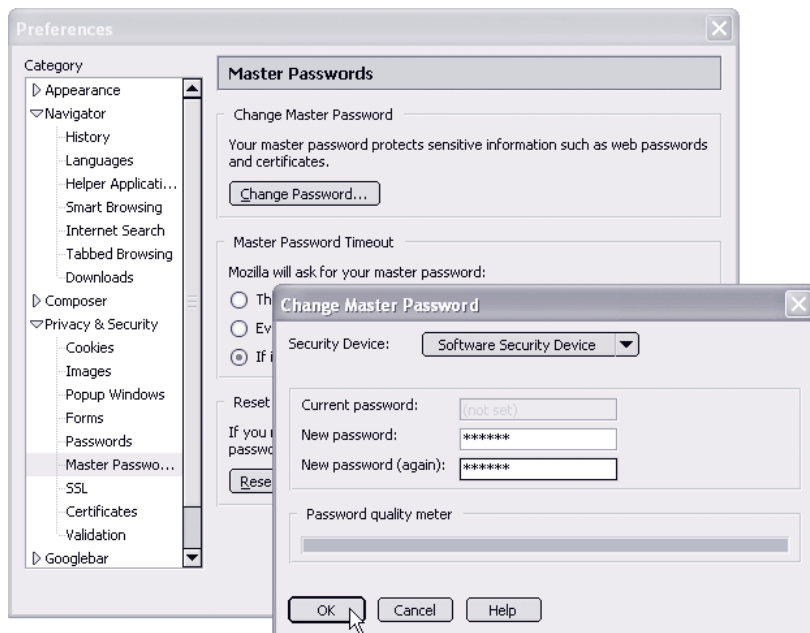


Figure 7.

A few other settings in Mozilla will help keep your Password Manager data secure. Always fill in the check box labeled Use Encryption When Storing Sensitive Data on the Passwords preferences dialog box. That will keep snoops from being able to read your passwords, even if they were to steal the file in which Mozilla stores them.

Password Manager Software Eases the Pain

Using your browser to manage passwords helps you only to keep tabs of the passwords you enter into web pages. But we enter passwords into other applications as well: Your e-mail client program, your file compression utility, Word, Excel, Quicken, Money, and other programs will prompt you for a password when you run the program or open certain documents. Do you want to spend half an hour going through all your different passwords until you find the right one, every single time you run one of these programs, or do you want to use a program that can keep tabs on your passwords, and enter them for you? Yeah, we thought so.

Googling for password manager software will bring you to a huge number of programs that will accomplish the task, but it won't give you any indication about how good the programs are. Most password managers have about the same functions, so as an example of how you would use a password manager, we'll walk you through using a pretty good shareware program called Password Agent, from Moon Software (<http://find.pcworld.com/44264>). Password Agent can store 25 different username/password combinations for free; if you decide that

you like the program and want to use it to store even more passwords, Password Agent costs \$20 to register.

Create a New Password File and Password-Protect It

Before you can start storing passwords, Password Agent makes you create a *password file*, which you then must protect with a master password. Once you've installed Password Agent, click the linked text Create A New File in the program's dialog box. Enter your new password (six or more characters, please) and a password hint, so you don't forget what the password is.

Start Adding Accounts to Your Password File

Once you've created your password store, Password Agent creates an Explorer-like interface that lists all the passwords you've archived (or created) using the tool. At first, the window will be empty, with only one item—Root—listed in the left pane. Password Agent lets you categorize your accounts, so you can keep them better organized; "Root" is just the top level of this categorization tree. If you click Root in the left pane, you'll see all your entries; click a folder under Root if you just want to see that category of your stored passwords.

To add an entry into your password database, click Entry | New Account in the Password Agent window. The Title field is just a name you can give the account, but the User ID field is where you enter the actual username that needs to be entered in the login window. The Password field will already be filled in with a randomized password, though you can select this password and delete it, and then enter your existing password, if you already have one.

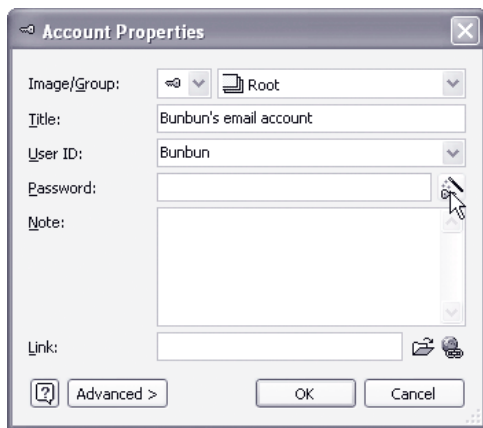


Figure 8.

The randomized password is one of Password Agent's coolest features, if you know how to use it. If you click the icon that looks like a magic wand-tapping a key (located to the right of the Password field in the New Account dialog, as shown in Figure 8), you can customize virtually every aspect of how the program generates the password.

The password generator can create massively complex, as-long-as-40-character passwords made with any combination of the typical *password factors*—upper- and lowercase letters, numbers, and/or special characters (punctuation marks). It lets you use a few of the options (just numbers, or just lowercase letters, for instance), or you can create a pattern out of the factors you prefer. Use the password generator only when a password calls for specific restrictions on the size or factors used (a six-digit numeric PIN for your ATM card, for example).

Change Your Passwords Regularly

Even though programs like Password Agent can generate strong passwords and enter them into

programs or web forms automatically, they cannot prevent others from trying to break your passwords. If someone were to guess or crack a password you used, they might be able to log into your accounts or web sites for months before you discovered they were doing so. The only solution to this problem is to change your passwords periodically. Fortunately, Password Agent makes it easy to keep track of when you need to make changes like this.

Open the account information for any account, and click the Advanced button. To the right of the field labeled Expires, click the small, square icon; you can choose to make the program “expire” the password in 15 days; one, three, or six months; or a year from the current date. When the expiration date appears, you'll be prompted to log into the password-protected site, application, or document and change the password.

Make Up Strong Passwords on Your Own

With so much of your personal data stored on a hard drive or on the Internet, the best way to maintain your privacy is to create tough passwords and change them regularly. You could use a password manager application to create your passwords for you, but they won't be as memorable as if you come up with them yourself. Here are a few cool techniques you can use to come up with passwords (using paper and pencil) that no one else will guess but you'll be able to recall easily:

- *Turn any memorable string of words into a memorable password.* Make the password out of the first (or last) letter of each word in a phrase, or a list of words. The list you use can be a favorite quotation, or perhaps the names of your children, brothers, or favorite football teams. Robert A. Heinlein did just that in his 1966 novel *The Moon Is a Harsh Mistress*, where he made up the secret word “tanstaaf!” from the first letter of each word in the sentence, “There ain’t no such thing as a free lunch.” If you used the first sentence in this paragraph the same way, your password would be “Tamsowiamp!”—a pretty tough password to guess.
- *Turn words into numbers and special characters.* Adding anything from the number row of your keyboard (either the numbers or the shifted special characters) to a password makes it much stronger. For instance, you could turn a memorable pet emergency (“My three dogs chased a cat up a tree”) into the password m3dcac^at (where you use the caret symbol to mean the word “up”).
- *Blend the letters of two or more words into one password.* Rather than using your mother’s name as a password, you could combine the words mom and Faye into the password Fmaoyme, by alternating letters from the two words. Need a new password? Just reverse the letters to make emyoamF. Change the letter o into a zero, and you get a tougher-to-crack version of the same password.

Even if you have a good memory, it’s wise to store the passwords you come up with in a password manager application, just in case.

Hardware Devices Can Be Password Helpers

Software isn’t the only way to manage passwords: Biometric devices, which measure some physical characteristic of your body, can help you better manage passwords by using a fingerprint, a photo the computer takes of your face or eye, or your voice as a password replacement. While biometric technology is making waves in Homeland Security circles, few people realize you can buy biometric readers to use at home, too.

Learn More about Biometrics

In its August 2004 issue, *PC World* reviewed some of the biometric devices you can buy today to secure your computer, in a story titled “Products for the Paranoid” (<http://find.pcworld.com/44096>).

NOTE

Andrew Brandt is an editor at *PC World*, and worked on the story linked here; *PC World* and McGraw-Hill/Osborne, the publisher of this book, have no other business relationship.

Fingerprint readers can cost anywhere from \$50 to \$200, depending on the technical sophistication of the device and how portable it is. Some third-party keyboards and mice have fingerprint readers built right into the product, and even a few laptops are starting to get on board with the trend.

In general, it’s important to remember that biometrics aren’t really a replacement for passwords,

and the biometric products sold to the general public can't make a weak or easily guessable password any more secure. What they do is provide a very convenient way to enter passwords when you're prompted to do so. Rather than having to remember long and complex passwords, when you have a biometric device plugged into your computer, you can simply enter the password once, and tell the biometric software to keep track of it. Thereafter, when you want to log into something, the program asks you to put a finger down on the sensor.

Biometrics, simply put, make it easier to enter passwords when prompted to do so. They don't, however, fix the inherent problems with passwords—that they can be guessed, or stolen, or cracked through brute force. Keep that in mind when considering buying a biometric device.

Using Other Password Keepers

While it can be handy to keep tabs of passwords on a PC or laptop, sometimes it can be inconvenient to do so. For example, if you're traveling and normally keep your passwords in a password manager application on your desktop computer, you might forget to bring that data on a business trip. When it comes time to log into the VPN at work, you might be up a creek without a paddle.

Fortunately, several kinds of devices can keep tabs of your important passwords. You could use your cell phone or PDA, but computer scientists have found serious weaknesses in the security of those devices, and if you lose the handheld or phone, anyone who finds it could easily get access to that sensitive data. Instead, take a look at the gear you



Figure 9.

can find in Thinkgeek.com's Security Gadgets section (www.thinkgeek.com/gadgets/security) to get an idea of what you can use.

For folks who are serious about security and who need a portable, secure device to transport passwords, Mandyllion Labs created the ebp Lite (\$70, www.mandyllionlabs.com), a device the size of a car alarm remote (shown in Figure 9) that can store 20 username/password combinations, can generate random passwords, and is difficult to crack.

If you're looking for something that doesn't require a lot of effort, the USB Wireless Security Lock (\$50, <http://find.pcworld.com/44266>) won't keep tabs of your passwords, but it will lock your computer as soon as you step away from it. A small radio transmitter (shown in Figure 10) hangs on your keychain or slips in your pocket. When you're near the receiver, it detects the transmitter's radio signal and unlocks the PC.



Figure 10.

Megamet's VME USB BioDrive XP (\$80 and up, depending on storage capacity, <http://find.pcworld.com/44268>) is a USB thumbdrive-type storage device with a biometric reader built right in (see Figure 11). Using a fingerprint, the owner of the device can manage passwords, encrypt files stored on the device or the text of e-mail messages, and lock anyone else out of a PC.



Figure 11.

What's the Future of Passwords?

The password, as it exists today, is a dinosaur—a throwback to a time before automated worms existed that could log every keystroke computer users make, and before phishing messages emerged that trick people into sending their passwords to a con artist. But though one password is insufficient, a lot of companies are starting to believe that two passwords may be just the ticket.

Businesses call the arrangement “two-factor authentication,” but it boils down to having one password that you make up for yourself and another password that you get from someplace else. This is the computer equivalent of the security provided by a safety deposit box: your key alone can't open the box, and neither can the bank's key; both parties need to use both keys at the same time.

Here's how one method might work: Your bank includes, with your monthly statement, a card with 50 passwords printed on it. Each password hides behind the same silvery stuff that obscures the numbers on a scratch-off lottery ticket. When you want to log in to your bank account online, you scratch off the silvery stripe covering one password and then log in to the web site with your user name, the password you created, and the password on the scratcher card. After you've used the scratched-off password, you can never use it again.

The security benefits here are clear. Even if someone guesses the password you made up for your bank account, they still can't get in unless they hold your card of passwords. If someone finds your password card, they can't get in unless they can also guess the password you invented. Some banks in Europe already use this method; no U.S. bank uses it yet for consumer accounts.

Businesses have relied on RSA Security's SecurID devices for years. The SecurID Key Fob, about the size of a car-alarm remote, displays a new six-digit code every 60 seconds. Anytime you want to log into an RSA SecurID-protected computer or site, you must enter your user name, your password, and the RSA SecurID code displayed on the device at the moment you log in.

Using two passwords solves a great many security problems. It won't matter whether a keystroke logger records what you type, because one of your passwords will expire the moment the hacker gets it. You won't have to invent elaborate—and easily forgotten—passwords, and your finances and other personal information will remain safe.

New Developments in Wireless Networking

Wireless Ethernet technology has sparked a flurry of new product development that uses the flexible communications infrastructure created by this standard to move audio, video, and data in new ways. In this spotlight on technology section, we will present three devices that make use of this standard to enhance your ability to make media a part of your life.

From the car to the office to the entertainment center, 802.11 wireless Ethernet can link your computer and media in ways that were impossible just a few years ago, transmitting files to the car from the PC, transmitting video from a security camera to your workplace, and transmitting your media to stereo and television systems throughout the home.

While this is only a preview of the technologies to come in the next few years, it serves as an exciting example of the power of this medium to make media-sharing and communication easier.

Wireless Omnifi DMP2 Plays Digital Audio and Video in Your Car

Browse the aisles of any high-end audio/video superstore or boutique and you will find dozens of devices designed to play MP3 and WMA audio. Some have adapters to inject audio into your car's stereo system but lack the sound quality demanded by car audio purists. In-dash car audio equipment will play your digital media as well, but the common issue facing those with hundreds of digital tunes is how to get them into the unit. Most in-dash models play your MP3s off CD media, but that sort of puts the CD back in the picture; doesn't it?

Rockford Corporation's Omnifi division has the answer. The DMP2 digital media player has 60 Gigabytes of storage capacity for digital audio and video files (see Figure 12). These files are decoded by the DMP2 and played over your vehicle's existing audio/video systems. Files are transmitted wirelessly over your 802.11g wireless home network from your computer directly to the DMP2 in your car.

With space for thousands of songs and hours of video, this device opens a new level of convenience to digital music enthusiasts. Installable by any car-fi shop, it uses an application loaded onto your home computer to browse and download selections to the unit. No longer do you have to transfer your music or video files with cables or discs. Downloads can even be scheduled during nighttime hours to load in the



Figure 12.

morning's news for your commute. Visit Omnifi's web site, www.omnifi.com, for more information.

Security Cameras Without Wires

One of the drawbacks of closed-circuit security cameras is the necessity of stringing all that coaxial cable. It is often difficult to get cable to some of the best locations for good coverage. Wireless security cameras are doing a great job in this area, but most have proprietary wireless technologies.

With the recent proliferation of 802.11 wireless Ethernet, many manufacturers are working to add this feature to their offerings. One of the most versatile of these is the Linksys WVC11B Wireless-B Internet Video Camera (see Figure 13).

This camera can transmit high-frame rate MPEG-4 video using 802.11b wireless Ethernet. It includes its own built-in web server and can be programmed to send you an e-mail video clip when it detects motion. Imagine seeing who has been walking their dog in your backyard while you



Figure 13.

are away at work. If you are quick with the phone, maybe you can even get the sprinklers turned on in time!

For more information, check out Linksys' web site at www.linksys.com.

Getting Media Files Out of the Office

Digital media files are a great way to entertain yourself while working on budgets in the home office, but sometimes you'd like to listen while you are relaxing in the family room, or watch a downloaded video on your big-screen TV. You can do that without wires or expensive equipment to translate your computer graphics to a television image by using one of the new wireless media players.

D-Link Systems manufactures the DSM-320 MediaLounge Wireless Media Player for this purpose. It can browse and play digital audio and video files directly from your computer on your

home stereo or television system. It supports MP3, WMA, and WAV audio formats; MPEG-1, -2, and -4, AVI, and QuickTime video formats; and most common graphic file formats. It will also play streaming media broadcasts from RadioAOL.

It includes a remote control, uses menus displayed on your television, and looks right at home in the entertainment center (see Figure 14).

MEDIA CENTER PCS

Media Center PCs, designed for use with Microsoft's Windows XP Media Center Edition, can form the digital media hub for a home. Products like those in this section can work with Windows XP MCE to enhance and extend this capability.

The DSM-320 supports the Intel Universal Plug and Play audio/video specification, a specification designed to allow home media devices to find and communicate with each other, so it will interface automatically with other devices supporting this spec.

More information on this and other media devices is available at D-Link's web site at www.dlink.com.

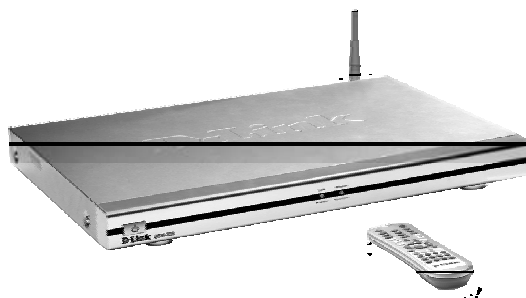


Figure 14.