Global Information Assurance Certification Paper

Something Phishy: How to Avoid Being Caught in the Net of Specialized Spam

GIAC Security Essentials Certification (GSEC) Practical Assignment
Option one, Information Security Research (Version 1.4b)

Karen Olk
March 8, 2005

Abstract

Spam, or unsolicited e-mail, has become an expansive and expensive problem for both the business and casual Internet user. Piles of unwanted e-mail, some 38% of the 31 billion e-mails sent, accumulate daily.[1] Receipt of these unwanted e-mails can come at a high cost of both time and finances.

A new breed of spam causing an increasing amount of cost and concern consists of "phishing" e-mails. Through seemingly legitimate correspondence, phishers disguise themselves as bona fide companies and surreptitiously attempt to lure recipients to bogus websites for the purpose of divulging personal information. A successful phishing attack will result in the user handing over enough personal information, such as a Social Security Number, for the cyber-thief to steal their identity. Once an identity is stolen, it can be used to commit any number of crimes, including emptying the pockets and destroying the credit rating of the victim. The victims of a successful phishing attack can find themselves in a precarious financial situation not of their own making and with little recourse or remedy.

This paper describes the history of phishing scams, its potential consequences, and guidelines by which Internet users may best situate themselves and reduce the likelihood of their vulnerabilities being exploited.

Introduction

Despite the message in the seemingly legitimate e-mail received, the user was sure there couldn't be anything wrong with their CitiBank account. The e-mail warned that if the recipient did not update the account "immediately", said account was in jeopardy of being deactivated. "Deactivated!" thought the user, "Well, that can't be good". All the user had to do, the e-mail instructed, was click on the provided link and enter their Social Security and credit card numbers in the space provided. The instructions seemed simple enough, and CitiBank appeared genuinely concerned about their ongoing relationship. An e-mail of this nature, complete with the full-color CitiBank logo and "support@ CitiBank.com" return e-mail address, might not have aroused suspicion, had the user actually ever owned a CitiBank account of any kind.

The scam is called phishing and just as malicious telemarketers fish for information via telephone and (all-too-often successfully) coax people out of their bank account numbers, credit card numbers, passwords, and any other useful personal tidbit to aid in identity theft, today's scam artists increasingly use spam (unsolicited commercial e-mails) and fake Web pages as a means to this malevolent end.

With the combination of spam and bogus websites as bait, cyber thieves cast a

wide net and “fish” for victims willing to reveal their personal information. Phishers are scam artists who send out thousands of forged e-mail messages at a time, often disguised as legitimate messages from a large, well-known, institution.

The “ph” spelling is something of a terminology tradition amongst hackers, dating back to the 1970’s when hackers would break into the US telephone system to make free calls; an activity widely referred to as “phone phreaking”. [2]

The Federal Trade Commission reports it received 215,000 complaints of identity theft last year. That's an increase of 33 percent from the previous year. The commission says identify theft is the number-one reported scam. And those are just the complaints made to the FTC. Experts say millions of people are victims of identity theft each year, and the numbers continue to rise. [3]

While surely not all malicious telemarketers have hung up their hats, spam was widely considered one of the greatest destructive forces of the Internet in 2004. An increasing amount of spam includes phishing expeditions and attacks. According to the Anti-Phishing Working Group (AWPG), reported e-mail fraud and phishing attacks increased by over 4,000% last year alone.

The Second Conference on E-mail and Anti-Spam suggests that “as e-mail has grown from a tool used by a few academics on the Arpanet to a ubiquitous communications tool, it has evolved from a piece of simple, plain text in an inbox into a rich graphical medium that can be viewed, sorted, signed, encrypted, shared, archived, searched, prioritized, etc. Spam, following the growth of e-mail, has changed from a minor curiosity, to a nuisance, to a multi-billion dollar problem.” [4]

Below, figure 1 demonstrates the proliferation of phishing attacks and the associated costs:

Figure 1

Increase in phishing attacks, December to June:	**1,126%**
Estimated number of people who received phishing e-mails in the past year:	**57 million**
Recipients who opened a phishing e-mail:	**19%**
Recipients who divulge personal or financial information to phishers:	**3% to 5%**
People who are duped into acting on a phishing e-mail that was identified as probably fraudulent:	**1 in 10**
Phishing attacks using spoofed e-mails:	**92%**
Amount lost in fraud April 2003-2004:	**$11.7 billion**
SOURCES: Anti-Phishing Working Group, Gartner, Mailfrontier, Sunbelt Software[5]	

"If you think of phishers initially as petty thieves, now they're more like an organized crime unit," said Paris Trudeau, senior product manager for Internet-

security firm SurfControl. [6]

The Anti-Phishing Working Group (APWG), a coalition of banks and technology companies, claims to be "the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing and e-mail spoofing of all types". [7] Membership driven AWPG is sponsored by a plethora of dedicated defenders of security, including VeriSign, SAIC, McAfee, Symantec, and Microsoft. A few minutes regularly spent at http://www.antiphishing.org checking up on the latest permutations of the phishing epidemic have the potential to save even the most astute security professional unnecessary headaches.

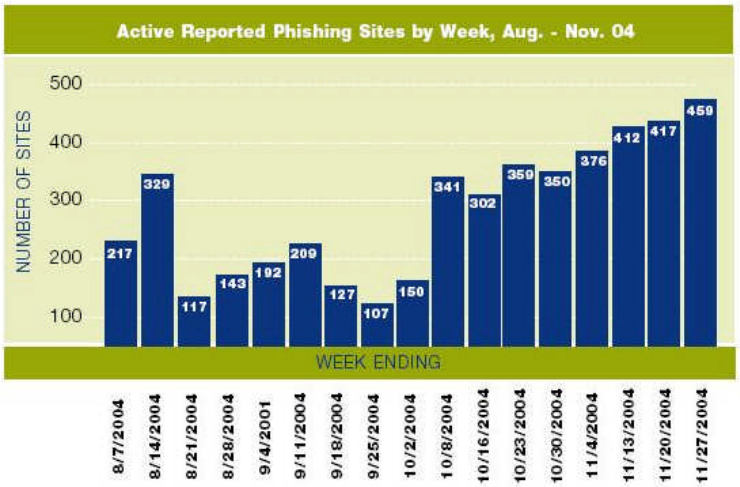
According to the Anti-Phishing Working Group, "by hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to [respond to attacks]."

The APWG identified 8,459 new and unique phishing e-mail messages in November 2004, nearly four times the number reported in August 2004 (see figure 2).

Figure 2

Phishing Sites Reported by Anti-Phishing Work Group: Aug-Nov 2004

SOURCE: Anti-Phishing Work Group



8

Popular recent phishing expeditions include attacks in the form of seemingly innocuous e-mails from eBay, VISA, AOL, Citizens, U.S. Bank, and KeyBank. Especially insidious phishing e-mails may use a variety of techniques to create the most dangerous kind of scam; the *successful* attack. A lethal combination of non-threatening persuasion from a spoofed sender and a 'masked' link delivers a highly convincing one-two punch. Any information gathered can be used by malicious phishers to generate a highly personalized attack.

Aside from the annoyance, the incredible amount of e-mail traffic generated by these phishers can cause many headaches; from bogging down networks and clogging e-mail servers (causing expensive downtime), to compromising the

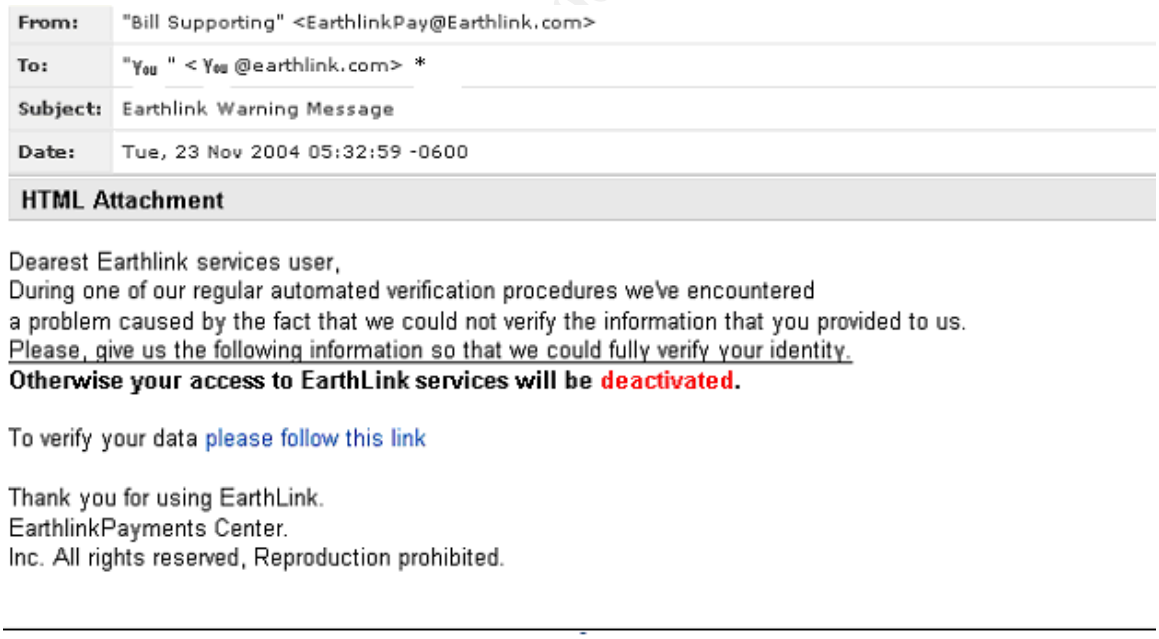
security of both corporate networks and Internet Service Providers (ISP's).

The inherent danger phishing attacks pose to the user is that once an identity is stolen or damaged, it can take years of paperwork and legal fees to clear one's credit history. In the meantime, victims find themselves with severely limited purchasing power, unable to buy cars, houses, or other high-ticket items. Identity theft victims often find they qualify only for poor loan rates, if any at all, and their economic hands are tied. Once passwords and other personal information have been obtained through what looks like a legitimate Web site, bank accounts can be emptied, identities stolen, and credit abducted, often without detection.

"A lot of drug lords are getting into phishing," says Avivah Litan, a vice president and research director at (researcher) Gartner. "It's easier and more lucrative than selling cocaine." [9]

Sometimes containing misspellings, poor grammar, and attempts at personalization, below are representations of typical phishing attacks (see figure 3, below)*:

Figure 3



From:	"Bill Supporting" <EarthlinkPay@Earthlink.com>
To:	"You " < You @earthlink.com> *
Subject:	Earthlink Warning Message
Date:	Tue, 23 Nov 2004 05:32:59 -0600

HTML Attachment

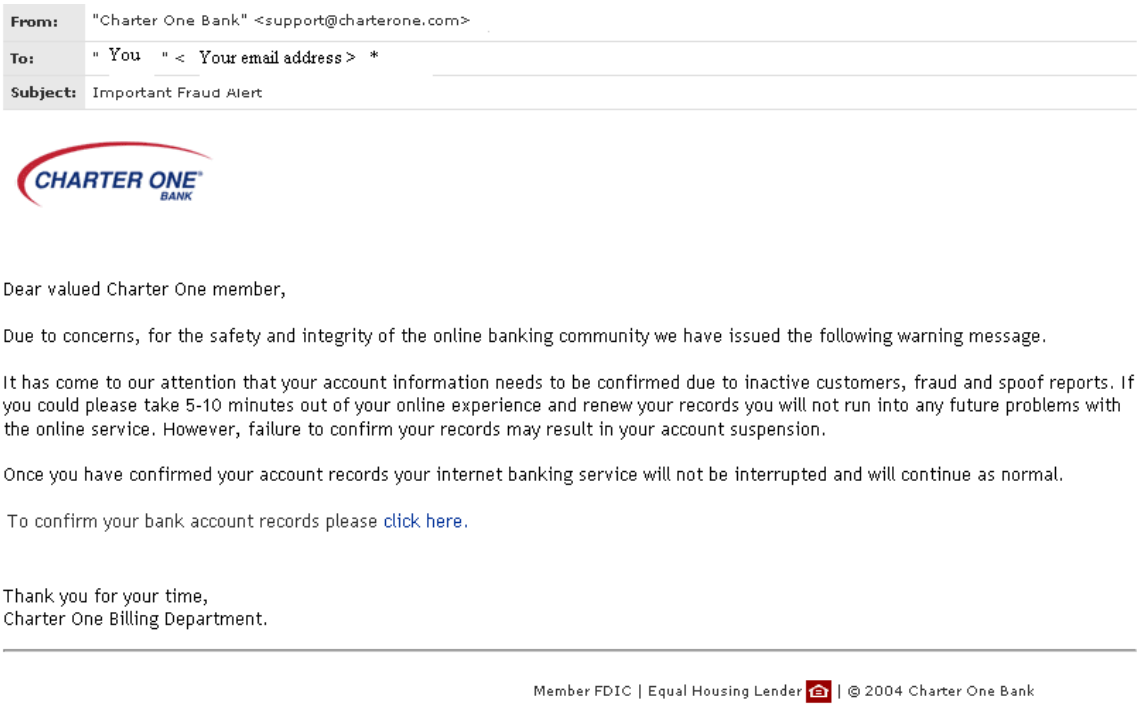
Dearest Earthlink services user,
During one of our regular automated verification procedures we've encountered
a problem caused by the fact that we could not verify the information that you provided to us.
Please, give us the following information so that we could fully verify your identity.
Otherwise your access to EarthLink services will be deactivated.

To verify your data please follow this link

Thank you for using EarthLink.
EarthlinkPayments Center.
Inc. All rights reserved, Reproduction prohibited.

Insertion of company logos and official-looking footer information can assist in the illusion of legitimacy, thereby further encouraging users to click on a malicious link. The following example (figure 4) demonstrates another phishing e-mail:

Figure 4



From: "Charter One Bank" <support@charterone.com>
To: " You " < Your email address > *
Subject: Important Fraud Alert

CHARTER ONE BANK

Dear valued Charter One member,

Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message.

It has come to our attention that your account information needs to be confirmed due to inactive customers, fraud and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.

Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.

To confirm your bank account records please click here.

Thank you for your time,
Charter One Billing Department.

Member FDIC | Equal Housing Lender | © 2004 Charter One Bank

**Note*: *All identifying information has been altered.*

According to PCWorld, as many as 20 percent of people who receive this type of spam not only click the link in the message, but enter their personal information as well. [10]

The number of online financial scams grew dramatically in the fall of 2004, driven in part by the proliferation of dynamic phishing ploys. In addition, online fraud forums and phishing software can assist phishers by automating the design and deployment of their scams. Online forums provide hubs of illegal activity where personal identifying information is traded, sold, and bartered by phishers.

Phishing e-mails and WebPages can contain viruses (or "spyware") with keystroke loggers that capture customers' online banking passwords. This particular scam, which uses both a spoofed site and malware/spyware to redirect users to fraudulent sites, is known as "pharming". [11]

Would-be thieves emulating AOL or Citibank have been known to register plausible-looking "cousin" domains like aolaccountupdate.com or mycitibank.net. E-mail links then send customers to these "cousin" pages which display the logo of the company to aid legitimacy. Phishers can even direct recipients to a well-known company's real website, but then collect their personal data through a faux pop-up window that ships it to a server overseas. Online identity theft, which requires little skill or capital, can be, and is, perpetrated from around the world. [12]

Defending Against Attacks

As a rule, personal information should never be distributed over the Internet. However, due to the proliferation of online banking, bill payment options, and a new world of online purchasing opportunities, some of the luster and rigidity has been removed from this golden rule. Users opting to participate in online transactions containing sensitive information must understand that there is no such thing as a 100% secure transaction. For the sake of convenience, users must be willing to accept some risk.

As General Benjamin W. Childlaw stated in 1954, "Simply put, it is possible to have convenience if you want to tolerate insecurity, but if you want security, you must be prepared for inconvenience".[13]

Without the ability to verify the sender, all e-mail is potential spam and the value of every e-mail is compromised. Ensuring that people are who they claim to be is central to enhancing public safety and improving commerce.

In 1996, The National Institute of Standards and Testing (NIST) published their Federal Information Processing Standards Publication 186 (FIPS 186) which established the Digital Signature Standard (DSS). [14]

A digital signature confirms that an e-mail message, macro, or program originated from the trusted source that signed it while assuring that the message, macro, or program has not been altered.[15] S/MIME, Secure Multipurpose Internet Mail Extensions is a method of security that allows users to exchange encrypted and digitally signed messages with any S/MIME–compliant mail reader (which includes such vendors as ConnectSoft, Frontier, FTP Software, Qualcomm, Microsoft, Lotus, Wollongong, Banyan, NCD, SecureWare, VeriSign, Netscape, and Novell). An S/MIME digital signature allows an e-mail recipient to verify the authenticity of a "from" address. S/MIME messages are encrypted or digitally signed by the sending client and decrypted by the recipient. [16]

It isn't always easy to identify phishing ploys. If ever in doubt about an e-mail, recipients should call the provider in question to verify authenticity. Increasingly, suspicious e-mails can be reported via e-mail or over the phone to the fraud departments at frequently targeted companies.

The AWPG has compiled a list of recommendations to help avoid becoming a victim of phishing scams. This list consists of the following general rules:

1) Be suspicious of any e-mail with urgent requests for personal information.

2) Don't be fooled by e-mails with upsetting or exciting statements that

encourage you to react immediately.

3) Don't use the links within an e-mail to get to a webpage. (For example, instead of clicking on www.PayPal.com in an e-mail, manually type the address into your browser. Doing so will protect you from seemingly legitimate links that actually redirect you to bogus sites).

4) Don't fill out any forms in e-mail messages that request personal financial information.

5) Communicate information such as credit card numbers only via a secure website or the telephone. To make sure you're on a secure Web server, check the beginning of the Uniform Resource Locators (URL) in your browser address bar. It should be "https" rather than "http". The "s" signifies a secure connection.

6) Consider installing a Web browser toolbar such as EarthLink's ScamBlocker or Cloudmark's SafetyBar to alert you before you visit known phishing/fraud websites.

7) If an e-mail message is not personalized, assume it's not a valid message.

8) Log in to your online accounts regularly, and check bank, credit, and debit card statements to ensure that all transactions are legitimate.

9) Ensure that your operating system and browser is up-to-date and security patches have been applied.[17]

APWG suggests that users forward the entire phishing attempt, including all headers, to the APWG (reportphishing@antiphishing.com) and the Federal Trade Commission (spam@uce.gov). It is also recommended that a complaint be filed at the Internet Fraud Complaint Center of the FBI, via their website, www.ifccfbi.gov. Such actions help track the proliferation of both known and developing phishing scams and assist in the overall security and sanitation of the Internet.

The US Department of Justice also offers generalized tips for avoiding identity theft, both online and off. They suggest that all bank statements, credit card bills, and other correspondence containing sensitive personal information be shredded before being discarded. Also, obtaining an annual review of credit reports (from Equifax, Experian, and/or TRW) is good practice to help determine the existence of any fraudulent accounts. It is also recommended that you keep the amount of personal information in your wallet or purse to an absolute minimum and withhold your Social Security Number whenever possible.

The US department of Justice warns Americans to be extremely cautious when divulging their Social Security Numbers, as the rise in identity fraud can likely be linked to relying on Social Security Numbers as a means of identification. [18]

If you have been a victim of a successful phishing attack, the APWG suggests reporting the theft of your information to your bank, credit card issuer, and/or proprietary service (i.e., eBay) immediately. To protect your credit rating, be sure to report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation. Request that they place a fraud alert and a victim's statement in your file and request a (free) copy of your credit report to check whether any accounts were opened without your consent. Also request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft. Time is of the essence as your liability under federal law for unauthorized use of your accounts may depend on how quickly you report the loss. Many companies have toll-free 24 hour phone lines to handle exactly this type of emergency.[19]

Phishing software

While companies develop safeguards to protect their clients (such as ISP's filtering of e-mails) fighting phishing on a browser level is becoming an important basic layer of defense.

Browser updates and patches are constantly in the works to prevent exploitation, but often the most immediate action one can take is merely to remain aware of susceptibilities. For example, a known vulnerability in Mozilla could be exploited by phishers (the flaw is due to the fact that the dialog box incorrectly displays long sub-domains and paths)[20]. The flaw is known to affect Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows and Mozilla Firefox 1.0, but could affect other versions as well. [21]

Thanks to a known Microsoft Internet Explorer issue, phishers can make legitimate-looking sites appear in the IE status, address, and title bars. It took Microsoft over one month to create a patch for this flaw. [22]

Microsoft suggests the following steps to help hinder the progress of phishers: [23]

1. Install the MS04-004 Cumulative Security Update for Internet Explorer (832894). The Internet Explorer security patch can be downloaded by visiting: http://support.microsoft.com/?id=833786.
2. Verify that there is a lock icon in the lower right Status bar. This lock icon confirms the name of the server providing the viewed page.
3. To identify the actual URL of a Web page, Microsoft suggests using a JScript command in Internet Explorer. To do so, type the following command, in its entirety, into the address bar and then press enter:

   javascript:alert("Actual URL address: " + location.protocol + "//" + location.hostname + "/");

The JScript message box will indicate the actual URL Web address for the Web site that you are visiting. By running this script, you will be provided the full URL for any hyperlink. Microsoft suggests users be wary of any address containing the characters %00, %01, and/or @.

In order to limit the damage inflicted by a successful phishing attack via spoofed website or malicious hyperlink, other actions Microsoft suggests include reading e-mails in text versions only and setting your Internet zone security level to "High" in Internet Explorer. These remedies have the unfortunate side-effect of also limiting e-mail, scripts, ActiveX Controls, and other content.

In lieu of improvements to the browsers themselves, some organizations have taken drastic steps in trying to solve the malicious spam problem in-house. For example, MasterCard International is making efforts to track down culprits and shut down Web sites that pose as their own, and on January 5, 2005, eBay launched a private mail service for all of its users, specifically to help protect them from phishing scams. The eBay mail service provides each user with a personalized in-box. Found under the new heading of "My Messages", eBay and eBay alone can use these private mailboxes to correspond with their users. [24]

eBay, the number one holiday online shopping site with nearly fifty million users last season, also depends heavily upon educating its community to recognize phishing scams, according to spokesman Hani Durzy. [25]

eBay is one amongst many businesses that cater to online consumers and who are taking note and developing plans. "If a consumer doesn't trust e-mail at all, then it inhibits our ability to communicate with them," said Kurt Van Etten, the auction giant's security program director. "And if they're not comfortable using credit cards online, then that will affect our business. For us, this is a trust issue."[26]

Another line of defense is the spam and/or phish blocking application. For example, Internet provider EarthLink offers a downloadable toolbar (www.earthlink.net/home/software/toolbar) which is available to all Internet users. EarthLink's "ScamBlocker" checks browser entries against a growing list of known scam sites. Once the application is installed, every time a user browses the Internet an icon appears indicating whether each site has been deemed

"safe"  or "neutral"  . This user-friendly tool helps simplify computer security for the masses, regardless of skill-level.

Clicking on either icon will produce a pop-up window offering further explanation. A site is deemed "safe" when it meets ScamBlocker's safety standards. This rating is determined based upon who owns the webpage and where they are located. The analysis pop-up provides the organization name and their specific geographic location.

A site earns a "neutral" rating when the application cannot guarantee that the site is safe, yet it has found no specific indication of fraud. Oftentimes in this case, the geographical location and/or the owning organization cannot be determined and therefore is not displayed in the analysis pop-up.

When a ScamBlocker user requests the site of a known scammer, they will be immediately redirected by the tool and receive the following warning, complete with flashing, attention-grabbing text (see Figure 5):

Figure 5

e goes on to explain what has happened and why the user has been redirected. It succinctly informs users about malicious sites and the potential repercussions of accessing the particular site they are seeking. Users will be alerted before entering a known scammer's territory, and strongly encouraged to cease and desist at this point. However, if they still wish to proceed, they are given the option to do so (see Figure 6):

Figure 6

While EarthLink's visual safety rating icon can be an effective way to alert users of a dangerous situation when they have otherwise grown increasingly desensitized to pop-up security warnings, it is not a universal solution to the problem of phishing. For example, the EarthLink Scam Blocker requires use of Internet Explorer v.6 and is not compatible with browsers that are considered generally more secure, such as Netscape, Safari, and Mozilla Firefox.

Cloudmark Gateway Solutions Immunity and Authority provides a "SafetyBar", also for Internet Explorer. The Cloudmark "SafetyBar" is currently in development with anticipated full release scheduled for March 2005. This anti-phishing application operates similarly to the EarthLink tool, and provides real-time information from over one million users, in 153 countries, to assist in the designation of "good" (safe), "Unknown", or "Unsafe" URL's. SafetyBar is free, and the beta version can be downloaded by visiting:

http://www.cloudmark.com/iebeta.

In the meantime, many other proprietary anti-spam and anti-phishing tools have been propagated, including SunBelt Software's iHateSpam for Exchange V1.6, which boasts a robust engine specifically designed to target phishing attacks.[27] While remaining transparent to the user, the iHateSpam tool uses a real-time feed and near-constant updates (of known phishing sites, e-mails, and even phone numbers) to catch phishing e-mails and automatically quarantine them.

Just as many spyware "removers" contain spyware themselves, e-mails claiming to "secure" your accounts can actually be phishing scams. An example follows as Figure 7:

Figure 7

Phishing e-mails are evolving and becoming more and more clever and therefore more and more dangerous. In the e-mail above, a warning about phishing is an attack in and of itself. Even the most security conscious user may be enticed by this breed of attack, not noticing that the provided link re-directs them to an information collection farm.

The EarthLink ScamBlocker tool gave the link above (http://www.myaccount.earthlink.net) a big green thumbs up icon, but both Internet Explorer and Mozilla Firefox alerted to potential hazards of proceeding based on compromised authenticity of the site's security certificate. Internet Explorer produced the following pop-up window:

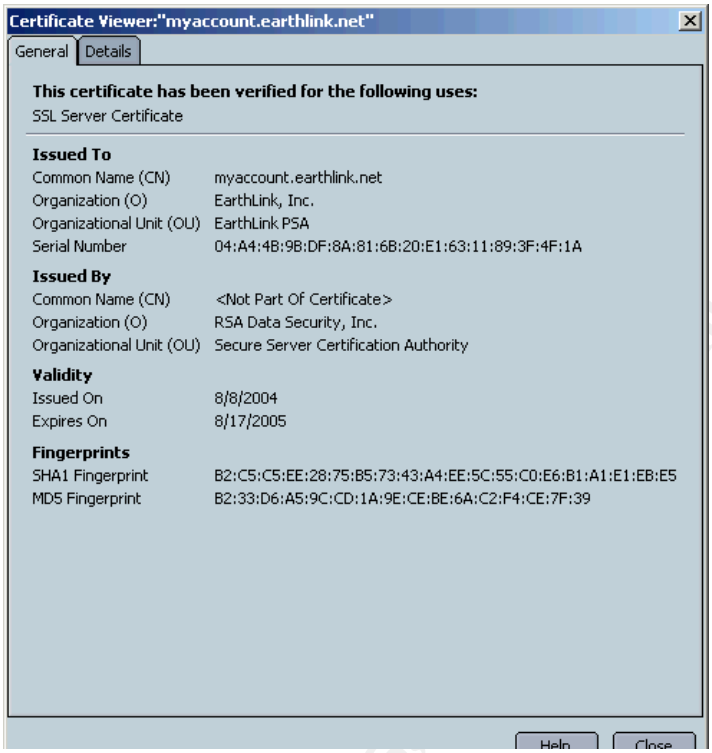
Figure 8

While Mozilla Firefox offered the following pop-up:

Figure 9

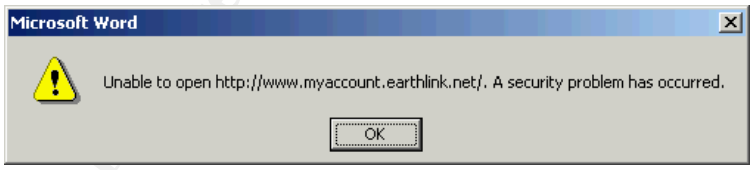
Clicking on the “View Certificate” button produces the following:

Figure 10



Even Microsoft Word recognizes a “security problem” when the http://myaccount.earthlink.net link is clicked from within this very document. Microsoft Word provides a pop-up indication that progress has been halted, but no further information:

Figure 11



Unfortunately, the users most likely to fall for the usual phishing techniques are often the least likely to seek out and/or install any tools to prevent successful phishing ploys. Their best defense against scams of many varieties might be to ensure correct implementation of their firewalls, including updated hardware and firmware. Properly administered hardware provides another essential layer of safety. To ensure that hardware is up to date, a list of update sites for the more popular vendors is provided below:

- Linksys: http://www.w2knews.com/rd/rd.cfm?id=050117TB-Linksys
- Netgear: http://www.w2knews.com/rd/rd.cfm?id=050117TB-Netgear
- Dlink: http://www.w2knews.com/rd/rd.cfm?id=050117TB-DLink
- Belkin: http://www.w2knews.com/rd/rd.cfm?id=050117TB-Belkin

Regulatory Highlights

The “Controlling the Assault of Non-Solicited Pornography and Marketing”, or CAN-SPAM Act, was signed by the President on December 16, 2003 and went into effect in the United States on January 1, 2004. This anti-spam act requires unsolicited commercial e-mail senders to identify themselves clearly and accurately in the "from" line of any e-mails, include subject line text consistent with message content, provide a valid postal address, and contain an opt-out mechanism. [28]

According to a spam sample analyzed by MX Logic, an e-mail security solutions developer, as of July of 2004, an average of only 0.54 percent of spam was in compliance with the legislation. [29]

While the CAN-SPAM Act of 2004 did not demonstrate any significant impact in decreasing spam, Microsoft, America Online, Earthlink, and Yahoo! Filed the first major industry lawsuits under the CAN-SPAM act in March 2004. The lawsuits named hundreds of defendants, with more than 90 percent of them identified only as “John Doe.” As of the first anniversary of Britain’s Privacy and Electronic Communications Regulations (December 2003) aimed at stopping unsolicited e-mail, not a single offender has been prosecuted. [30]

On July 15, 2004, President Bush signed a bill into law that toughens penalties for identity thieves. Known as the Identity Theft Penalty Enhancement Act, or ITPEA, the measure sets up punishment guidelines for anyone who possesses someone else's identification-related information with intent to commit a crime.

The ITPEA says that anyone who, while engaged in any of a long list of crimes, knowingly "transfers, possesses, or uses, without lawful authority" someone else's identification will be sentenced to an extra prison term of two years with no possibility of probation. An automatic five years of prison will be awarded any identity thief who commits “major crimes associated with terrorism”, such as aircraft destruction, arson, airport violence, or kidnapping of top government officials. In addition, ITPEA rewrites another section of the law, making mere possession of "identification of another person with the intent to commit, or to aid or abet a crime” illegal. [31]

Conclusion

With phishing, as with any other scam, your best defense is a good offense. Since users have a limited scope of accessibility to the perpetrators of phishing attacks, and limited legal recourse, following as many of the preceding tips as feasible will help limit your vulnerability.

Remember to be wary of generalized e-mails and personalized e-mails calling you to immediate action; especially those from major corporations, Internet

providers, credit card companies, and banks. Rarely would any of these organizations legitimately find the need to contact clients personally via e-mail, and they would never request that personal information, specifically Social Security Numbers, be transferred electronically via mass e-mailing. Just about anyone could send an e-mail asking for information; it is the responsibility of the individual to protect him or herself by not divulging personal information unnecessarily, especially one's Social Security Number.

Social engineering and end-user imprudence are often the most serious security flaws a computer system can suffer. Be proactive and be aware. Make use of all available layers of protection, from hardware and software updates, to spam and scam blocking tools.

In order to effectively fight the scammers, both education and legislation are required. A combined package of awareness, cynicism, and vigilance often provides the best protection. Check the APWG website regularly to stay abreast of current known scams.

The only way to ensure that your computer is absolutely protected against Internet scams is to unplug it. Permanently. Barring that solution, each user is responsible for protecting himself by remaining at least one stroke ahead of the big bad opportunistic fish as they swim amongst us in an expanding sea of technology.

© SANS Institute 2000 - 2005 Author retains full rights.

Works Cited

[1] ITFacts.biz - open database of IT market research, statistics, sales figures, analyst opinions and forecasts. Retrieved from: http://www.itfacts.biz/index.php?id=P1470

[2] Santos (2004). Phishing and the Threat to Corporate Networks. Retrieved from: http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf

[3] Brad Grimes (2004). Identity Theft Gets Phishy, How to Protect Yourself. Retrieved from: http://www.pcworld.com/news/article/0,aid,115140,00.asp

[4] Second Conference on E-mail and Anti-Spam (CEAS) (2005). Retrieved from: http://www.gupade.org/Eventos/350.aspx

[5] iHateSpam for Exchange (2005). Sunbelt Software. Retrieved from: http://www.sunbelt-software.com/product.cfm?id=931

[6] Phishing. CNN.com (2005). Retrieved from: http://www.cnn.com/2005/TECH/internet/01/20/tech.phishing.reut/index.html

[7] What is Phishing and Pharming? (2005) Anti Phishing Working Group. Retrieved from: http://www.antiphishing.org/

[8] Postini (2005). E-mail Security Annual Review and Threat Report. Retrieved from: http://www.postini.com/whitepapers/ThreatReport.pdf

[9] Alice Dragoon (2004). Foiling Phishing. Retrieved from: http://www.csoonline.com/read/100104/phish.html

[10] Brad Grimes (2004). Identity Theft Gets Phishy; How to Protect Yourself. Retrived from: http://www.pcworld.com/news/article/0,aid,115140,00.asp

[11] What is Phishing and Pharming? Anti Phishing Working Group (2005). Retrieved from: http://www.antiphishing.org/

[12] Alice Dragoon (2004). Foiling Phishing. Retrieved from: http://www.csoonline.com/read/100104/phish.html

[13] General Benjamin W. Chidlaw. December 12, 1954. Retrieved from: The Spy Museum, Washington D.C.

[14] Federal Information Processing Standards Publication (186) Digital Signature Standard (1994). Retrieved from: http://www.itl.nist.gov/fipspubs/fip186.htm

[15] Microsoft Office 2000 Glossary. Retrieved from: http://www.microsoft.com/resources/documentation/office/2000/all/reskit/en-

us/o2kglossary.mspx

[16] RSA Security. RSA Laboratories. 5.1.1 What is S/MIME? Retrieved from: http://www.rsasecurity.com/rsalabs/node.asp?id=2292

[17] Consumer Advice: How to Avoid Phishing Scams. Retrieved from: http://www.antiphishing.org/consumer_recs.html

[18] Declan McCullagh (2005). Season Over for Phishing? Retrieved from: http://news.com.com/Season+over+for+phishing/2100-1028_3-5270077.html

[19] Consumer Advice: What To Do If You've Given Out Your Personal Financial Information. Retrieved from: http://www.antiphishing.org/consumer_recs2.html

[20] Ingrid Marson (2005). Firefox Flaw Raises Phishing Fears. Retrieved from: http://asia.cnet.com/news/security/printfriendly.htm?AT=39212469-39037064t-39000005c

[21] John Layden (2005). The Register. Retrieved from: http://www.theregister.co.uk/2005/01/07/mozilla_flaws/print.html and Matthew Broersma (2005). Computer World. Retrieved from: http://www.computerworld.com/printthis/2005/0,4814,98757,00.html

[22] Brad Grimes (2004). Identity Theft Gets Phishy. Retrieved from: http://www.pcworld.com/news/article/0,aid,115140,00.asp

[23] Microsoft Help and Support. Retrieved from: http://support.microsoft.com/?id=833786

[24] Stephanie Olsen (2005). CNETNews. eBay Fights Back Against Phishers. Retrieved from: http://asia.cnet.com/news/security/0,39037064,39211930,00.htm

[25] Leslie Brooks Suzukamo (2004). Don't Get Bitten by the Internet Phish. Retrieved from: http://www.crime-research.org/news/12.06.2004/828/

[26] Dawn Kawamoto (2005). Firms Seek to Reassure Shoppers Over Security. Retrieved from: http://news.com.com/Firms+seek+to+reassure+e-shoppers+over+security/2100-1029_3-5583047.html?tag=nl

[27] iHateSpam for Exchange (2005). Sunbelt Software. Retrieved from: http://www.sunbelt-software.com/product.cfm?id=931

[28] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. Retrieved from: http://www.spamlaws.com/federal/108s877.html

[29] Web Host Industry Review (2005). CAN-SPAM Act Compliance Down. Retrieved from: http://www.spamfo.co.uk/component/option,com_content/task,view/id,92/Itemid,2

[30] Postini. E-mail Security Annual Review and Threat Report (2005). Retrieved from: http://www.postini.com/whitepapers/ThreatReport.pdf

[31] Declan McCullagh (2005). Season Over for Phishing? Retrieved from: http://news.com.com/Season+over+for+phishing/2100-1028_3-5270077.html

Last Updated: January 23rd, 2019

Upcoming Training

SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event