Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Phishing: An Analysis of a Growing Problem

Email has become an invaluable communication tool for both business and personal use. Among the many security issues that now affect computer users, there is a growing threat known as "phishing". Phishing attacks are perpetrated by criminals who send deceptive emails in order to lure someone into visiting a fraudulent web site or downloading malicious software, expressly for stealing sensitive information such as credit card numbers, account information, passwords, etc. This paper gives an in-depth analysis of what phi...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Phishing:

An Analysis of a Growing Threat

Anthony Elledge

GIAC Security Essentials Certification (GSEC) Practical

Version 1.4b, Option 1

Original Version: May 2004

Updated January 2007

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

ABSTRACT

E-mail has become an invaluable communication tool, both for business and personal use. Among the many security issues that affect computer users, there is a rapidly growing threat known as "*phishing*". Criminals use phishing attacks to lure the unsuspecting into visiting a fraudulent web site, calling a fraudulent phone number, or downloading malicious software, expressly to steal sensitive information such as credit card numbers, account credentials, social security numbers, PINS, or passwords.

This paper gives an in-depth analysis of phishing: what it is, the technologies and security weaknesses it takes advantage of, the dangers it poses to end users, and insights into what can be done to curb the effects of this crime.

1. INTRODUCTION

You receive an e-mail from your credit card company informing you that your account has been deactivated because of suspicious activity. The message requests you to click a web link and log in to verify your account information. Following the instructions, you are directed to what appears to be the "Online Update" page of your credit card company. Here you are asked to enter your name, password, account number, social security number, and PIN. It all seems legitimate: the logos look proper, the web address of the page looks convincing, and the format of the site is the same as you remember. However, this is a scam; the e-mail is a fraud, and now a cyber-criminal has your personal information. He or she can now use or change your account or open new accounts in your name. You have become a victim of a growing crime called phishing.

Every day millions of e-mails are sent around the globe, millions of web pages are accessed to gather information, and millions of people use online sites to transact business. We strive to trust the systems that are in place to deliver our e-mail messages and to route us to the proper web servers. We want to believe that e-mail is from "reputable" sources, and we are keen to assume the web sites we visit are legitimate. Unfortunately, a growing number of cyber-thieves are using these same systems to manipulate us and steal our private information; they take advantage of people's trusting nature, or, in some cases, their naiveté.

In this analysis I will explain the concepts and technology behind phishing, show how the threat is much more than just a nuisance or passing trend, and discuss how gangs of criminals are using these scams to make a great deal of money. I will give some hints and suggestions you can use to protect yourself from these scams using defense-in-depth techniques, and explain a few of the tools and technologies being developed to combat the serious threat of identity theft and online fraud.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2. WHAT IS PHISHING?

Phishing, also known as "brand spoofing" or "carding", is a term used to describe various scams that use (primarily) fraudulent e-mail messages, sent by criminals, to trick you into divulging personal information. The criminals use this information to steal your identity, rob your bank account, or take over your computer. Counterfeit web sites, using "hijacked" company brands and logos, are created to lure you into revealing information you would not want to be public knowledge. These digital thugs are "*phishing*" for any data they can obtain to prey on people and further their criminal activities.

The Anti-Phishing Working Group (APWG), states that the term *phishing* "comes from the analogy that Internet scammers are using e-mail lures to 'fish' for passwords and financial data from the sea of Internet users" [2]. Apparently, the "*ph*" was used as a tribute to the term "phone phreaking", a technique used in the early days of hacking to take advantage of security weaknesses in the phone systems. Phishing is defined as the use of "spoofed" (hoax) e-mails and fraudulent web sites for the purpose of fooling users into revealing personal data [1]. Although e-mail is the primary channel for phishing attacks, some scams are using instant messaging (IM), fake news bulletins, and social communities such as MySpace™ to fool users into divulging personal information.

The concept of phishing has actually been around for years. The term "phishing" was first used by hackers to describe stealing America Online® (AOL) accounts by acquiring usernames and passwords. With the ubiquitous spread of e-mail and internet access, the potential for criminals to take advantage of the technology has increased considerably in the last few years, with an almost exponential increase in incidents since 2003, according to many organizations that are trying to track this trend. Flaws in e-mail protocols, security weaknesses in browser software, a basic lack of computer security education, and continuing susceptibility to social engineering attacks all contribute to the increase in incidents, as criminals are able to exploit these weaknesses to their advantage.

3. THE THREATS FROM PHISHING

One of the primary threats from phishing is identity theft. Consumers go to great lengths to protect their personal information, but a single breach of security can expose a person to a multitude of threats, including credit card fraud, damaged credit, having an identity used for criminal activity, stolen bank information, unauthorized use of accounts (online and otherwise), or stolen money. There are also intangible threats, such as damage to credibility, loss of trust, or embarrassment; having personal information stolen can cost a great deal more than lost cash. According to The Identity Theft Resource Center, the average time spent repairing the damage caused by a stolen identity is approximately 600 hours and it can take years to completely recover [8]. For consumers, this can equal lost salary, lost time, frustration, stress, and embarrassment, not to mention a sense of being violated.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Phishing is not just a “small-time” operation. Phishing is a business, and billions of dollars are being made by criminals while consumers and businesses are left to suffer the consequences. There are gangs of phishers organized all over the world, but primarily in Eastern Europe, Asia, Africa, and the Middle East, using sophisticated and elaborate schemes to steal personal information [1].

Phishing is also used extensively by organized crime groups [31]. There is a great deal of money at stake, and if a gang can steal bank account information from only a small percentage of those who get duped, thousands, or possibly millions, of dollars can be stolen. A recent article in Consumer Reports, based on their “State of the Net” survey, stated, “Online consumers who fell prey to phishing schemes experienced a five-fold increase in financial losses since 2005” [30]. Recently, a major Swedish bank had losses over $1 million from a phishing attack that targeted the bank’s customers. Another attack, on E-Trade™, used stolen identities, acquired from a hacked computer, to carry out a “pump-and-dump” scheme, in which the criminals drove up the prices of low-priced stocks through high-volume purchases and then sold those shares at a profit. The cost of the fraud: close to $18 million. Ameritrade™ had a similar incident, losing close to $4 million [38]. This is a very real threat, not only to consumers, but also to the companies that are targets of these scams, and, moreover, to the entire worldwide financial systems.

Terrorists are known to use phishing and other identity theft scams to gain employment, obtain fake identification as cover for attacks, and to finance their activities. For example, an Al-Qaeda group in Spain used stolen credit cards to setup their crimes and make purchases for the group. They also used stolen calling cards for communications [31].

Companies whose brands are hijacked (used fraudulently) may be poised for all matter of loses. They can lose money in the form of stolen cash, lost productivity, reimbursements to customers, or they may lose customers who believe the company is to blame for not protecting them, no matter how unfounded this may be. Scams can erode consumer confidence in companies that are targets of the schemes, particularly high-profile ones, leaving the company with public-relations troubles, and a company’s branding has a real possibility of becoming irrevocably tarnished.

Legal action is increasingly being pursued against companies for losses by customers who become victims of phishing. Whether or not the litigation is successful, the damage to the company’s image and the cost of legal fees can be substantial. Some companies offer complete compensation to customers whose accounts are abused. While this may be a good customer-relations tactic, with phishing attacks on the rise, this could cost a great deal to a high-profile company such as Amazon.com ® or Bank of America ®, particularly if they have a substantial number of claims.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The number of phishing attacks has increased drastically over the past few years, according to the APWG. Increasingly sophisticated techniques are being used and more devious attacks developed. Figure 1 depicts the number of unique phishing reports to the APWG between November 2005 and November 2006:

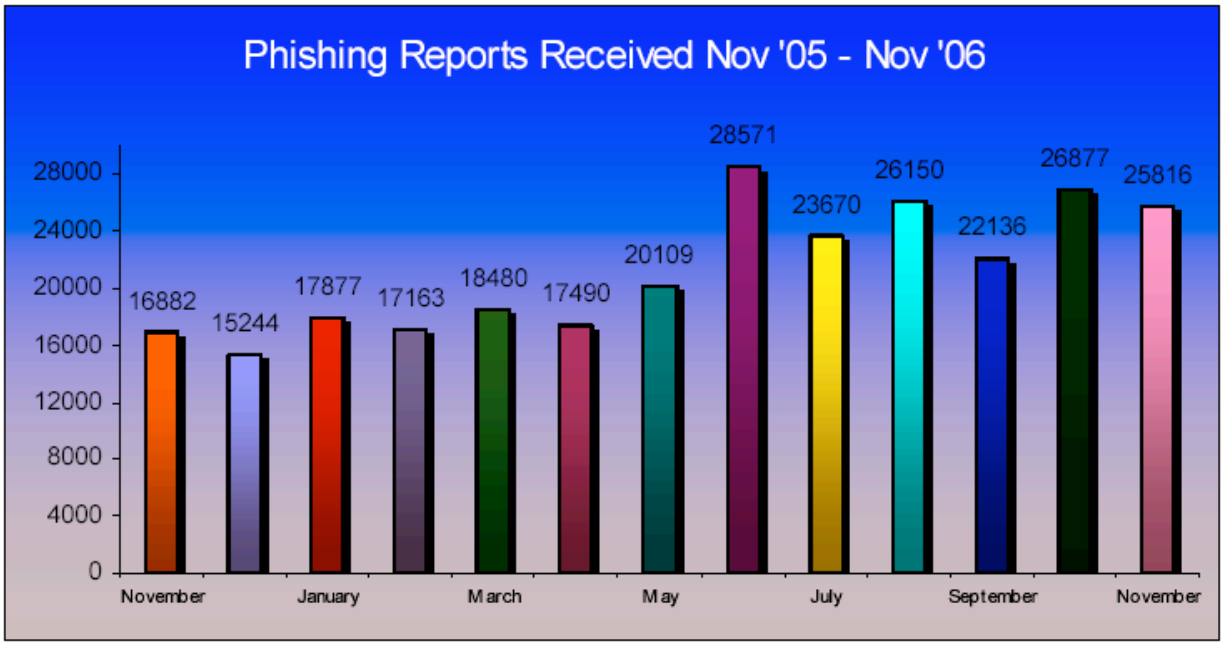

Figure 1. Phishing reports received November 2005 – November 2006. *Courtesy of the Anti-Phishing Working Group.*

Figure 2 shows the dramatic rise in the number of unique phishing websites reported as of November 2006. With this level of increase, coupled with the increase in sophistication, the threat to consumers and businesses is significant.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

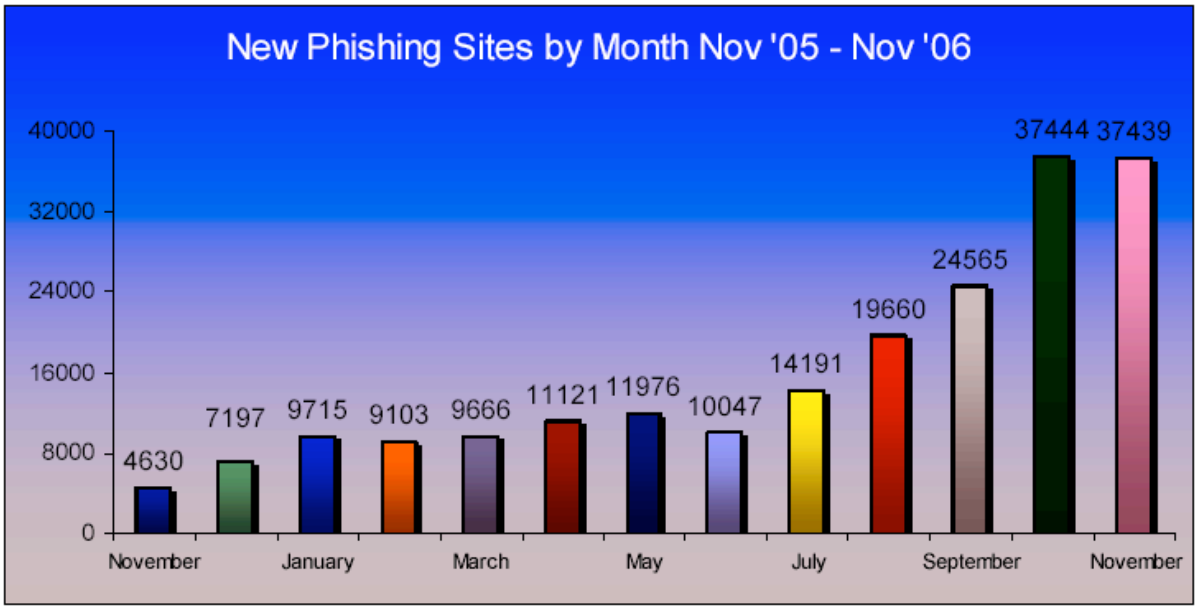

Figure 2. New phishing sites by month, November 2005 – November 2006. *Courtesy of Anti-Phishing Working Group*

A threat that many experts have grown more concerned about is the level of trust consumers have in e-mail, online commerce, and the companies they deal with online. Many institutions have stopped communicating with customer's via e-mail altogether to help eliminate the possibility that the user may become a victim of phishing. This seems to point to a disturbing consequence of the increase in all forms of online fraud, not just phishing: if consumers become wary of using e-mail and the Internet, online commerce may begin to suffer, according to many experts. Could this point to a shift in the way online banking and commerce is implemented?

4. A TECHNICAL BACKGROUND

To understand how phishing works and why it is so easy to perpetrate, a bit of technical background regarding the protocols, technology, and tactics behind the schemes may be helpful. The following are some of the main elements related to phishing attacks:

Simple Mail Transfer Protocol (SMTP)

SMTP is the protocol used to transmit e-mail over the Internet. It was originally described in a Request for Comments (RFC) by Dr. Jonathan Postel in 1982 (RFC 821). According to the RFC, "the objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently." [13] Notice that it doesn't include "securely" in that statement. SMTP has no built-in security measures to confirm who is sending an e-mail. All it does is communicate with an SMTP server on the receiving side, in essence, telling the other

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

system “who” it is, who the e-mail is from (sender), and who the e-mail is destined for (recipient). There is no guarantee that the sender of the e-mail is legitimate or if their address is fake.

The sending SMTP server initiates a MAIL command to the receiving SMTP server. This MAIL command indicates the sender of the e-mail. The receiving server will reply if it is able to receive mail and if a user with the specified address is a user on that system. The sending server then transmits a RCPT command to identify the recipient of the e-mail [13]. The two systems negotiate back and forth until the message is delivered, at which time the transmission is complete and the servers say “ok” and “goodbye”, so to speak. Nowhere is there any validation to confirm the sender of the message. Researchers are working to make e-mail protocols more secure; however, for the near future, this is what we have to work with.

```
             +----------+                 +----------+
+------+     |          |                 |          |
| User |<-->|          |      SMTP       |          |
+------+     |  Sender- |Commands/Replies| Receiver-|
+------+     |   SMTP   |<--------------->|    SMTP  |     +------+
| File |<-->|          |    and Mail     |          |<-->| File |
|System|     |          |                 |          |     |System|
+------+     +----------+                 +----------+     +------+


              Sender-SMTP                 Receiver-SMTP
```

Figure 4. The SMTP Model. (Courtesy of The Internet Engineering Taskforce, http://www.ietf.org/rfc/rfc821.txt)

HTML-based E-mail

E-mail messages can be transmitted as either plain text, with no graphics or formatting, or they may be formatted as mini web pages, capable of displaying graphics, formatted text, even able to run scripts. This makes phishing a much easier task. For this reason phishers usually send their hoax e-mails in HTML format, embedding graphics and formatted text to make it look more like a legitimate communication from the spoofed company. Logos, banners, even ads are placed within the e-mail to entice the recipient to believe that the message is authentic. If the message was plain text, with only a URL (Uniform Resource Locator) link, the user *may* become more suspicious and less likely to click on it.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

HTML Forms

One scheme involves using HTML-based forms within an HTML-formatted e-mail. The code in the form is hidden; therefore, the phisher is able to hide a bogus URL in a Submit button that the user presses after entering his or her personal information. As a result, it is more likely that the casual user will be enticed by a form-based attack [11].

Domain Naming System (DNS)

DNS is the hierarchical "database" that converts numerical internet protocol (IP) numbers to human-readable names. When you type in *www.somesite.com* the name is associated with the IP number and takes you to the server at that address. There are several security issues with DNS. Cyber-criminals may "hijack" a domain, redirecting traffic from the legitimate web site to a malicious site that is setup to look identical to the original (pharming), or, more easily, they can create a totally new domain name that looks so similar that an unsuspecting user may not notice the difference. One incident involved a phishing scam that came from the domain *www.aol-billing.net*, a fraudulent domain name entirely unassociated with America Online, but it appears convincing to an unsuspecting user.

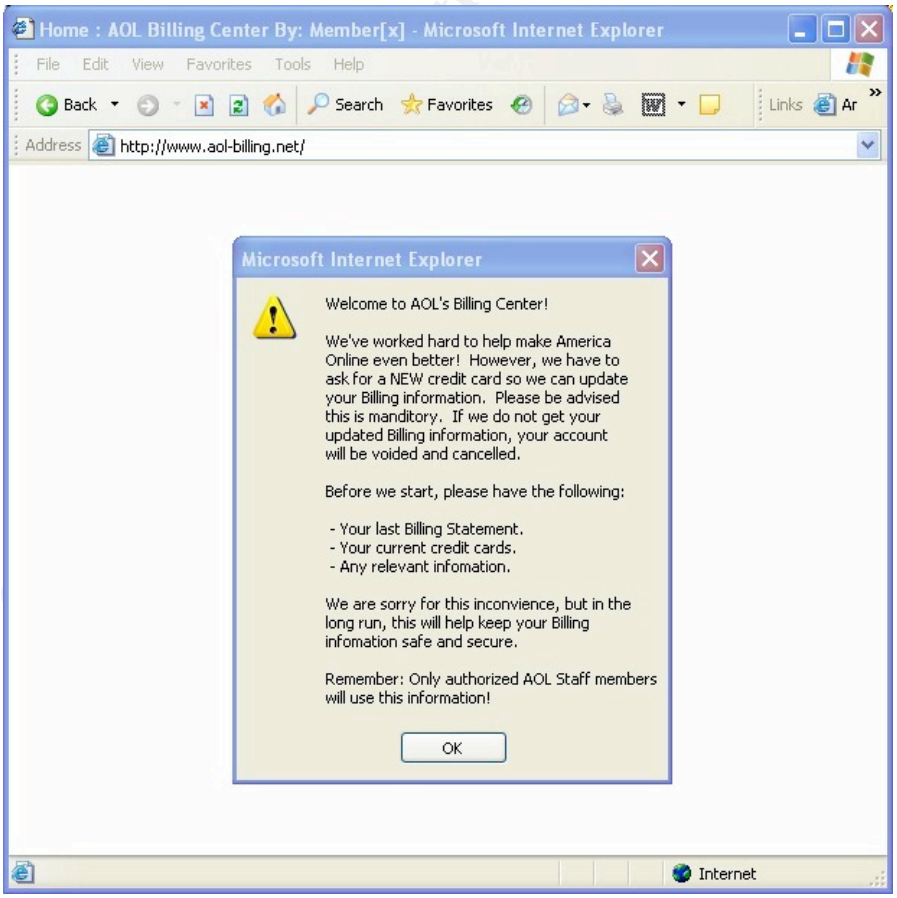

Figure 5. Fraudulent AOL billing web site. Courtesy of Anti-Phishing Working Group (http://www.antiphishing.org/phishing_archive/aol_03-10-04.htm)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Trojan Horse

A Trojan horse is a malicious software program (malware) that masquerades as legitimate software. Malware can be installed by worms or viruses, or unknowingly by the user, thinking the software is a game or utility or a browser plug-in. It may also be installed via Internet Relay Chat (IRC) sites. More sophisticated phishing scams use Trojan horses to install keystroke loggers to capture a user's passwords and account numbers, or install programs to take screenshots of the system. These images may have usernames, passwords, or credit card numbers that are then forwarded to the phisher.

Browser Insecurities

There are security holes in web browsers that can make a phisher's crime easier to accomplish. A glitch in (un-patched versions of) Microsoft Internet Explorer™ allows a specially crafted URL to load a browser window that appears to be displaying any address the attacker wants [19]. The attacker embeds a URL into an e-mail using the form:

http://www.sometrustedsite.com%01%00@malicious-site.com/malicious.html [23]

When a mouse cursor is over the link, it appears to be a link to *www.sometrustedsite.com*; however, when clicked, the link points to *malicious-site.com*, where a fake web page has been set up. This hole was fixed by Microsoft, but it may only be a matter of time until another hole is found that will allow some other type of fraud. This underscores the need to keep up with all security patches [43].

Malicious Javascript

One of the more sophisticated techniques discovered, according to the Anti-Phishing Working Group, involves the use of scripting to create fake browser address bars or other areas of the browser interface, known as the "chrome". The script fakes the browser chrome—modifying the address bar, status bar, menus, etc.—making it indistinguishable from the real browser. When a user types in an address, the malicious code can route them to the fraudster's web site. Even the "https" and the "lock" icon within the browser can be forged, making the user think they are safe, when in fact they are not.

Cross-Site Scripting

Cross-site scripting (XSS) involves the injection of malicious code into a web application. If a web application—the login page of a bank for example—is not properly designed or does not perform proper validation, malicious code can be inserted and run on that site. A phisher could lure an unsuspecting user to follow a link to a vulnerable site and craft the URL in such a way that his malicious code runs on the bank's site. The user thinks he is browsing safely on the bank's page, when actually he is running the malicious code. The code can then do any number of things, such as displaying a fake login form or an

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

"Update Your Information for Our Records" form. The information that is entered by the user is then redirected to the phisher's fake site. Many well-known sites have been vulnerable to this type of attack, and it continues to be a major problem. According to SANS Institute, "Cross site scripting is the most pernicious and easily found web application security issue." [41].

Social Engineering

One of the most effective tools in the phisher arsenal is the ability to fool someone into divulging personal information—this is social engineering. Social engineering methods are used to make a person believe they are dealing with a legitimate person or company, when in fact they are not. The hoax e-mails used in phishing schemes allege to be from a trusted entity, or an instant message seems to come from a "buddy", so the user is more likely to trust them. Social engineering can be a very successful ploy, not only for phishing scams, but for other criminal activities as well.

5. THE ATTACK

Traditional Attack

A "typical" phishing attack is launched using spam e-mail messages, usually sent to thousands or even millions of e-mail addresses. The e-mails are forged with a "From" or "Reply to" address that makes them appear to be from a reputable or trusted source, such as a bank or credit card company. The messages are often sent in Hyper-Text Markup Language (HTML) format (as opposed to text-only) and may use logos, URLs, legal disclaimers, etc., taken from the spoofed company's website. This makes the attack all the more insidious since the average user may not question an e-mail if it appears to be from his or her bank and has that bank's logo on it.

Phishers play the odds when sending their mass-mailings. Of the thousands of messages sent, only a small percentage of the recipients may actually be a customer of the spoofed company. For instance, if the phisher has spoofed PayPal ®, an online payment company, the number of e-mails sent to actual PayPal customers who then fall for the scheme might be relatively small; however, it is estimated that around five percent of the phishing e-mails sent actually are successful [1]. This can result in quite hefty profits for the scammers.

There have been many different variations of phishing scams, but the e-mail messages are usually structured to prey, ironically, on the computer user's fear of being a victim of fraud or hacking, or may be a message stating that the company needs to update their records:

"*Our records show your account information is out of date. Please click on the following link to confirm your information*" …

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

If the victim follows the link, their browser is directed to an address that might look very similar to the one they would expect. This is another ploy used by phishers: registering domain names with similar looking addresses or using character replacement (using the number "1" for the lowercase letter "L" for example) to disguise the fake address. Many people can be fooled since they may not notice the difference. The URL can also be displayed within the e-mail as the actual legitimate address (e.g., www.aol.com), but another web address—the phony phisher address—has been embedded using deceptive techniques (explained earlier). The victim may be taken to a web site that looks identical to their bank's, or eBay ®, or AOL ®, with the same icons, graphics, and text. The fraudulent site is set up to display an interface for the user to enter his or her information, thinking they are entering it at the company's web site. Some of the more well-known and publicized phishing scams involve high-profile sites such as eBay and PayPal. Scammers use company logos and designs to make the messages look legitimate. The message may tell the user that money needs to be transferred or that their account is out of date and needs to be modified. When the user follows the link, they are taken to what they believe to be the legitimate web site and are asked to enter personal information, such as their bank account or social security number. The scammers capture this information and use it to steal the victim's identity or to fraudulently use accounts.

Figure 3. Spoofed eBay web page. Courtesy of AskDaveTaylor.com. (http://www.askdavetaylor.com/0-blog-pics/ebay-phishing-page.png)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Spear Phishing

Computer users have become more educated about the threats from online fraud and phishing, avoiding some of the more common schemes, so criminals have begun to change their tactics. An attack dubbed "spear phishing" has become more prevalent. Spear phishing, according to The APWG, is a targeted attack on a certain individual, group, or organization. The phisher sends an email disguised to look like it came from within an organization, for example from the Human Resources department or the local area network (LAN) manager. Users are much more likely to open an email (and its attachments) if it appears it came from within. The message will often have an attachment, disguised, for example, as a Microsoft ® PowerPoint presentation, and entices the user to open the file. However, the file is in reality crimeware (software created expressly to steal financial information [39]) created to infect the computer with a Trojan horse and open a backdoor into the system. Now the crooks have a route into the internal corporate network. The Department of Defense recently became a target of spear phishing attacks, prompting the Joint Task Force-Global Network Operations to give special attention to educating DOD employees. According to a Federal Computer Week article quoting a source at the Joint Task Force-Global Network, "Attempts have been made against all ranks in all services in all geographic locations. DOD civilians and military contractors have also been hit by spear phishing attacks."

Vishing

Traditional web-based phishing attacks are now evolving into sophisticated phone scams [33]. Voice Over Internet Protocol (VoIP) is becoming a popular alternative to traditional phone lines. Phishers use these VoIP numbers, available through retailers such as Skype™ or Vonage™, to setup a war dialer (software to sequentially dial phone numbers) to call numbers within a specific region [33]. When a person answers, they are "alerted" to some type of fraudulent activity on their credit card account or that their bank account has been compromised. They are directed to call a phone number to confirm personal data. The phone number is in fact attached to the VoIP account of the scammer. You can guess the rest.

Botnets

Botnets have become a major security issue in the last few years. According to Trend Micro, botnets—networks of compromised machines infected with malicious programs—have been identified as a leading cause of phishing [35]. Some botnets can contain hundreds or even thousands of machines—colloquially called "zombies". These networks are used to send spam, primarily, though they can be used for other criminal purposes. In June 2006, botnets sent an estimated 80% of e-mail spam, an increase of 30% from 2005 [35].

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Pharming

Though not a phishing attack per se, pharming is used by the same criminals to redirect web users from legitimate commercial web sites to malicious sites, which can then be used to elicit information for identity theft. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning. This technique is not new; however, the proliferation of online banking and commerce makes it attractive to phishers.

The "Phishing Kit"

RSA Security has recently discovered what they are calling a "Universal Man-in-the-Middle Phishing Kit". According to an article on the Dark Reading Room web site, "this is an all-in-one package that provides the raw materials to launch sophisticated phishing exploits that appear to be operating on legitimate web sites. The kit lets buyers create man-in-the-middle attacks, in which the victims communicate with a legitimate web site via a fraudulent URL set up by the fraudster. This allows them to capture victims' personal information in real-time." [29] A user must still be duped into clicking a URL, but they are interacting with the legitimate site (e.g., their bank's web site), yet using the fake URL, allowing the attacker to intercept ***any*** personal information entered by the user…in real-time! The kit also allows the attacker to impersonate multiple sites, without configuring or buying another kit. This is considered "next generation" phishing technology, but it's expected to proliferate in the next year, according to Marc Gaffan, director of marketing for consumer solutions at RSA [29].

Instant Messaging and Social Networks

Phishers also use instant messaging (IM) technology and social communities such as MySpace™ for phishing scams. In the IM attack, users receive an IM message that often appears to be coming from a buddy-list contact [34]. The victim is lured into clicking a URL and, as in other phishing scams, is directed to a fraudulent web site. Fake MySpace login pages are also created to capture user's email and passwords, allowing the account to be compromised and used to spam other accounts. In addition, IM and social networks are often mediums for crimeware or malware.

6 - WHAT CAN BE DONE?

Many experts contend that phishing is less of a "technology problem" and more of a "user problem"; that the responsibility ultimately lies with the user being aware of where they are browsing, what information they are giving over the Internet, and to whom they are giving the information. Others are more concerned that the sophisticated techniques used by phishers are becoming more difficult to detect, even for experienced computer users; casual or less-technical users are much less likely to be able to discern a legitimate e-mail, web address, or web site from a fake one. Social engineering ploys can be very effective in these situations.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Education

Education is a vital component of the phishing battle—as well as other online scams. The Federal Trade Commission suggests some things to remember:

(paraphrased from http://www.ftc.gov/bcp/conline/pubs/ alerts/phishregsalrt.htm)

- Don't reply to e-mails asking to confirm account information. Call or logon to the company's web site to confirm that the e-mail is legitimate.
- Don't e-mail personal information. When submitting information via a web site, make sure the security lock is displayed in the browser.
- Review credit card and bank account statements for suspicious activity
- Report suspicious activity

The Department of Justice recommends that users Stop, Look, and Call [26]:

(paraphrased from http://www.antiphishing.org/doj_special_report_on_phishing_ mar04.pdf)

- Stop: Don't react to phisher ploys of "upsetting" or "exciting" information
- Look: Look closely at the claims in the e-mail. Also look at the links and web addresses
- Call: Call or e-mail the company in question to verify if the e-mail is legitimate

Computer users should make an effort to keep abreast of computer security issues in the news, and use common sense when giving information anywhere: online or otherwise. If an e-mail (or phone solicitor or web site, etc., etc.) asks for personal information, that should be an immediate red flag that something may not be legitimate and needs to be confirmed. Legitimate companies will generally not solicit personal information via e-mail. If personal information is requested via a web site, the user should make certain he or she is connected to the proper site and that the communications are encrypted.

Technology

Unfortunately, phishing usually involves social engineering tricks, and, thus, even the best defenses that a company might have in place to combat outside threats are sometimes useless against these types of attacks. Although education is likely the best defense against phishing scams, there are technologies that make phishing harder to accomplish. When implemented with a defense-in-depth approach, software and hardware can be installed to slow the phishers down.

- *Two-factor Authentication*

  One of the more promising technologies to thwart phishing schemes involves two-factor authentication. This method uses a layered approach to validate a user's

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

credentials by using two separate methods to verify a user. A two-factor authentication technique currently being offered uses one-time passwords that expire after a single use. These passwords are generated using a shared electronic key between the user and a bank. A login is authenticated by not only the user's credentials (username/one-time password), but also the key that generates the password. If a password does happen to get stolen, it will not matter since it expires after a single use.

- *Firewalls*

  There are e-mail firewall products that implement rules to block spam and phishing scams at the perimeter. These products offer "heuristic" rules that are updated as new phishing schemes are found. They not only block the spam, they verify the IP numbers and web addresses of the e-mail source and compare them to known phishing sites. For larger organizations, this can be an effective defense against spam and phishing.

- *Anti-virus Technology*

  Though phishing scams are usually not considered a "viral" problem, if a user is infected with a worm that, in turn, installs a Trojan horse that can capture personal data, then anti-virus technologies are effective. Security best-practices direct that all users should implement an anti-virus product regardless of whether they are concerned about phishing or online fraud.

- *Browser Enhancements*

  Recent versions of Microsoft Internet Explorer, Mozilla Firefox, Netscape, and Opera offer new security features aimed at controlling phishing attacks and other online fraud. Using databases of known phishing sites, the browsers can look up a site and let the user know of the danger. These features are certainly a step in the right direction, thought they are not 100% accurate. Microsoft and the Mozilla Foundation have been at odds as to how accurate each of their respective anti-phishing technologies is [37]. If history is any indication, the phishers will most certainly try and find ways to defeat the browsers. Time will be the judge as to how effective these new browser technologies are.

- *Digital Certificates*

  Security begins with establishing trust between a user and a web site. Digital certificates are a way to establish this trust in the form of an encrypted digital key system. A public and private key structure is established whereby a company has a private key, obtained from a Certificate Authority (CA), and a user who wishes to make

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

secure transactions obtains the corresponding public key from the company. When the user logs into the company's server, the keys have to match or the transaction will not be processed. The problem with this method is that the private keys could be stolen if not kept completely secure. If the private key is compromised, then a hacker could use the digital key to masquerade as the key's owner.

- *Secure E-mail Protocols*

  There is a push within the industry to modify the existing e-mail transport protocols and include built-in security at this lower level. Validating the identity of the originating sender of a message would go a long way in preventing phishing attacks. There are encryption methods for sending e-mail, but many believe they are difficult for the average user to implement. Built-in encryption may eliminate the need for using separate encryption methods, allowing transparent authentication for the user. It would also eliminate the possibility of keys being stolen or hacked, thus allowing an attacker to decrypt secure messages. Several companies are working on this, but it may be years before something is available.

- *Communication*

  Companies need to communicate with their customers to keep them apprised of scams or other threats. They should make policies clear and make sure the customers are aware of how information will be gathered and disseminated.

- *Phish Feeding*

  John Brozycki, in a presentation for The SANS™ Technology Institute, describes a technique called Phish Feeding. This approach uses an automated "attack" to feed phishing sites bad data, attempting to make the phisher's scam less profitable, and more frustrating. According to Mr. Brozycki's presentation, this technique "reduces the value of the data the phishers plan to sell", "provides fake values that the targeted institution may be able to monitor", "frustrates the phishers", possibly making them "move on to easier targets", and "creates a reputation of being difficult to phish", therefore lowering your odds of being a target in the future [42]. Mr. Brozycki discusses this very interesting topic in a presentation available at the SANS™ website:

  http://www.sans.edu/resources/student_presentations/PhishFeeding.pdf

- *Defense-in-Depth*

  To be secure, a defense-in-depth approach must be put in place. Users and

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

companies need to be educated about the scams and risks, authentication methods need to be employed, firewalls should be in use, anti-virus technologies should always be installed, browser-based anti-phishing technologies should be considered, companies should communicate with their customers, and digital certificates and other encryption schemes should be implemented. When these layers of protection are utilized, the chance of a phishing attacks being successful is greatly reduced.

Litigation

Several states, including Arkansas, California, New York, Utah, and Virginia have anti-phishing laws [38]. These laws, many of which are based on the proposed (but, as of this writing, not enacted) federal Anti-Phishing Act of 2005, provide varying levels of punishment for criminals who are caught committing phishing fraud. The problem is, according to many security professionals, catching the crooks is difficult. It is very easy for them to hide their tracks, and many of the phishing sites are only operational for a few days or weeks before they are changed or moved. Though penalties have increased for phishing and other identity theft crimes, and prosecuting the offenders is paramount, it is my opinion that laws and litigation will not curb the phishing problem; only education and technology will be the ultimate solution.

Companies Need to be Prepared

Regardless of education or technology put in place, companies need to be prepared for the impacts of phishing and other online fraud attacks. Costs related to reissuing credit cards, re-establishing accounts, reimbursing customers for losses, and possible litigation, are just a sampling of expenses a company may have to absorb. These costs could be quite significant, particularly if hundreds of accounts are compromised.

Many experts suggest that companies need to have a disaster recovery plan in place to cover phishing attacks, similar to plans that cover any type of digital security breach or a natural disaster. Recovering from a large-scale phishing scam could, in theory, be detrimental to a company's revenue and to its customer's trust.

7 - CONCLUSION

Phishing scams can pose a significant threat to consumers and the companies they deal with. The number of online scams has increased significantly, and the techniques the criminals employ have become more and more sophisticated. These and other online cons show little sign of slowing. On the contrary, scams are on the rise, and companies and individuals need to be aware of the consequences.

There is no "magic bullet" or "pixie dust" that can make these threats go away. No single technology can keep fraudsters at bay and keep our personal information completely safe. There

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

are ways to make the crimes more difficult to accomplish, but a well-crafted phishing attack has a significant chance of being successful. There will have to be more done to stop the spread of these attacks and make them unprofitable and less appealing for the would-be phishers.

More research and development of anti-fraud technologies, more education of computer users, and aggressive prosecutions of the criminals who commit these crimes will go a long way to curb the threat, but these alone will most likely have little impact in the number of schemes.

Consumers need to become more educated concerning online threats and vulnerabilities. Companies need to make sure that online fraud and scams are reported and that their customers are kept apprised of scams that may affect them. The security community needs to work to find new ways to make e-mail and online commerce as bullet-proof as it can possibly be. This is a monumental task, but there are a great number of extremely talented people with many brilliant ideas out there. If something is not done, the way we do business online will change, and almost certainly not for the better.

Further Information

Valuable information about phishing can be found at The SANS™ Technology Institute:

http://www.sans.edu/resources/leadershiplab/phishing.php

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

REFERENCES

1. The Anti-Phishing Working Group. "What is Phishing?" URL:http://www.antiphishing.org/ (March 2004)

2. The Anti-Phishing Working Group. "Origins of the Word Phishing." URL: http://www.antiphishing.org/word_phish.htm (March 2004)

3. Author Unknown. "How to Obscure any URL". PC-Help. January 2002. URL: http://www.pc-help.org/obscure.htm (March 2004)

4. Library of Spoof E-mail Hoax Scams and Fake Web Pages. MillersMiles. URL: http://www.millersmiles.co.uk/identitytheft/spoof-email-and-spoof-web-page-library.htm (April 2004)

5. Bright, Mat. "Spoof Email Phishing Scams and Fake Web Pages or Sites. Part 1". February 2004. URL: http://www.millersmiles.co.uk/identitytheft/gonephishing.htm (April 2004)

6. Bright, Mat. "Spoof Email Phishing Scams and Fake Web Pages or Sites. Part 2". February 2004. URL: http://www.millersmiles.co.uk/identitytheft/oah-2.htm (April 2004)

7. Bright, Mat. "Remember the Phone Phreaks?" February 2004. URL: http://www.millersmiles.co.uk/identitytheft/phishing.html (April 2004)

8. The Identity Theft Resource Center. Identity Theft Facts and Statistics. February 2004. URL: http://www.idtheftcenter.org/facts.shtml (April 2004)

9. Gelles, Jeff. "Consumer Watch: 'Phishing' Scams Continue to Bite". March 27, 2004. URL: http://www.philly.com/mld/philly/business/columnists /jeff_gelles/8288622.htm (April 2004)

10. Hurst, Pat. "Millions at Risk from Cyber 'Phishing' Gangs". February 29, 2004. URL: http://www.crime-research.org/news/29.02.2004/95 (April 2004)

11. Glenbrook Partners Consulting. "Phishing". Customer briefing. February 23, 2004. URL: http://www.paymentsnews.com/2004/02/phishing.html (April 2004)

12. Dvorak, John C. "Gone Phishing. Scams for Personal Information Are Getting Worse". April 15, 2004. URL: http://abcnews.go.com/sections/ scitech/ZDM/phishing_commentary_pcmag_040415.html (April 2004)

13. Postel, Jonathan B. "Simple Mail Transfer Protocol". RFC 821. August 1982. URL: http://www.ietf.org/rfc/rfc821.txt (April 2004)

14. Trinity Security Services. "Identity Thieves go PHISHING". January 31, 2004. URL: http://www.itsecurity.com/papers/trinity14.htm (April 2004)

15. Jack, Rodney. "Online Phishing Uses New Bait". April 6, 2004. URL: http://www.vnunet.com/News/1154101 (April 2004)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

16. Columbo, Jon. "Bugwatch: Foiling Phishers". April 7, 2004.
URL: http://www.vnunet.com/News/1154148 (April 2004)

17. Moulds, Richard. "Whose Site is it Anyway?". March 29, 2004.
URL: http://www.net-security.org/article.php?id=669 (April 2004)

18. Barrett, Jennifer. "Phishing Fallout". April 15, 2004.
URL: http://msnbc.msn.com/id/4741306/ (April 2004)

19. Gray, Patrick. "IE Bug Provides Phishing Tool". December 10, 2003.
URL: http://news.zdnet.co.uk/internet/security/0,39020375,39118421,00.htm (April 2004)

20. Gonsalves, Antone. "Latest Trojan Phishing for Personal Data". January 16, 2004. URL:
http://www.techweb.com/wire/story/TWB20040116S0007 (April 2004)

21. Lemos, Robert. "New Mimail Mixes Tricks for Paypal Scam". January 16, 2004. URL:
http://news.com.com/2100-7349-5142647.html (April 2004)

22. Festa, Paul. "IE Bug Lets Fake Sites Look Real". December 10, 2003.
URL: http://news.com.com/2100-7355-5119440.html?tag=nl (April 2004)

23. Secunia Advisories. Internet Explorer URL Spoofing Vulnerability. February 2, 2004 (Last update) URL: http://secunia.com/advisories/10395/ (April 2004)

24. Author Unknown. "Phishing Tackle". January 12, 2003.
URL:http://www.cbronline.com/cbr_archive/538daca4f949786480256e
12004a1d48 (April 2004)

25. Author unknown. "Huge Surge in Phishing Scams As Fraudsters Seek Financial Gain". April 21, 2004. URL: http://www.messagelabs.com/
news/virusnews/detail/default.asp?contentItemId=850&region=america (April 2004)

26. Criminal Division, Department of Justice. "Special Report on Phishing". March 2004. URL:
http://www.antiphishing.org/doj_special_report_
on_phishing_mar04.pdf (April 2004)

27. News Release. "Tumbleweed announces new release of email firewall to stop email phishing scams and improve anti-spam effectiveness". October 28, 2003. URL:
http://www.itsecurity.com/tecsnews/oct2003/oct277.htm (April 2004)

28. Federal Trade Commission Consumer Alert. "Is Someone 'Phishing' for Your Information?"
March 2004. URL: http://www.ftc.gov/bcp/conline/pubs/
alerts/phishregsalrt.htm (April 2004)

29. Wilson, Tim. "For Sale: Phishing Kit." Dark Reading Room. January 12, 2007.
URL:http://www.darkreading.com/document.asp?doc_id=114608&f_src=
darkreading_section_296 (January 2007)

30. Author unknown. "US CONSUMERS LOSE MORE THAN $8 BILLION TO ONLINE THREATS ACCORDING TO CONSUMER REPORTS SURVEY". Consumer Reports. September 2006.
URL: http://www.consumerreports.org/cro/cu-press-room/pressroom/2006/9/

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

0609_eng0609son_ov.htm?resultPageIndex=1&resultIndex=4&searchTerm=
phishing (January 2007).

31. McAfee, Inc. Whitepaper. “Identity Theft”. January 2007.
URL: http://www.mcafee.com/us/threat_center/white_paper.html (January 2007).

32. Brewin, Bob. “DOD battles spear phishing”. Federal Computer Week. December 2006. URL: http://www.fcw.com/article97186-12-26-06-Web&RSS=yes (January 2007)

33. Jaques, Robert. “Cyber-criminals switch to VoIP 'vishing'”. VNUNet article. July 2006. URL: http://www.vnunet.com/vnunet/news/2160004/cyber-criminals-talk-voip (January 2007).

34. Hicks, Mathew. “Phishing Dips into Yahoo IM.” Eweek. March 2005. URL: http://www.eweek.com/article2/0,1895,1779798,00.asp (January 2007)

35. Multiple authors. “Botnet Threats and Solutions”. TrendMicro. November 2006. http://www.antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf (January 2006)

36. McCue, Andy. “Hackers Nab $1 Million from Nordea Bank.” Business Week. January 2007. URL: http://www.businessweek.com/globalbiz/content/jan2007
/gb20070119_387969.htm?campaign_id=rss_daily

37. Lemos, Robert. “Microsoft, Mozilla compete on anti-phishing data”. SecurityFocus. November 2006. URL: http://www.securityfocus.com/brief/356?ref=rss (January 2007).

38. Greenemeir, Larry. “New From Cybercrooks: Fake Chrome, Pump-And-Dump”. InformationWeek. October 2006. (January 2006).

39. Wikipedia definition. “Crimeware”. http://en.wikipedia.org/wiki/Crimeware (January 2007).

40. Ramzan, Zulfikar. “Phishing and Cross-Site Scripting”. Symantec Security Response. July 2006. URL: http://www.symantec.com/enterprise/security_response/weblog/2006/07/
phishing_and_crosssite_scripti.html (January 2007).

41. SANS Institute Top-20 (2006 Annual Update). URL: http://www.sans.org/top20/ (January 2007).

42. Brozycki, John. “Phish Feeding: An Active Response to Phishing Campaigns”. The SANS Technology Institute presentation. October 2006.
URL: http://www.sans.edu/resources/student_presentations/PhishFeeding.pdf (January 2007).

43. SANS Security Essentials Training. December 2003.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**