Anatomy of a Phishing Email

Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz

MailFrontier, Inc., 1841 Page Mill Road, Palo Alto, CA 94304, USA

Summary

This paper discusses the tricks employed by email scammers in "phishing" emails, which are emails that spoof a reputable company in an attempt to defraud the recipient of personal information. These tricks are classified according to whether they are employed in the fraudulent emails or used in the fraudulent Web pages accessed by a link provided in the email. All of the examples used within the paper were taken from fraudulent emails forwarded to MailFrontier, Inc., from its customers.

1 Introduction

Fraudulent emails are on the rise as scammers "spam" recipients with email frauds that range from the very simple to the very sophisticated, which can fool even the savvy Internet user. Fraudulent emails harm their victims through loss of funds and identity theft. They also hurt Internet business, because people lose their trust in Internet transactions for fear that they will become victims of fraud. [8], [10] and [16] For example, many people believe using on-line banking increases the likelihood that they will become victims of identity theft, even though on-line banking provides more secure identity protection than paper and mail based systems. [16]

"Phishing" is an email scam that attempts to defraud people of their personal information including credit card number, bank account information, social security number, and their mother's maiden name. The term phishing was coined because the fraudsters are "fishing" for personal information. The Anti-Phishing Working Group received 1197 unique phishing email messages in May 2004, averaging 38.6 a day. [3] From November 2003 to April 2004, phishing emails increased an average of 110% each month. [2] Approximately 57 million U.S. adults believe they have received a phishing email message. [10] Phishing emails are also growing in languages such as Spanish, French, German, and Dutch. [17] For May 2004, MailFrontier's Phishing Index shows that 1 out of 10 people who evaluated a phishing email, which had been labeled as suspicious by MailFrontier, were still fooled into acting upon the email. Mi2g, a company that sells products for electronic banking, estimates economic damage in 2003 from phishing scams to be between $32.2 billion and $39.4 billion. [9]

This paper explores numerous tricks used in phishing emails. Generally, fraudulent Web sites are quickly discovered and shut down. Within this limited time, scammers attempt to gain the trust of the recipients and convince them to act. Phishing email messages employ a variety of deceptive devices to appear as though they originated from a legitimate company and to conceal its actual origin. This paper explores tricks in fraudulent email messages and tricks used on fraudulent Web sites.

2 Tricks Used in Fraudulent Emails

This section discusses tricks used in phishing emails. Section 3, starting on page 5, describes deceptive devices used in the fraudulent Web sites, which are accessed through links in the original email.

2.1 "Spoofing" Reputable Companies

In phishing email messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters "spoof," or mimic, a reputable company. The companies

spoofed most often are Citibank, eBay, and PayPal. The most targeted industry is financial services. Internet retailers and Internet service providers are also targeted. [2] and [10]

These phishing emails are mass mailed: an estimated 3.1 billion phishing email messages were sent worldwide in April 2004. [18] Many of the recipients are not customers of the spoofed companies and may quickly realize that the email is fraudulent, or may believe that the email was mistakenly sent to them and ignore the email. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. Fraudsters use the following tricks to mimic a reputable company:

Using a Company's Image
When spoofing a company, scammers not only claim to be from a reputable company, but they also go to great lengths to emulate the company's visible branding. The fraudulent emails often contain the company's logo and use similar fonts and color schemes as those used on the company's Web site. Many fraudulent emails simply reference images from the legitimate company's site.

Links to the Real Company Site
The main link in a fraudulent email sends the recipient to the fraudulent phishing Web site, but many fraudulent emails include other links that send the recipient to sections of the real company's Web site.

Email Appears to Be From the Spoofed Company
To further convince the recipient that the email originated from the reputable company, the scammers use a "from" email address that appears to be from the company by using the company's domain name (e.g., @ebay.com, @paypal.com).

2.2 Reply Address Differs From the Claimed Sender

In some fraudulent emails, the email claims to be from a credible company, but is set to reply to a fraudulent reply address. The following are some examples from fraudulent emails:

From:	EarthLink Security Dept.	From:	Citibank
Reply-To:	earthlink8770@1-base.com	Reply-To:	citibank3741@collegeclub.com

2.3 Creating a Plausible Premise

After convincing the recipient that the email originated from a credible company, the email must contain a plausible premise that persuades the recipient to divulge personal information. The emails may claim that the recipient's account information is outdated, a credit card has expired, or the account has been randomly selected for verification. Ironically, the email messages often use people's fear of fraud to defraud them: the emails may claim that the company has installed new security software and the recipient must renew the account information, or the email might claim that the account has been compromised by some sort of fraudulent activity and the account must be confirmed. There are numerous approaches, and each tries to create a scenario that would convince the recipients that they must provide the requested information.

2.4 Requires a Quick Response

In the short time that fraudsters have to collect information before their sites are shut down, they must convince the recipients to respond quickly. The following are examples of urgent requests sent in fraudulent emails:

"If you don`t respond within 24h after receiving this Mail Information your account will be deactivated and removed from our server (your account suspension will be made due to several discrepancies in your registration information as explained in Section 9 of the eBay User Agreement."

"Please, give us the following information so that we could fully verify your identity. Otherwise your access to Earthlink services will be closed."

2.5 Security Promises

Phishing emails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient's trust. The following are assurances that were included in fraudulent emails:

"Remember: eBay will not ask you for sensitive personal information (such as your password, credit card and bank account numbers, social security number, etc.) in an email." *Note: This email sends you to a fraudulent Web site that does ask for your personal and account information.*

"Your information is submitted via a secure server. EarthLink keeps all of your contact and billing information confidential and private."

Fraudulent email messages also frequently use the TRUSTe symbol at the bottom of the email. The TRUSTe symbol is meant to be used by businesses that agree to a high standard of personal information protection. (*See* http://www.truste.org/) Unfortunately this symbol is abused in phishing emails.

2.6 Collecting Information in the Email

The earliest phishing emails used HTML forms within the email to gather information. This method of phishing is still used in some of today's scams. Once the information has been entered, the email must provide a method of sending the information to the fraudster. Generally the "Submit" button at the bottom of the form causes the information to be sent to the fraudster's specified location.

In the two examples below, the "action" attribute shows the actual destination of the submitted information. In the first example, the form is located in what appears to be an eBay email, but the action attribute shows that the information was actually sent to "www.christmas-offer.com."

<FORM action=http://www.christmas-offer.com/sendmail.php method=get target=_blank>

<FORM action="http://mail.yahoo.com/config/login?/ebay.php" method="post" name= "mailbomber" target="_blank">

2.7 Links to Web Sites That Gather Information

Now most phishing emails provide a link that takes the recipient to a Web site instead of using forms within the email. Some fraudsters register domain names that are very similar to those owned by a reputable company. For example, one fraudulent eBay email message used the following link: "http://ebay-securitycheck.easy.dk3.com/Ebayupdatessl.html."   The real eBay site is located at www.eBay.com.   The fraudster registered the domain name "http://ebay-securitycheck.easy.dk3.com" in the hopes of fooling the recipient into believing that this URL is owned by eBay. Other fraudsters try to conceal the true destination of the link by using HTML coding tricks.

2.8 Link Text in Email Differs From Link Destination

In fraudulent email messages, the link text seen in the email is usually different than the actual link destination. In the following example, the email looks as though it is going to send the user to "http://account.earthlink.com," but instead sends the user to "http://www.memberupdating.com."

 http://account.earthlink.com

2.9   Using onMouseOver to Hide the Link

Some fraudsters use the JavaScript event handler "onMouseOver" to show a false URL in the status bar of the user's email application. The following code was taken from a fraudulent PayPal email. When the user puts the

mouse over the link, the status bar will show "https://www.paypal.com/cgi-bin/webscr?cmd=_login-run." However the link actually takes the user to "http://leasurelandscapes.com/snow/webscr.dll."

```
<A onmouseover="window.status='https://www.paypal.com/cgi-bin/webscr?cmd=_login-run'; return true"
onmouseout="window.status='https://www.paypal.com/cgi-bin/webscr?cmd=_login-run'"href="http://
leasurelandscapes.com/snow/webscr.dll">https://www.paypal.com/cgi-bin/webscr?cmd=_login-run</A>
```

2.10 Using the IP Address

In the example in section 2.8 above, the code clearly shows the true destination of the link: "www.memberupdating.com." Frequently, fraudsters attempt to conceal the destination Web site by obscuring the URL. One method of concealing the destination is to use the IP address of the Web site, rather than the hostname. An example of an IP address used in a fraudulent email message is "http://210.14.228.66/sr/." An IP address can be obscured further by expressing it in Dword, Octal, or Hexadecimal format. [5]

2.11 Using the @ Symbol to Confuse

When the at symbol (@) is used in an "http://" or "https://" URL, all text before the @ symbol is ignored and the browser references only the information following the @ symbol. In other words, if the format *<userinfo>@<host>* is used, the browser is directed to the *<host>* site and the *<userinfo>* is ignored. This trick is used by scammers in hopes of fooling the person viewing the email code into thinking the link is going to the site listed before the @ symbol, while it actually links to the fraudulent site after the @ symbol.

In the example below, the link may appear to be sending the user to eBay at "http://cgi1.ebay.com.aw-cgiebayISAPI.dll." However, this text before the @ symbol is ignored and the link sends the user to "210.93.131.250/my/index.htm," which is the fraudulent Web site's IP address.

http://cgi1.ebay.com.aw-cgiebayISAPI.dll%00@210.93.131.250/my/index.htm

To further conceal the URL, the @ symbol can be represented by its hexadecimal character code "%40." [5]

2.12 Hiding the Host Information

Links in emails using the *<userinfo>@<host>* format discussed in section 2.11 sometimes take the trick a step further by inserting a null or other unprintable character before the @ symbol, which prevents the host information from being displayed in the address bar of the browser. Web browsers generally display the URL information for the current Web page in the address bar. However, if the *<userinfo><null>@<host>* format is used in the link in the email, some versions of Microsoft Internet Explorer will not display the host information. [12] For example, if a fraudster uses the format *<userinfo><null>@<host>*, the *<userinfo>* is displayed in the browser address bar in Microsoft Internet Explorer and the *<host>* information is concealed. Using the same example given above:

http://cgi1.ebay.com.aw-cgiebayISAPI.dll%00@210.93.131.250/my/index.htm

The character represented by "%00" causes only the userinfo "http://cgi1.ebay.com.aw-cgiebayISAPI.dll" to be displayed in the browser address bar, but the Web page is actually accessed by the host information, "210.93.131.250/my/index.htm."

Microsoft released a patch for version 6 of Internet Explorer that no longer allows the use of the @ symbol in URLs. After the patch has been installed, using an @ symbol in a URL causes an "invalid syntax error" message. [13] Unfortunately another vulnerability was recently discovered in Internet Explorer: if the fraudster has control of the Web server's DNS configuration, the fraudulent Web page can cause Internet Explorer to display a different URL than the page's actual URL. Moreover, this vulnerability is more serious than merely giving a false appearance to the user: it also allows a fraudster to defeat Internet Explorer's security zone privilege model and possibly execute scripts and other malicious code on the client's PC. [14] URL vulnerabilities were also found in Mozilla [1], and in Opera browsers. [15]

2.13 Using Hexadecimal Character Codes

Fraudsters can also hide URLs by using hexadecimal character codes to represent the numbers in the IP address. Each hexadecimal character code begins with "%." This next example combines a few of the fraud tricks mentioned above:

http://www.visa.com%00@%32%32%30%2E%36%38%2E%32%31%34%2E%32%31%33

The URL is put in *<userinfo><null>@<host>* format. On computers using Microsoft Internet Explorer that have not installed the patch, only the www.visa.com is displayed in the address bar, but the browser window displays the site at "%32%32%30%2E%36%38%2E%32%31%34%2E%32%31%33," which is the fraudulent Web site's IP address hidden in hexadecimal character code. The code converts to: "http://220.68.214.213" (Conversion tool located at http://www.zegelin.com/computers_files/ref/ACSII.htm).

2.14 Redirecting the URL

A URL can be further obscured by using a redirection service. For example, cjb.net and tinyurl.com provide redirection services that assign the user an alias for the user's specified URL. For example, a URL such as "http://tinyurl.com/3" is provided by tinyurl.com when the user enters a URL into the site. When a redirection service is used, the provided link sends the user to the service site (e.g., cjb or tinyurl) and the service site then forwards the user to the intended site. This service is useful for replacing long URLs, but unfortunately it can be abused by fraudsters because it hides the true destination of the link.

Some fraudsters have even gone to the effort to redirect their URL twice. The link "http://r.aol.com/cgi/redir?http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn" was found in a fraudulent Citibank email message and shows a double-redirect. First the browser is sent to "http://r.aol.com/cgi." Then the browser is redirected to "http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn," which is an alias provided by cjb.net. Finally cjb.net redirects the browser a second time to the intended Web page (the actual URL is stored at cjb.net and is accessed through the cjb.net alias).

2.15 Switching Ports

Web pages are accessed on servers through ports. A port can be specified by following the URL with a colon and the port number. If no port is specified, the browser uses port 80, the default port for Web pages. Scammers occasionally use other ports to hide their location. In the following example, the IP address after the @ symbol is followed by ":8034", which represents the specified port of 8034.

http://www.citibankonline.com:ac-KTtF4BD6y4TZlcv6GT5D@64.29.173.91:8034/

Some scammers even hack into a legitimate company's server and host their Web site on the server using a higher numbered port. The legitimate company may be completely unaware of the fraudulent site.

3 Tricks Used in Fraudulent Web Sites

Scammers use all of the phishing email tricks to fool users into submitting their personal information. In most phishing emails, this means convincing the recipients to click on a link in the email, which brings them to a fraudulent Web page. Once there, the fraudster must continue to convince the recipients that their personal information is required. The following include deceptive devices used by scammers on their fraudulent Web pages.

3.1 Continuing to Spoof the Company

Fraudsters continue to emulate the company they are spoofing in the fraudulent Web pages by using, images from the real Web sites, and similar fonts and color schemes. Some use the code from the real company's Web

pages and merely change a few essential details, such as where the information is submitted or a link to forward the user to another fraudulent Web page. Many fraudulent Web pages look virtually identical to the real Web site.

3.2 SSL Certificates

A URL that begins with "https://" (instead of "http://") indicates that information is being transmitted over a secure connection and the company has been issued an Secure Sockets Layer (SSL) certificate. Some fraudulent sites use an "https://" URL to appear as a legitimate site. The following is a link to a fraudulent PayPal site:

    https://www.paypal.com%01[string of ~ 60 "%01" elided]@207.173.185.20/f/

Clicking on this link brought the user to "https:// 207.173.185.20/f/" and opened a security alert, which warned the viewer that the certificate had been issued by a company that the user had not chosen to trust and the name on the security certificate was invalid or did not match the name on the site. However, most users are unsure what this information may indicate and these warnings are not uncommon when trying to access legitimate sites. Even with this warning, an invalid or fake certificate may make the user feel more secure in the transaction.

3.3 Gathering Information Through Web Pages

Once the recipient follows the link to the fraudulent Web site, information is gathered through forms and sent to the scammers. This process is similar to sending information through forms in emails, as discussed above. However, using Web pages instead of email forms provides more flexibility to the fraudsters. Not only do the fraudulent Web pages have forms to gather information, many often contain introduction pages, pages indicating the information is being processed, and pages thanking the recipient for the information. Frequently, the browser is redirected to the real company's Web site after the information has been collected in an attempt to further fool the recipient into believing that the request for the information came from the spoofed company.

3.4 Checking the Browser

JavaScript allows browser name and version detection. Some fraudsters use this information to restrict which browsers can view their site. In a PayPal fraud, the Web page was coded to only show the fraudulent Web page if the user opened the page in Internet Explorer. If the user tried to open the page in a different browser, the browser was redirected to the real PayPal site. Fraudsters might use this trick because they are taking advantage of a security hole or function that is only available on a specific browser.

3.5 Fake Address Bar

Another trick used on fraudulent Web pages is displaying a fake address bar. One method of accomplishing this is to use JavaScript to close the browser's address bar and display a fake address bar that is part of a table in the Web page, with the first row containing the fake address bar and the second row contained the rest of the fraudulent Web page. The fake address bar can appear to contain a legitimate "https://" URL by using a form field with an assigned value. More recently, fraudsters are using JavaScript to create fake address bars by opening a very small second browser window that appears as just a small white box displaying a fake URL that covers part of the address bar of the fraudulent Web page.

3.6 Using Pop-Ups

Many fraudulent Web pages are opened as pop-ups. Fraudsters cause the email link to go to the fraudulent Web site, which generates the fraudulent pop-up, and then redirects the main browser window to the real company site. This transaction appears to the user as a pop-up over the real company site. Fraudsters use this technique to make their information gathering appear more credible. Some fraudsters use JavaScript to reopen the fraudulent pop-ups if closed until the user fills out the requested information.

Using a pop-up with the browser menu disabled discourages the viewer from saving the page. The viewer is limited to saving the source code by right-clicking on the pop-up, selecting View Source, and saving the code.

3.7 Disabling Right-Click

As discussed above, using pop-ups makes it difficult to save the page. Some fraudsters take their fraudulent pop-ups a step further and use JavaScript to disable the right-click function, which prevents the user from viewing and saving the source code. Sometimes the right-click function is also disabled on fraudulent Web pages that are opened in the menu browser window. However, when this occurs, the user can use the menu bar at the top of the page to save or view the source of the page.

The right-click functionality is disabled by coding the Web page to display an alert if the user clicks on the right mouse button. The following is JavaScript taken from a fraudulent PayPal Web site.

```
function click() {
if (event.button==2) {
alert('WARNING ! © Copyright 1999-2004 PayPal. All Rights Reserved.')}}
```

3.8 Processing Submitted Information

Some fraudulent Web sites apparently process the information provided by the victim when the information is submitted. For example, some sites run the credit card numbers to ensure they are valid, while others send the user ID and password information through the real company's site to verify that they are legitimate. If the user submits false or incorrect information, the page generates an error message. The Web site will not continue to the next step unless the user enters valid information.

3.9 Buying Time to Access Accounts

In some phishing scams, the fraudsters try to buy some time before their victims check on their accounts to give the fraudsters an opportunity to use the personal information they have acquired. The scammers indicate in either the email message or the Web pages that it will take a certain amount of time for the account to be updated. They hope that this will prevent their victims from checking their accounts during this time period. Here are some examples from phishing scams (*Note: The misspelled words and poor grammar are another indication that these are fraudulent requests for information*):

"Your submited information will be verified by eBay Accounts Management Departament in 24 hours."

"This process will take 5 days, period when you will not be able to acces your eBay account. After this period you will receive instructions to enter and securise your eBay account."

4 Using Viruses to Phish

This paper focuses on phishing email messages that directly collect information from the recipient through either the email message or through a fraudulent Web site. Phishing can also be conducted through viruses or trojans, which can be sent as attachments to emails or as downloads on Web sites.

For example, fraudsters created phishing emails that contained a link that sent the user to a Web site that took advantage of a vulnerability in the Compiled Help File (CHM) functionality in Internet Explorer to download a keylogging trojan onto the user's computer. This trojan recorded any information entered into designated bank Web sites and sent the data to the fraudster. [4] and [11] Recently, another virus called Scob, took advantage of three different flaws in Microsoft products. The virus infected hundreds, if not thousands, of Web sites, including many trusted sites, and downloaded a keylogging trojan onto the Web sites' visitors' computers. Once infected, a computer recorded the user's keystrokes, including credit card numbers, bank accounts and passwords, and sent the information to the scammers. [6]

5 New Trends & Conclusion

Generally fraudulent emails use generic salutations such as Dear Customer or Dear Member, or insert the email address as a salutation. By educating companies to address their customers by name, generic emails can be identified as fraudulent. However, an article by SFGate.com reports that hackers were able to trick merchants into providing access to their accounts. The hackers were able to download customer information including names, email addresses, home addresses and transaction information. This data can now be used in fraudulent emails not only to personalize the salutation, but also to reference recent transactions, making them even more convincing. [7] Fraudsters will continue to adapt and expand their methods to reach and defraud their victims.

Email fraudsters go to great lengths to fool even the most wary of Internet users. Although it is important to educate people about email fraud, many of the tricks outlined in this paper will escape the average Internet user. Email fraud will only continue to get more sophisticated. By analyzing the tricks used by the scammers, we are better equipped to create technology that can surmount Internet fraud.

6 References

1. Aughton, Simon. "Phishing Vulnerability Identified in Mozilla." <u>PC Pro</u>. 14 June 2004.
   <http://www.pcpro.co.uk/?http://www.pcpro.co.uk/news/news_story.php?id=58926>
2. Anti-Phishing Working Group (APWG). "Phishing Attack Trends Report - April 2004." May 2004.
   <http://www.antiphishing.org/APWG_Phishing_Attack_Report-Apr2004.pdf>
3. Anti-Phishing Working Group (APWG). "Phishing Attack Trends Report - May 2004." June 2004.
   <http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf>
4. Dawnstar posted "'Sydney Opera House Fire' Trojan Warning," 16 June 2004, and "The 'Insulting' Trojan,"
   7 June 2004. <http://www.codephish.info/>
5. "How to Obscure Any URL: How Spammers and Scammers Hide and Confuse." 13 Jan. 2002.
   <http://www.pc-help.org/obscure.htm.>
6. Jesdanun, Anick. "Web Virus May be Stealing Financial Data." <u>The Mercury News</u>. 25 June 2004.
   <http://www.mercurynews.com/mld/mercurynews/business/technology/9012883.htm>
7. Kirby, Carrie. "New Scam Threat at eBay: Hackers Obtained Information on Some Customers."
   <u>SFGate.com</u>. 16 March 2004. < http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/
   03/16/BUG5T5LCM31.DTL&type=business>
8. Leyden, John. "Fear of Phishing Hits E-Commerce" <u>The Register</u>. 5 May 2004.
   <http://www.theregister.co.uk/2004/05/05/phishing_fears_survey/>
9. Liddell, Craig. "On-line Payment Reduces Identity Fraud." <u>Electricnews.net</u>. 6 April 2004.
   <http://www.enn.ie/frontpage/news-9406748.html>
10. Litan, Avivah and John Pescatore. "Catching Phishers Requires More than Bait" <u>Gartner Research</u>. 8 June
    2004. <http://www.protectingthenet.com/archives/Phishers.pdf>
11. Manion, Art. "Cross-Domain Vulnerability in Outlook Express MHTML Protocol Handler." <u>US-CERT</u>.
    Revised 26 April 2004. <http://www.us-cert.gov/cas/techalerts/TA04-099A.html>
12. Manion, Art and Shawn Hernan. "Vulnerability Note VU#652278: Microsoft Internet Explorer Does Not
    Properly Display URLs." <u>US-CERT</u>. 17 Feb. 2004. <http://www.kb.cert.org/vuls/id/652278.>
13. Monosson, Rich. "Microsoft Issues Critical Update on URL Spoofing." <u>Netcraft</u>. 3 Feb. 2004.
    <http://news.netcraft.com/archives/2004/02/03/microsoft_issues_critical_update_on_url_spoofing.html>
14. Munro, Jay. "Security Watch Letter: Adware, Phishing Plague IE Users" <u>PC Magazine</u>. 14 June 2004.
    <http://www.pcmag.com/article2/0,1759,1612119,00.asp>
15. "Opera Fixes Phishing Flaw" <u>TechWeb News</u>. 4 June 2004.
    <http://www.techweb.com/wire/story/TWB20040604S0002>
16. Van Dyke, James. "Online Account Management as the Antidote to Fraud: Financial Institutions and Billers
    Must Revamp Their Web Features and Messages." <u>Javelin Strategy & Research</u>. March 2004.
    <http://www.javelinstrategy.com/rp.html>
17. Varghese, Sam. "Phishing Spreads in Europe." <u>smh.com.au</u>. 10 May 2004.
    <http://www.smh.com.au/articles/2004/05/10/1084041315645.html?oneclick=true>
18. Warner, Bernhard. "Billions of 'Phishing' E-mails Sent Monthly." <u>Reuters</u>. 6 May 2004.
    <http://www.ladlass.com/archives/002196.html>