



PHISHING

Kathleen Ting
COEN 150
22 February 2005

I. Abstract

Phishing is a type of fraud in which online fraudsters send out emails or links to Web pages mimicking popular Web sites in order to trick Internet users. These phishing emails and sites generally seek sensitive information, such as bank account numbers or passwords from Internet users. Currently phishing is the fastest growing segment of spam sent worldwide, a crime victimizing both legitimate online companies whose brands are being hijacked and consumers who are unwittingly providing their personal information to criminals.

This paper gives a thorough analysis of what phishing is, the technologies and security risks it takes advantage of, and the dangers it can pose to companies and consumers alike; this paper also provides ethical insight into what can be done to keep from being phished and who is responsible for protecting people from phishers.

II. Introduction

Phishing is a nickname for a particular form of identity theft via computer. The name is an appropriate metaphor for a crime in which email lures are used to fish for personal information from unsuspecting victims. The con men, or phishers, actually steal two identities: first, they hijack the names, logos, and even legal disclaimers of trusted banks, online retailers, credit card companies, Internet service providers, and brokerage firms directly from the respective firms' own websites with a right-click of the mouse. This makes the attack all the more insidious since the average user often does not question an email stamped with the requisite logo and legal disclaimer. Second, they use the spoofed emails and websites to fool people into divulging

personal data—credit card numbers, account user names and passwords, Social Security numbers, and so on. The phishers then use that data to charge goods onto the victim’s credit card or to steal money from the victim’s bank account.

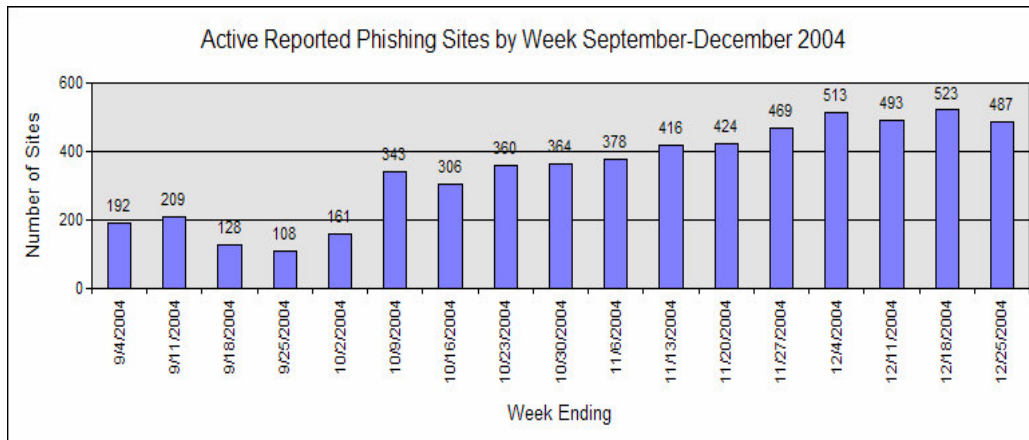
The Anti-Phishing Working Group (APWG), an online industry law enforcement consortium, explains that the term *phishing* “comes from the analogy that Internet scammers are using email lures to fish for passwords and financial data from the sea of Internet users.”¹ The *ph* in *phishing* was also chosen, in part, to pay tribute to the term *phone phreaking*, a technique for dialing free long-distance telephone calls.

On the Internet, phishing—also called carding or brand spoofing—is a scam where the perpetrator sends out legitimate-looking emails appearing to come from some of the Web’s biggest sites—including eBay, PayPal, MSN, Yahoo, BestBuy, and America Online—in an effort to phish out personal and financial information from the hapless user. Phishers use any number of different social engineering and email spoofing ploys to trick their victims. In a recent case before the Federal Trade Commission (FTC), a 17-year-old male sent out messages purporting to be from America Online, stating a billing problem with recipients’ AOL accounts. Furthermore, the phisher’s email displayed AOL logos as well as legitimate links. When recipients clicked on the “AOL Billing Center” link, however, they were taken to a spoofed AOL Web page asking for credit card numbers, personal identification numbers (PINs), social security numbers, bank account numbers, and passwords.

This paper analyzes phishing, the technologies and security risks which it takes advantage of, the dangers it poses—as well as detailing how to keep from being the next phishing victim.

III. Phishing Statistics

Gartner, Inc., a Connecticut-based research firm, reports that 57 million Americans either are sure that they have received email attacks from phishers or believe they may have; 11 million have clicked on the link in the email; and 1.78 million—about three percent of those attacks—recall disclosing sensitive financial or personal information. Of those, 980,000 were actually scammed.² According to APWG chairman Dave Jevans, the rate of attack has been growing exponentially since October 2003.³ The APWG compiled statistics of 282 phishing attacks launched last February, 402 last March, and an astounding 1,974 attacks last July. If these statistics don't seem all that impressive, keep in mind that each attack spawns tens of thousands of emails. The following chart⁴ depicts the number of new schemes reported to the APWG between September and December of 2004.



Further phishing statistics from Gartner, Inc. indicate a yearly loss of 1.2 billion dollars, which is an estimate since most phishing fraud is not given due credit. Identity theft victims often do not link an unauthorized charge to an email they responded to weeks—or even a year—before, and with good reason. In fact, your

chances of telling if these messages are spoofed were better a year ago—they tended to be full of spelling and grammatical mistakes, as evidenced by one such email:

“Unfortunately and according to our successful achievements laterly, our customers where fooled by receiving a fraudulent e-mails that appeared to be form Citibank which are in fact sent by imposters.”⁵

In an ironic twist, phishers now prey on our fears of becoming fraud victims with emails such as the following: “We recently noticed one or more attempts to log in to your account from a foreign IP address, and we have reasons to believe that your account was used by a third party without your authorization. We have established an offline verification system solution designed to maximize confidentiality, integrity and authenticity. If you are the rightful holder of the account, click on the link below.”⁶

Now phishers will often copy the actual language used by the companies they’re impersonating. Terry Cobb, a 36-year-old power plant worker from Hobbs, New Mexico, was lured by just such an email. “I had just signed up for AOL,” he says, “and two days later I got an e-mail, with the company insignia and everything, saying that my information wasn’t complete, and if I didn’t submit the information, my account would be canceled immediately.” A month later, his credit card statement showed purchases of stereo equipment worth \$2000.⁷

Once the message has been devised, the phisher emails it to anywhere from tens of thousands to a million people. From those successfully lured, only three to five percent will actually be bilked for a couple of hundred dollars each. The reasoning behind the relatively modest amount is that a few hundred dollars from a few

thousand people doesn't attract much attention, but still adds up to a sizable paycheck. Another reason, as Cliff Stoll, author of *The Cuckoo's Egg*, found out the hard way, is that authorities find it hard to justify the time and expense it takes to investigate thefts of relatively small amounts, even thousands of them.

Nevertheless, there is no guarantee that all phishers will always be content to just digitally pick pockets. "Once they get your data," says Jevans, "there's really nothing to stop them from opening a credit line in your name, or getting a second mortgage on your house."⁸ According to the Identity Theft Resource Center, the average time spent repairing the damage caused by a stolen identity is approximately 600 hours and can take years to recover completely financially as well as emotionally from the frustration, stress, embarrassment, and sense of being violated.⁹

IV. **Who phishes?**

All kinds of people; it is a low-overhead crime carried out with equipment readily available from your local Fry's. Zachary Keith Hill of Houston, Texas, was a 19-year-old teenager when he phished Terry Cobb. In October 2003, Helen Carr, a 55-year-old Akron, Ohio grandma, was sentenced to 46 months in prison, after she and her partner stole 429 credit card numbers while impersonating AOL. Coming from an ethical standpoint, does the punishment fit the crime? Put differently, will a prison sentence actually deter a determined phisher from ever phishing again?

But Junior and Grandma are not at the helm of phishing; it has become organized crime's new favorite enterprise. "All you really need is three people," says Jevans. "A spammer to handle the e-mails; a financial criminal to launder the credit card

numbers; a mastermind to take care of the web graphics.”¹⁰ Phishing, it turns out, is part of the global economy. “The attacks are coming from Eastern Europe, Asia and Africa,” explains John Curran, a supervisory special agent for the FBI. “We’ve been getting a lot of cooperation from other countries.” He points out a joint U.S.-Romanian investigation that succeeded in netting a phisher who had scammed a half-million dollars.¹¹

V. Simple Mail Transfer Protocol (SMTP)

Written by Jonathan Postel,¹² this protocol describes the transmission of email over the Internet. While it “transfers mail reliably and efficiently,” SMTP does not transfer email securely. With the reason that SMTP has no built-in security measures to authenticate who is sending an email—it only tells the SMTP server on the receiving side who it is, who the email is from (sender), and who the email is for (recipient). There is no guarantee that the sender of the mail is legitimate or that the address was not spoofed.

The sending SMTP server initiates a MAIL command to the receiving SMTP server. This MAIL command indicates the sender of the email. 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 email.¹³ The two systems acknowledge back and forth until the message is delivered, at which time the transmission is complete. Due to an architectural flaw, the existence of the sender of the message is not double-checked. As a result, email spoofing, the forgery of an email header so that the message

appears to have originated from someone or somewhere other than the actual source, is possible.

Although an SMTP service extension (specified in RFC 2554)¹⁴ allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed email, senders insert commands in headers that will alter message information. Consequently, it is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Phishers spoof email to come from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information—any of which could be used for a plethora of criminal purposes. Real examples¹⁵ of spoofed email—which tend to convey a sense of urgency—are as follows:

- “We periodically review accounts - your account will be put on restricted status. To lift this restriction, you need to complete our credit card verification process.”
- “Due to technical security update you have to reactivate your account.”
- “We are having problems with the billing information in your account. We would appreciate it if you would visit our website eBay Billing Center and fill out the proper information that we need to keep you as an eBay member.”
- “Recently our customers have reported receiving fraudulent e-mails that appear to be from Bank One. Please login and learn more about what's happening and how to protect yourself.”

VI. **HTML-based Email**

Email 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, and so they tend to send their hoax emails in HTML format, embedding graphics and formatted text to make the email look more like a legitimate communication from the spoofed company. Logos, banners, and even ads are placed within the email to entice the recipient to believe in the authenticity of the message. If the message were in plain text, with only a URL link, the probable arousal of the user's suspicion would prevent him from clicking on the URL.

VII. **HTML Forms**

A new scheme involves using HTML-based forms within an HTML-formatted email. The code in the form is hidden; therefore, the phisher is able to hide a bogus URL in a *submit* button, which the user subsequently presses after entering his personal information. As a result, it is more likely that a user will fall for such a form-based attack.

VIII. **Domain Naming System (DNS)**

DNS is the hierarchical database that translates numerical Internet Protocol (IP) addresses into human-friendly names. Again due to architectural flaws, there are several security issues with DNS. For one, hackers can hijack a domain, redirecting traffic from the legitimate site to a malicious site set up to look identical to that site.

Another ploy used by phishers is to register domain names with similar looking addresses or using character replacement, such as using the number 1 for the lowercase letter L—to disguise that the address is phony. Yet another ruse is to edit the Uniform Resource Locator (URL) used to find a Web site. The attacker embeds a URL into an email as <http://www.sometrustedsite.com@malicious-site.com>. If the email supports colored fonts, the malicious destination—the Web site to which the user will be taken—will be white, that is, invisible.¹⁶

IX. Trojan Horses and Spyware

A Trojan horse is a malicious software program that masquerades as legitimate software. This can be installed by worms or viruses such as the Mimail¹⁷ virus or unknowingly downloaded by the user—through Internet Relay Chat (IRC) sites, for instance—thinking that it is a game, utility, browser plug-in, or Internet Explorer patch.¹⁸ More sophisticated phishing scams, resembling spyware, are using Trojans to install keystroke loggers to capture a user’s passwords and account numbers, or to install programs that take screenshots of the system. These images, containing usernames, passwords, or credit card numbers, are then forwarded to the phisher. Spyware is software that covertly collects information about the user’s activities (keystrokes, Web sites visited, etc.) and provides that information to a third party. It is used to intercept legitimate communications between the victim and a legitimate organization. The attacker uses pre-positioned spyware on the victim’s computer to extract sensitive information. This can be accomplished from a previous worm or Trojan attack.

X. Malicious Javascript

According to the APWG, one of the more recently discovered cunning tactics involves the use of JavaScript to create a fake browser address bar.¹⁹ This scam effectively bypasses the need to exploit the Internet Explorer security hole that allows disguised URL's to be embedded within the email by using JavaScript to display a fake address bar in the browser that cannot be distinguished from the real one. By disregarding whatever address the user typed in, the malicious code will unfailingly send the user to the phisher's Web site instead.

XI. Social Engineering

In a social engineering attack, scammers pretend to be in a position of authority in order to lure gullible account-holders into entering sensitive information about their accounts. In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a con game. For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in hopes of getting him to reveal information that compromises the network's security. The con might call the authorized employee with some kind of urgent problem; social engineers often rely on the innate helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques.

Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess, and so are careless about protecting it. Frequently, social engineers will dig through dumpsters for valuable information, memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to themselves but guessable by others. Security experts predict that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system.²⁰

XII. What You Can Do to Protect Yourself

Many experts contend that phishing is less of a technology problem and more of a user problem, in that phishers don't force their way into getting what they want, but rather fool people into opening the deadbolted doors themselves. Hence, 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. That said, other experts are becoming more concerned that if the insidious tactics used by more and more phishers are difficult to detect even for experienced computer users, how will less technical users be able to discern a legitimate email, Web address, or Web site from a spoofed one? Compounding the ethical dilemma is that social engineering ploys can be very effective in these spoofing situations. Prevention includes educating people about the value of

information, training them to protect it, and increasing people's awareness of how social engineers operate.

Although a company's best defenses may sometimes be useless against social engineering, it doesn't let the company off the hook (no pun intended), because there are technologies that make phishing, if not impossible to accomplish, at least harder to carry out. One such technology is two-factor authentication using a nonce (one-time password that expires after a single use). This way if the nonce is stolen it will not matter as it expires after one use anyway. The nonce is generated using a shared electronic key between the user and the bank. The user is verified not just with the username and nonce but also by the key that generates the password. However, if the shared electronic key is compromised, then the user has no way of authenticating the bank.

Furthermore, there are email firewall products that implement rules to block spam and phishing scams at the perimeter. These software products implement heuristics, which are updated as new phishing schemes are discovered. They not only block spam, but also verify the IP numbers and Web addresses of the email source and compare them to known phishing sites (an automated version of samspade.org).²¹ Although phishing scams are not considered viruses, anti-virus software can be effective if the user's computer was first infected with a worm, which installed a Trojan that captures personal data.

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 when a company obtains a

private key from a Certificate Authority (CA) and the user obtains the corresponding public key whenever he wishes to correspond with the company. When the user logs into the company's server and the keys don't match, then the user knows that the site is not legitimate. However, if the private key is compromised, then the user has no way of authenticating the Web site, just like with the bank's electronic key.

As mentioned earlier, SMTP has no built-in security features. Given that validating the identity of the originating sender of a message would go a long way in preventing phishing attacks, either the SMTP security extension must be implemented, or some other embedded encryption method for sending email—the ultimate goal being to provide transparent enough authentication for the user, so he uses it on every email. With built-in encryption, the user would not have to deal with public and private keys and so would no longer fret about key compromise.

Avoid becoming a victim of a phishing scam by using common sense and a little skepticism when receiving unsolicited emails. Consumers need to do their part also and would be well served by following the below suggestions culled from MailFrontier, the Department of Justice, and the Federal Trade Commission:²²

- Don't reply to emails asking to confirm account information. Call or log on to the company's Web site to confirm that the email is legitimate. Never respond to an email that looks like it came from your bank or any of your credit card companies, no matter how official it appears. Banks usually want you to access your account through their website—not an email link. Phishing emails stand out because they don't follow the rules.

- Open a new browser window each time you log on to a web site that displays personal information. When you are done at that site, log out and close that browser window.
- Be sure to read emails that say they are from companies you know. Sometimes a real email will have a spelling or grammatical error, but anything more than one error is suspicious.
- Scroll over the links in emails you receive and check them. In some email systems, you can scroll over the different links in an email and see the actual contents of the link. For instance, while the email may purport to be from PayPal, the link content says www.paipall.com. As URLs can be disguised, don't take a suspect link at face value.
- Never use a link in an email to get to any Web page. If you must go there, type the URL directly into your browser's address bar.
- Never enter your personal or credit information into a form in an email. If you feel the email is legitimate, call the company or visit their Web site and log in to provide the requested information.
- Expect good customer service. Unless your name is "eBay user" or "johndoe99," the email is probably spoofed.
- Don't email personal information. Never give your bank account information, credit card numbers, Social Security number, passwords, PINs, or date of birth to anyone who asks for it by email. When submitting information via a Web site, make sure the security padlock is displayed on

the browser's status bar or <https://> starts the beginning of the Web address in the address window.

- Never respond to any offer to buy anything by clicking on the link in the email.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances and to determine whether they have mailed your statement. Check your online accounts at least weekly—often, information obtained through phishing is not used right away.
- Report suspicious activity to the Federal Trade Commission's fraud hotline at (877) IDTHEFT (877.438.4338). Forward the actual phishing email to uce@ftc.gov, the company from which it supposedly comes, and the Internet Crime Complaint Center (www.ifccfbi.gov) a partnership between the FBI and the National White Collar Crime Center.
- Apply the latest patch for your Web browser and operating system. Use and maintain your email protection software for spam blocking, fraud blocking, and anti-virus.
- Stop, Look, and Call
 - Stop: Don't react to phisher ploys of upsetting or exciting information. Do not reply to or click on a link in an email that warns you, with little notice that an account of yours will be shut

down unless you confirm your billing information. Instead, contact the company cited in the email using an authenticated telephone number or other form of communication that you are sure is genuine.

- Look: Look closely at the claims in the email. Also look at the links and Web addresses.
- Call: Call or email the company to verify that the email is legitimate. Look for a domestic telephone number on a company or agency website, and call the number to verify the legitimacy of the Web site. Many phishing attempts originate from outside the U.S. and thus are not likely to have a working domestic phone number. As a further precaution, particularly against U.S. based phishing efforts, verify the number with directory assistance or company information that you know is reliable.

XIII. Summary and Conclusion

Fraud is not new; businesses have fought the fraudster since the beginning, not just of e-commerce, but of commerce. As business practices evolve to keep pace with emerging technology, fraudsters also adapt to the new opportunities that technology offers. By understanding phishing as a distinct and more sophisticated type of email threat, and by seeking solutions designed specifically to stop phishing, companies can protect themselves and customers. Costs related to reissuing credit cards, re-establishing accounts, reimbursing customers for losses, and possible litigation are a

mere sampling of the costs a company may have to absorb due to phishing. If hundreds of accounts were compromised, these costs can easily skyrocket. Recovering from a large-scale phishing scam would be detrimental not only to the company's bottom line, but also to maintaining the trust of their customers.

Heeding the adage that an ounce of prevention is worth more than a pound of cure, eBay has developed a signal on its toolbar that lights up green when the user is on a legitimate eBay site, and red when the site is a known imposter. Brightmail,²³ a company who produces spam-fighting software, has devised a program that detects and thwarts phishing attacks. EarthLink has a free phisher-blocking tool called ScamBlocker that gives a safety rating for each Web site you visit, and will alert you if you're entering a known phisher site. Microsoft, eBay, PayPal, and Visa announced last Tuesday their decision to participate in a network that would develop a central database of known scammers in an effort to curb the growing menace of phishing attacks. IT security firm WholeSecurity will operate the newly launched Phish Reporting Network that would allow companies to report fraudulent sites to a central database. These sites can then be blocked by the member companies from their individual security applications. Tim Lee, vice president of global e-commerce at Visa, added, "Visa is focused not just on shutting down phishing sites, but preventing phishing emails from ever reaching consumers."²⁴ Visa is rightly taking the lead in the fight against phishing as the ethical responsibility ultimately lies with the corporation. If ISPs (Internet Service Providers) and law enforcement were to crack down upon phishers they would inadvertently infringe on the privacy and freedom of innocent consumers.

Nonetheless, no safeguard is perfect. Whatever preventions white hat programmers cook up, black hat programmers, given enough time, will eventually dismantle. Furthermore, phishers don't break down the door; they fool you into opening the door and giving them your secrets. With that in mind, the question for consumers is not "Are you paranoid?" but rather "Are you paranoid enough?"

Endnotes

- ¹ “The Anti-Phishing Working Group (APWG),” 19 February 2005 <http://www.antiphishing.org>.
- ² “Phishing statistics” 19 February 2005 <http://www3.gartner.com/Init>.
- ³ APWG.
- ⁴ APWG.
- ⁵ Jamie Malanowski, “Don’t Take the Bait,” *Reader’s Digest* December 2004: 100.
- ⁶ Malanowski 101.
- ⁷ Malanowski 103.
- ⁸ APWG.
- ⁹ “The Identity Theft Resource Center,” 19 February 2005 <http://www.idtheftcenter.org/facts.shtml>.
- ¹⁰ APWG.
- ¹¹ Malanowski 102.
- ¹² Jonathan Postel, “RFC 821: Simple Mail Transfer Protocol,” 19 February 2005 <http://www.ietf.org/rfc/rfc821.txt>.
- ¹³ Postel.
- ¹⁴ J. Myers, “RFC 2554: SMTP Service Extension for Authentication,” 19 February 2005 <http://www.ietf.org/rfc/rfc2554.txt>.
- ¹⁵ APWG.
- ¹⁶ JoAnne Holliday, “Authentication 3: On the Internet,” 19 February 2005 <http://www.cse.scu.edu/~jholliday/COEN150W05/coen150w05.htm>.
- ¹⁷ “Mimail Prevention and Cure,” 21 February 2005 <http://insight.zdnet.co.uk/internet/security/0,39020457,39117972,00.htm>.
- ¹⁸ “IRC help,” 19 February 2005 <http://www.irchelp.org/irchelp/security/warez.html>.
- ¹⁹ APWG.
- ²⁰ “Social Engineering,” 19 February 2005 <http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html>.
- ²¹ 19 February 2005. <http://samspade.org/>.
- ²² “Phishing,” 19 February 2005 <http://www.ftc.gov/bcp/online/pubs/alerts/phishregalrt.htm>.
- ²³ 19 February 2005 <http://www.brightmail.com/>.
- ²⁴ “Microsoft, Visa, eBay join phish reporting network,” 19 February 2005 http://www.newratings.com/analyst_news/article_696237.html.