INTERHACK

Interhack
5 E Long St Ste 1101
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Anatomy of Online Fraud: How Thieves Targeted eBay Users but Got Stopped Instead

Matt Curtin

June 20, 2003

Id: fraud-anatomy.tex,v 1.3 2003/06/20 19:06:39 cmcurtin Exp

Abstract

At 10 p.m. on Saturday, June 14, 2003, I received a call from a client. His wife had just received email that claimed to be from eBay, asking her to enter her credit card number. By 11 p.m., I had reports to the Internet service providers whose systems had been used to originate the message and to impersonate the eBay web site, as well as to FBI in Washington, D.C.

Here we discuss the fraud in detail, showing how it was constructed, how it was stopped, and what consumers can do to protect themselves against these kinds of attacks.

1 Introduction

Criminals have long preyed upon the expectations of users who can be fooled into doing things they shouldn't. The fact that this can now be done online—where fooling someone around the world is just as easy as fooling someone across town—should come as a surprise to no one.

Here we consider a recent scheme directed at eBay users, in an effort to collect their usernames, passwords, and credit card numbers.

The scheme involved sending email to eBay users, telling them that there was a problem with their credit card, and asking them to visit the eBay site, helpfully providing a link. While appearing to be from eBay, the email was actually from a cable modem user in Canada. Following the link in the email would not take the user to the actual eBay site, but an imposter.

2 Architecture of the Scheme

Two critical pieces of information were targeted in this scheme: the authentication credentials (i.e., username and password) and the user's credit card information. Figure 1 shows the critical steps of the scheme from beginning to end.

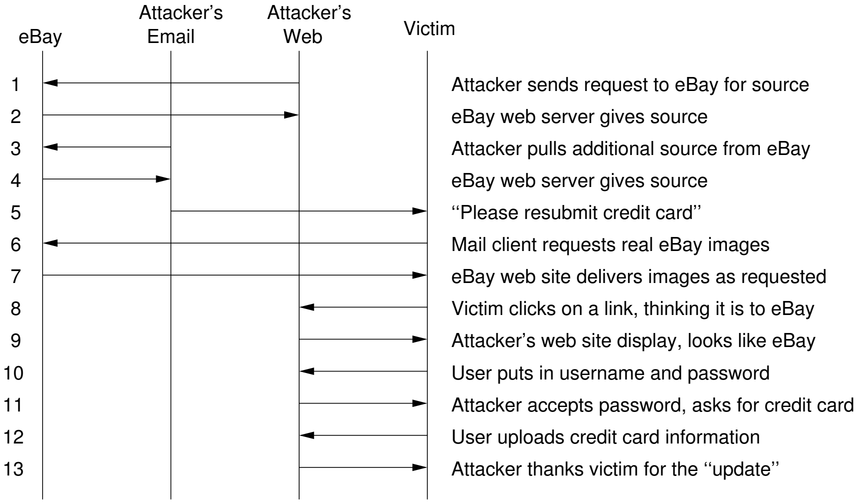
eBay
Attacker's Email
Attacker's Web
Victim
1
2
3
4
5
6
7
8
9
10
11
12
13
Attacker sends request to eBay for source
eBay web server gives source
Attacker pulls additional source from eBay
eBay web server gives source
"Please resubmit credit card"
Mail client requests real eBay images
eBay web site delivers images as requested
Victim clicks on a link, thinking it is to eBay
Attacker's web site display, looks like eBay
User puts in username and password
Attacker accepts password, asks for credit card
User uploads credit card information
Attacker thanks victim for the "update"

Figure 1: Interaction Diagram Showing Scheme

Each of the thirteen steps identified here supports one of three goals needed for the thief to achieve his objective. Those goals are creation of the fraudulent eBay site, directing users to the fraudulent site, and then operating the fraudulent site such that users never suspect what has happened.

2.1 Creating Fraudulent eBay Site

Creation of the fraudulent site is obviously necessary for this scheme so that users will be inclined to enter sensitive authentication and financial information.

Step 1. To build the fraudulent web site, the attacker simply sends requests to eBay for the HTML markup and images needed to render critical pages of the eBay site. Because the Web works by having clients (such as *Mozilla* or *Internet Explorer*) download HTML from the server and then display the results to the user, there is no way for eBay to stop users from downloading its source. In fact, easy replicability of content from one Web site to another is a critical *feature* of the Web.

Instructing the eBay site to send a copy of the source is as simple as having the attacker point his browser to `http://www.ebay.com/`.

Step 2. The eBay site responds to the request from the client, sending down the HTML source for the requested page. Capturing this information, instead of using it strictly for display on the attacker's monitor is as simple as using the "Save As" menu option in the browser.

The attacker now has the source code needed to replicate the "look and feel" of the eBay site on any server of his choosing. With some minor modifications to the code, the results of forms can be sent to new programs that reside on the attacker's computer, instead of the legitimate form processing software on the real eBay web site.

Step 3. Additional data might be needed to fetch things like images from the eBay web site, or to see what email from eBay actually looks like.

Step 4. eBay will naturally respond to the attacker's requests—which all by themselves are quite legitimate. It's important to understand that from eBay's perspective, no fraudulent activity has (yet) taken place.

Unbeknownst to eBay, however, the attacker has not been simply displaying the data he has downloaded. He has created a new site of his own, using the HTML and images from eBay, with modifications to ensure that the data submitted by the user will be collected by the attacker's site instead of submitted to the legitimate eBay web site.

Once the site is finished, it is put online, where it will await users who submit their information to it.

2.2 Directing Users to the Fraudulent Site

Step 5. eBay users now need to be convinced to connect to the fraudulent web site. The means for doing that is by sending an email message, crafted using eBay's look and feel, even including an image of the eBay logo. The text of the message is reproduced precisely in Figure 2.

With the exception of the truncated copyright notice, there seems to be very little indication of anything being amiss. Indeed, to non-experts, the reason given for having deleted the credit card information might even sound plausible.

Step 6. Mail client requests real eBay images. As the user's email client renders the fraudulent message, it will obey the HTML directive to fetch the eBay logo image from the legitimate eBay web site. A careful user might even be inclined to note the source of the eBay logo, which would tend to support the conclusion that the message itself is legitimate.

Step 7. eBay returns real images to client for display in the fraudulent email. Thus, the HTML is stolen from eBay and modified, sent by an attacker, the images come directly from eBay, and the link will connect the user not to the real eBay, but to the fraudulent Web site.

> Recently we attempted to authorize payment from your credit card we have on file for you, but it was declined.
>
> For security purposes, our system automatically removes credit card information from an account when there is a problem or the card expires.
>
> Please resubmit the credit card, and provide us with new and complete information. To resubmit credit card information via our secure server, click the following link:
>
> http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?SignIn
>
> This is the quickest and easiest method of getting credit card information to us. Using the secure server will ensure that the credit card will be placed on account within 24 hours.
>
> Copyright 1995-2003 Ebay Inc.
>
> All Rights Reserved. Designated trademarks and brands are the
> property of their respective

Figure 2: Text of Message Bringing Users to Fraudulent Site

2.3 Fraudulent Site Operation

Step 8. Victim clicks on the link, requesting source from attacker's Web server. Interestingly, the link that is displayed to the user[1] is not the actual URI of the link.

Careful examination of the email's HTML source will show the actual link. Figure 3 shows the HTML source of the paragraph and the link itself.

```
<p>Please resubmit the credit card, and provide us with new
and complete information. To resubmit credit card information
via our secure server, click the following link:</p>

<p> <a href="http://cgi3.ebay.com:aw-cgieBayISAPI.dll
SignInRegisterEnterInfo&amp;siteid=0co\_partnerid=2@
www.john33.netfirms.com/">
http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?SignIn</a>
  </p>
```

Figure 3: HTML Source of Fraudulent Email Message

The URI is very carefully constructed to appear to be legitimate but to redirect to the fraudulent Web site. Here we break the URI into its parts.

http:// This is the protocol identifier, and the separator characters showing an

[1] `http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?SignIn`

external link. The protocol in this case is HTTP, unencrypted. (A typical unsecured web link.)

cgi3.ebay.com: This is an optional section of a URI, reserved for the name of the user logging in, and the separator token (:) used to differentiate it from the next section.

aw-cgieBayISAPI.dllSignInRegisterEnterInfo&amp;siteid=0co_partnerid=2@ This tricky section is obviously constructed to appear to be linking deep down into the eBay web site, but in reality is being put into the optional password field of the URI. The giveaway is the @ character at the end, which means that what proceeded it is user and/or password data.

www.john33.netfirms.com/ The real site name to which the client will connect.

Step 9. Attacker's Web server answers the client's request, sending back the fraudulent HTML for the user's browser to display.

At this point, the user believes that he is following a legitimate link to the eBay web site. What the user sees instead is the illegitimate copy of the eBay web site created in steps one through four.

Step 10. Thinking he is seeing the real eBay web site, the user enters his username and password, sending them to the thieves running the fraudulent site.

Step 11. Fraudulent web site saves the username and password (thus allowing the attacker to login to the user's account on the real eBay site), and displays a page that asks the user to enter his credit card information again.

Note that no matter what the user enters, the fraudulent site will behave as if the username and password were entered correctly. This reinforces the idea to the user that the site is the correct one: when the user enters the right authentication credentials, the site accepts them, and only the user and eBay's server should know what those credentials are.

Step 12. User enters his credit card information and hits submit, sending the credit card information not to eBay, but the fraudulent site.

Note that because the site is not using cryptographic methods for authentication or session confidentiality, the credit card is also exposed to eavesdroppers.

Step 13. Fraudulent site sends back a "thank you" page, promising to update the eBay account within twenty-four hours.

At the end of the session, the user believes that he has updated his eBay account, and the attacker has collected the username, password, and credit card information of eBay users who fell for the scam.

3 Reporting the Fraud

Two collaborators (or one person doing two things) worked to launch the scheme: the sender of the fraudulent email and the operator of the fraudulent web site.

3.1 Finding the Web Site

First, we wanted to identify the fraudulent web site, since it was still active and capable of collecting sensitive information. As was identified above (in step 8), the web site to which clients were directed was `www.john33.netfirms.com`. Theoretically, WHOIS records should help us to contact the right folks. However, since registration of domain names is open to anyone, the perpetrators of fraud frequently submit fraudulent contact information to these records. [3] Additionally, some otherwise legitimate domains populate the WHOIS records with bogus data to avoid being targeted by spammers.

NetFirms is a fairly well-known hosting service, so the likelihood that their WHOIS records were incorrect wasn't especially high.

Since registration of Internet numbers is much more tightly controlled, WHOIS records for network numbers are much better maintained and less likely to contain bogus information. So even though checking the WHOIS record for NetFirms would probably get us the information we needed in this case, we opted to match the IP address to the network contact, as it is more general, and will work even if the fraudulent web site were hiding on a network whose administrators were harder to contact.

Using command-line utilities like *host* or *nslookup*[2] would reveal the IP address as [209.171.43.26].

Using the command-line utility *whois*[3], we were able to identify TELUS Communications as the network administrator. A phone call placed to TELUS got us connected to some helpful folks there who gave us the telephone number for their security and abuse contact.

A gentleman who answered the phone asked us to email details, along with a forwarded copy of the message showing the link to the fraudulent site to the abuse contact, and to send him a copy as well. He then promised to call over to the security group to be sure that someone would look at it quickly.

3.2 Tracking the Email

Our next step was to identify the source of the email. By reading the mail headers [1, 2] (shown in Figure 4), we can see that the source is u201n212.hfx.eastlink.ca [24.222.201.212]. A telephone call to Eastlink (in Halifax, Nova Scotia) alerts Eastlink to the problem. The helpful folks there ask for a copy of the message to be sent to their abuse contact.

[2] A Google search for "nslookup gateway" will locate many Web interfaces for this utility.

[3] The American Registry of Internet Numbers (ARIN) has a Web-based interface to WHOIS at `http://www.arin.net/tools/whois_help.html`.

Had this message originated from overseas, finding a reasonable point of contact might have been more difficult. In this particular case, it appears to be a high-speed cable modem Internet connection sent into someone's home.

Technically, the telephone call was unnecessary, but I placed it because I wanted to alert them to what was probably an ongoing incident of international wire fraud, and probably a lot of other things. It's a much bigger mess than, say, sending spam, and I wanted to be sure that it didn't sit in a queue for hours or days before someone was aware of the situation. That might be the kind of thing to which an administrator would want (after verification) to respond immediately.

```
Return-path: <support@ebay.com>
Received: from ms-mta-02.socal.rr.com ([10.10.4.126]) by
 ms-mss-03.socal.rr.com (iPlanet Messaging Server 5.2 HotFix 1.12
 (built Feb 13 2003)) with ESMTP id
 <0HGH006M6R8EL2@ms-mss-03.socal.rr.com>; Sat, 14 Jun 2003 14:48:14
 -0700 (PDT)
Received: from lamx02.mgw.rr.com (lamx02.mgw.rr.com [66.75.160.13])
 by ms-mta-02.socal.rr.com (iPlanet Messaging Server 5.2 HotFix 1.12
 (built Feb 13 2003)) with ESMTP id
 <0HGH00540QDXB0@ms-mta-02.socal.rr.com>; Sat, 14 Jun 2003 14:29:58
 -0700 (PDT)
Received: from ebay.com (u201n212.hfx.eastlink.ca [24.222.201.212])
 by lamx02.mgw.rr.com (8.12.8p1/8.12.8) with SMTP id h5ELm8Vb002000;
 Sat, 14 Jun 2003 17:48:09 -0400 (EDT)
Date: Sat, 14 Jun 2003 14:25:40 +1000
From: support@ebay.com
Subject: Billing Update Requested (URGENT)
To: mail@lamx02.mgw.rr.com
Message-id: <001400e8db46$dae47575$14814366@qijuhor.pgh>
MIME-version: 1.0
X-Mailer: QUALCOMM Windows Eudora Version 5.1
Content-type: multipart/mixed;
 boundary="----=_NextPart_000_00A0_62D10B0B.E5271C86"
Importance: Normal
X-Priority: 1
X-Virus-Scanned: Symantec AntiVirus Scan Engine
```

Figure 4: Headers of Fraudulent Email

3.3 Reporting to FBI

Since this was potentially very large fraud involving many victims, crossing state and national boundaries, this is no doubt of interest to law enforcement officials. As I am a member of InfraGard, I decided to report the matter through InfraGard.[4]

[4] Details on the procedure for getting information reported to InfraGard are available online at http://www.infragard.net/ireporting.htm.

3.4 Reporting to eBay

Finally, since eBay impersonated, it would likely want to be made aware of the incident in an effort to keep its users' accounts safe, perhaps locking out any that might appear to be involved in fraudulent activity.

It is noteworthy that the user who originally got the fraudulent email tried to find a way to report the incident to eBay, but was unable to find anyplace to report this kind of activity. Ultimately, we reported to `fraud@ebay.com`, and watched to see whether a bounce came in. One never did, but as of this writing—five days after the incident—we have yet to receive as much as an acknowledgment from eBay.

4 Self-Defense

There are some lessons here for end-users of systems that can help them to avoid falling victim to online fraud.

1. Don't be rushed.

   Fraud often depends upon someone making a quick decision, before having time to consider possible ramifications. Consider the original text of the fraudulent email: "This is the quickest way of getting information to us."

   If, as had been stated in the email, the account data had been deleted, the critical data would be safe, and the worst case scenario would be that the user would not get something for which he won a bid.

2. Follow established procedure

   If it seems strange to be asked for some kind of information in a strange sequence of events, or at a strange time, beware. If you made a credit card purchase, it would be either accepted or rejected quite soon—usually immediately.

   If the vendor has a mechanism for entering sensitive information, follow it. Beware of the dangers that could come from the appearance of deep linking.

3. Question things you don't understand

   If it doesn't make sense for a vendor to ask for your credit card number, don't be afraid to question it. If the explanation sounds fishy, don't be afraid to question it. Remember that when you're doing the buying, you're the boss.

4. Verify that you're talking to the site you think you are

   When you're connecting to a site that involves any kind of financial transaction, the connection should be "secured." In the browser, a small padlock will appear, and it will be locked. That tells you that the connection is encrypted, but it does not verify with whom you are speaking.

   Clicking on the lock will open a new dialog and present you with the option of viewing the certificate in use. Look at it and be sure that the URI is exactly what you think it is.

In this particular case, the fraudulent site made no serious attempt to impersonate a secured eBay server, so the lock never closed.

5 Conclusion

As the Internet becomes more of a normal part of every day life and commerce, it will become more frequently used as the means by which thieves attempt to perpetrate their deeds. Users need to be aware of the dangers, understanding the limits on how well they can be protected by others, and the need to defend themselves.

There is good news in this regard, however. The simple fact that I was able to pick up a telephone and talk to someone at a Federal law enforcement agency is a tremendous step forward from where we were even five years ago.

Companies that do business online, particularly with consumers, need to understand that they will be frequent targets for this kind of activity. (In the week following this incident, I was advised of two separate incidents of almost identical nature, targeted at Best Buy customers.) Such companies need to be sure that they are encouraging good security practice, such that an attacker cannot send something that is usual to receive that fools the user into doing something bad.

Successful security will require that we work together thoughtfully to identify and to stop fraud and other electronic crimes. It won't be quick and it won't be easy, but it can be done, reasonably and effectively.□

Matt Curtin, CISSP is the founder of Interhack Corporation, a professional services firm with information assurance, forensic computing, and information systems practices. His work includes published research in secure systems development, dozens of technical reports, and several books on online privacy and computer security. His information security work is cited by University courses worldwide and NIST. He has given expert testimony given in civil litigation dealing with Internet privacy and computer systems, work which recently led to clearer definition of "protected content" under the Electronic Communications Privacy Act of 1986 (ECPA) by the U.S. Court of Appeals for the First Circuit.

References

[1] Ken Lucke. Reading Email Headers. Web article, 1997. [online] http://www.stopspam.org/email/headers/headers.html.

[2] Doug Muth. The SPAM-L FAQ. Frequently Asked Questions Article, April 2002. [online] http://www.claws-and-paws.com/spam-l/.

[3] Jim Wagner. WHOIS Inaccuracies Hampering FTC. internetnews.com, May 2002. [online] http://www.internetnews.com/bus-news/article.php/1143131.