Analysis of the Phishing Email Problem and Discussion of Possible Solutions

Christine Drake[1], Andrew Klein[1], Jonathan Oliver[1]

[1] MailFrontier, Inc., 1841 Page Mill Road,
Palo Alto, 94304, USA

Abstract. With the growth of email, it was only a matter of time before social engineering efforts used to defraud people moved online. Fraudulent phishing emails are specifically designed to imitate legitimate correspondence from reputable companies but fraudulently ask recipients for personal or corporate information. Recent consumer phishing attempts include spoofs of eBay, PayPal and financial institutions. Phishing emails can lead to identity theft, security breaches, and financial loss and liability. Phishing also damages e-commerce because some people avoid Internet transactions for fear they will become victims of fraud. In a recent survey, both fraudulent and legitimate emails were misidentified 28 percent of the time and 90 percent of respondents misidentified at least one email. Based on these results, we cannot expect consumers alone to be able to recognize phishing emails. Instead, we must combine multiple solutions to combat phishing, including technical, legal, best business practices, and consumer education.

1 Introduction

"Phishing" is the term for an email scam that spoofs legitimate companies in an attempt to defraud people of personal information such as logins, passwords, credit card numbers, bank account information, social security numbers, and mothers' maiden names. For example, an email may appear to come from PayPal (using the same logo and color schemes), claiming that the recipient's account information must be verified because it may have been compromised by a third party. However, when the recipient provides the account information for verification, the information is really sent to a fraudster, who is then able to access the person's account. The term phishing was coined because the fraudsters are "fishing" for personal information.

The most traditional form of phishing collects personal information in a form in the email or through a fraudulent Web site accessed through a link provided in the email. More recently, some fraudsters use phishing emails as a means to secretly download a keylogging Trojan or spyware application onto the email recipient's computer. For example, fraudsters created a phishing email with a link that sent the user to a Web site, which downloaded a keylogging Trojan onto the user's computer. This application subsequently recorded all information entered by the user into bank Web sites specified in the program and sent the recorded information to the fraudster [12].

Drake C., Klein A. and Oliver J. (2005).
Analysis of the Phishing Email Problem and Discussion of Possible Solutions.
In *Proceedings of the 3rd International Workshop on Security in Information Systems*, pages 309-318
DOI: 10.5220/0002564803090318

Phishing emails range from the very simple to the very sophisticated, which can fool even the savvy Internet user. These fraudulent emails harm their victims through loss of funds and identity theft. They also hurt Internet business, because people are losing trust in Internet transactions [8, 9].

The most targeted industry is financial services. Internet retailers and Internet service providers are also targeted. Phishing emails are mass mailed: Billions of phishing emails are sent out every month [21]. According to a study by Gartner, approximately 57 million U.S. adults believe they have received a phishing email message [9].

More important than the number of phishing emails distributed is the number of people that are fooled by these emails. MailFrontier posted a test on its Web site testing whether people can correctly identify fraudulent emails (http://survey.mailfrontier.com/survey/quiztest.html). Over 300,000 people have taken this phishing test. MailFrontier also contracted a survey company to distribute a more comprehensive survey to over 1000 people. The results from both the test and the survey show that people misidentify both fraudulent and legitimate emails at a rate of over 28 percent and 90 percent of respondents misidentified at least one email. This paper discusses these results and the possible reasons why people fall for phishing emails. The paper then goes on to consider possible solutions to phishing.

2 Why People Get Hooked

When phishing emails first emerged many of them were poorly constructed. They did not contain the legitimate company’s images or links, and contained misspelled words and poor grammar. Lately fraudsters have invested a considerable amount of effort into convincingly spoofing legitimate companies. This section discusses how often people are fooled by phishing emails and how fraudsters use social engineering to lure in their victims.

2.1 The Survey Results

MailFrontier created a test consisting of 10 emails which asked participants to indicate whether each email was fraudulent or legitimate. A similar survey was created consisting of five emails. The 15 emails used in both the test and survey were almost evenly split between fraudulent and legitimate emails (seven fraudulent and eight legitimate). All of the emails used are real fraudulent and legitimate emails received by MailFrontier. The results from the test and survey show that the participants misidentified the emails 28 percent of the time; fraudulent emails were misidentified as legitimate at a rate of 31 percent and legitimate emails were misidentified as fraudulent at a rate of 19 percent.

The survey also grouped the participants’ responses by gender, age, marital status, whether the respondents had young children in the household, household income, region, and employment status. The results were consistent across all of these factors except age. The youngest age group was more likely to believe the emails were legitimate, and in each higher age group the participants were more likely to identify the email as fraudulent. These results held true whether the email was actually legitimate or fraudulent.

Table 1. Survey Responses by Age Group.

	≤ 24	25-34	35-44	45-54	55 +
Misidentified Fraudulent as Legitimate	37%	27.5%	26%	25.5%	21.5%
Misidentified Legitimate as Fraudulent	10%	12%	16%	17%	23%

One possible conclusion is younger Internet users have been raised using the Internet and are more accustomed to relying on the Internet for business transactions. To younger people, disclosing personal information over the Internet might seem more commonplace. Or perhaps older users have just learned to be more cautious or skeptical.

When analyzing these results it is important to remember that many of the recipients of phishing emails are not customers of the spoofed companies and may quickly realize that the email is fraudulent, or may believe that the email was mistakenly sent to them and ignore it. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. In the survey, the participants were asked to judge each email, whether or not they were customers of the legitimate or spoofed company.

The fraudulent emails used in the test are examples of very convincing phishing emails. The test did not use samples of some of the poorly crafted phishing emails. However, most of the phishing emails that are being sent today are very sophisticated. And the number of well crafted emails is expected to increase. The first phishing fraudsters were novices and this showed in the very basic emails that they sent. Then professional criminals began sending out phishing emails, and the emails became more sophisticated [14]. Now free phishing "kits" are available on the Internet, which contain everything necessary to effectively spoof a legitimate company, including graphics, Web code, text, and spammer software. With the availability of these kits, almost anyone can send out believable phishing emails [5]. Phishing emails are also growing in languages such as Spanish, French, German, and Dutch [19].

2.2 Using Social Engineering to Snare Victims

Fraudsters use social engineering in phishing emails, which is the use of psychological methods to manipulate victims into disclosing information [15].

The fraudsters attempt to gain the recipient's trust by making the phishing emails appear to originate from reputable companies. The paper, *Anatomy of a Phishing Email*, by Drake, et al., details the tricks used by fraudsters to spoof legitimate companies and hide any information about their fraudulent domains [2]. For example, the fraudulent emails often contain the company's logo and use similar fonts and color schemes as those used on the company's Web site. If recipients believe that an email was sent by a credible company, they may not scrutinize the content and simply provide the requested information.

Some phishing emails take advantage of people's need to follow through with commitments. For example, a phishing email may claim that its request for information is justified or required by a policy that the recipient agreed to when setting up the account. Many people feel compelled to abide by the agreement they supposedly made and will provide the requested information.

More frequently, fraudsters use fear to call the recipient to action. Ironically, the email messages often use people's fear of fraud to defraud them: the emails may claim that the company has installed new security software and the recipient must renew the account information, or it might claim that the account has been compromised by fraudulent activity and the account information must be confirmed. Other premises include claims that the recipient's account information is outdated, a credit card has expired, or the account information needs to be verified. There are numerous approaches, but in each case, the email threatens to terminate the recipient's account or claims it cannot provide adequate security if the desired information is not provided.

The results of the survey demonstrate that the phishing emails can convincingly appear to come from legitimate companies. Yet the participants in the study knew that none of the emails in the study pertained to their personal accounts or transactions. If a person were to receive a phishing email that purported to threaten his or her personal account, the person would be more prone to falling victim to the scam. Hence, using the survey results to estimate that people fall for fraudulent emails 31 percent of the time is a conservative estimate, because it does not consider how fear plays into a person's reaction to receiving a phishing email.

Well crafted phishing emails have the potential to fool large numbers of people through the implementation of various social engineering techniques. The use of such techniques can also damage real email based communications as people become suspicious of all email. Potential solutions, must consider not only stopping fraudulent email, but must allow and indeed encourage, the use of use of email as a communication medium.

3 Possible Solutions to Phishing

In 2004, the economic damage caused by phishing is estimated to have exceeded $44 billion worldwide compared to $14 billion in 2003 [10]. Yet misidentifying legitimate email as fraud is also damaging, because it hurts Internet business. For example, many people believe using on-line banking increases the likelihood that they will become victims of identity theft, even though on-line banking provides more secure identity protection than paper and mail based systems [18]. If solutions to phishing are not adopted, it is estimated that the United States e-commerce annual growth rate will shrink to 10 percent or less by 2007 [8]. This section discusses possible phishing solutions.

3.1 Applying Technical Solutions

There are a variety of techniques available which protect against phishing. These techniques include phishing black lists, encryption, authentication, URL exploit detection, and content filtering.

Phishing black lists are a popular technique. One method identifies when an email's sending IP address comes from a compromised machine. Determining that an email was sent from a Web server that is known for sending fraudulent email can be helpful. However, a compromised machine can send both fraudulent and legitimate emails. Hence, this identification should only be used as one indicator of fraud and not a conclusive determination.

Another method relies on the identification of a domain name or IP address used to host a phishing Web site. A black listed URL to a phishing Web site is a definite indicator of fraud and is a useful reactive technology. However, strictly relying on known phishing emails has limited value. Fraudsters quickly turn to new emails and domains. Based on data from June 2004, phishing Web sites are operational for only 54 hours on average before being shut down or abandoned [11]. This method also does not protect against customized attacks sent to specific individuals.

Encryption based methods are another technical solution that may help identify phishing emails as fraudulent and prevent them from reaching the inbox. For example, user-based authentication can be achieved by using Secure/Multipurpose Internet Mail Extensions (S/MIME), which encrypts messages and allows the recipient to authenticate the sender. However, managing encryption keys is too much of a burden for most people.

Another method is domain-based authentication, with variations including authenticating the email envelope, header, or domain in the header. These approaches would help to identify when an email is claiming to be from somewhere that it is not, but they will not stop phishing. For example, if a phishing email claimed to be from U.S. Bank, but really originated from the domain "pact-games.org" (this is an example from a real phishing email), domain-based authentication would flag this email. However, another real phishing email spoofed eBay and used the domain "ebay-customer-validate.info." Domain-based authentication would not catch this phishing email because it came from the domain that it claimed to be from. The fraudster had registered a domain that recipients may mistakenly believe belonged to eBay, but it did not try to falsify its domain.

Detecting URL exploits is another method used to prevent phishing. URL exploits attempt to disguise the true identity of the phishing Web site from the user. While URL exploits are a good indicator of phishing emails, they are not used in all phishing emails, and their use does not guarantee that the message is fraudulent. Legitimate emails also can legally use the same tricks.

One method of concealing the Web site destination is to show a different text in the email and hide the true URL in the email code. But many fraudsters take this a step further and also conceal the URL in the code. For example, the IP address of the Web site is used rather than the hostname. An IP address can be obscured further by expressing it in Dword, Octal, or Hexadecimal format. Other tricks include: using the @ symbol in the <*userinfo*>@<*host*> format, where the <*userinfo*> is ignored and the <*host*> information after the @ symbol is the true destination; using JavaScript, such as using OnMouseOver or functions to hide the link; and using redirection services to hide the final destination. A good phishing filter will be able to identify these techniques when used in an email and will use this as an indictor of a phishing email.

Content filtering can be an effective technique in protecting against fraudulent emails. However applying content filtering that is designed to prevent spam to defending against phishing is ineffective. Phishing email is designed to mimic legitimate correspondence, which makes it unique from spam. The specific features of phishing emails need to be considered when using content filtering.

Statistical methods can be used in content filtering to analyze the content and apply a judgment. To stop phishing, a statistical method needs to be specifically trained to recognize a phishing email, which is done by using both phishing emails and legitimate correspondence from targeted companies. This training will be able to identify content. However, this content identification needs to be combined with the other methods to give an effective determination of fraud [6].

Ideally, phishing filters stop phishing emails before they enter the inbox. However, if consumers are not protected by a good phishing filter, they may receive phishing emails and follow the link in the email to a fraudulent phishing Web site. Some technical solutions focus on identifying the fraudulent Web sites. For example, some vendors have created browser-based tool bars that alert customers when they have accessed a potentially fraudulent Web site. Some toolbars are customized for a particular company's toolbar such as eBay, while others are more general in their application [3, 4, 20]. Yet another toolbar feature called SpoofStick clearly shows the domain or IP address of the site. Because phishing emails often obscure the Web site link, this tool might provide some limited assistance. However, many legitimate sites use unintuitive domain names, while some fraudulent sites have domain names that may appear to be legitimate. None of the toolbar features protect against phishing emails that collect information in a form in the email. Also, they do not protect against Web sites that secretly download keylogging Trojans or spyware applications. Even though the toolbar might indicate that the Web site is fraudulent, once the Web site is open, the damage may already be done.

A combination of techniques should be used to stop fraudulent emails before they reach the inbox. However, other non-technical solutions must simultaneously be adopted to help prevent the damage from phishing emails.

3.2 Using Legal Solutions

On July 15, 2004, the Identity Theft Penalty Enhancement Act (ITPEA) was signed into federal law. Under this law, if a person uses someone else's identity without lawful authority to commit one of the felonies listed in the Act, the person will be given an additional 2-year prison sentence along with the punishment provided for the felony committed [16].

ITPEA also modifies Section 1028 of title 18 of the United States Code, which now makes it punishable to merely possess another's identification with the intent to commit a crime. However, all of ITPEA provisions require that a fraudster acquire a victim's personal information. This law does not punish the creation of the phishing emails or the fraudulent Web sites. It is very likely that someone must have already fallen victim to the scam and suffered a loss before the fraudster can be held accountable by this Act [16].

Senator Patrick Leahy has proposed the Anti-Phishing Act of 2004, introduced to the United States Senate on July 9, 2004. This Act criminalizes sending phishing emails and creating fraudulent Web sites for the purpose of committing fraud or identity theft. If passed, this Act will make every element of phishing a felony, with each element carrying a punishment of five years in prison and/or a fine of up to $250,000. Currently the Act is in committee and has not yet been voted on by the Senate [14, 17].

Passing laws that criminalize phishing will not stop these scams. The people sending phishing emails are stealing personal information to commit felonies. The possibility of the sentence being increased for stealing someone's identity, in addition to the underlying felony, will most likely not deter the fraudsters. Also, if the anti-phishing laws make conducting phishing scams in the United States too risky, fraudsters can send their emails from overseas [14].

3.3 Changing Business Practices

Although businesses cannot prevent phishing emails from winding up in their customers' inboxes, they can establish business practices that help the recipients recognize phishing emails and use processes that minimize the damage of phishing emails. Many companies in the past and some companies still today provide links in emails and request the recipient follow the link to either gather or provide information. However, many companies have begun to change their business practices to make it easier for their customers to recognize phishing emails, which help to ensure their customers' safety. Here are some suggested business practices:

- Businesses should always address their customers by name. Generally fraudsters do not have access to any of the customers' personal information. If businesses always address their customers by name, any email spoofing the companies with salutations such as Dear Member or Dear Customer can be identified as fraudulent.
- Businesses should not request personal information in an email. Instead, businesses should ask their customers to open a browser window and enter the businesses' URLs manually. Then, if required, their customers can log-in as they usually would.
- Businesses should notify their customers of their security and privacy policies.
- Businesses should provide a means for their customers to report phishing emails that target their company. In addition, businesses can post any information they have concerning phishing emails.
- Businesses can search domain names to see if there are registered domain names similar to theirs, which could possibly be used for phishing purposes.
- Businesses should inform their employees that they might receive phishing emails. A fraudulent email may appear to come from the company's IT department asking the recipient to update their password. If fraudsters get access to company records, they can personalize their phishing emails, making them more convincing.

- Businesses should make sure their customer support staff are aware of phishing emails and they can provide information on detecting and avoiding these scams.

In May 2004, a phishing email victimized over one million customers of a bank. The Ponemon Institute surveyed 411 randomly selected bank customers who had received the phishing email. All of the 411 customers surveyed clicked on the link in the phishing email, which took them to the fraudulent Web site. Also, all of them contacted the bank's customer service help line for guidance. Only 65 (16%) of the 411 provided personal information on the fraudulent site. However, 310 (75%) of those surveyed felt the bank did not provide adequate support and 243 (59%) decided to terminate their business relationship with the bank. It is crucial that businesses train their support staff to adequately provide information and guidance to their customers when they are faced with possibly fraudulent emails [13].

Businesses can also change how customers conduct business transactions in ways that can minimize the damage caused by phishing emails. For example, businesses can use authentication mechanisms, such as sending the customer a different password to their cellular phone for each requested business transaction, sending each customer a small hardware device that generates unique password tokens, or always referencing a "shared secret" (for example, the customer's favorite color) in business correspondence to differentiate legitimate correspondence from fraudulent emails. However, these methods may not be practical because they increase the company's cost of doing business and further inconvenience the company's customers [7, 9].

3.4 Educating Consumers

The solutions mentioned above will not prevent all phishing emails from entering inboxes. Consumers must also be educated on how to protect themselves from phishing emails. The following guidelines will help prevent consumers from falling victim to phishing scams.

- Consumers should avoid clicking on links in emails. Even if the link appears to come from a legitimate source, it should not be trusted. If the email asks recipients to visit a trusted site, consumers should manually type the URL into a browser window to ensure that you are visiting the real site.
- Some URLs claim to be sending consumers to a "secure" site by using "https" instead of "http." However, links and even browser address bars can be faked so that they falsely display an "https" URL. Users should manually type in a trusted company's URL. Then when providing personal information they should look for the "https" at the beginning of the URL, which indicates that the transactions are being conducted securely.
- Consumers should never send personal information in an email. If the request for information looks legitimate, recipients should contact the company directly. Recipients should not contact the company by using the information in the email, but should use the contact information from trusted correspondence (for example, contact information included on a bank statement or on the back of a credit card).

- Consumers should install products that can help identify phishing emails. It is best to install products that will help to prevent phishing emails from ever entering the inbox. However, other technology can provide another level of defense.
- Consumers should read the security policies of the companies with which they do business. Many companies provide information on their Web sites.

In the United States, phishing emails can be reported to: The Internet Fraud Complaint Center (a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center) at http://www1.ifccfbi.gov/index.asp; to the FBI "submit a tip" page at https://tips.fbi.gov/; or to the Federal Trade Commission by entering information on the ID Theft Complaint Input Form at https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.

4 Conclusion

The number of phishing emails has grown dramatically. The average monthly growth rate of new, unique phishing emails was 38% from July 2004 to December 2004, with 9,019 unique phishing frauds reported in December [1]. However, a larger concern is people are not able to differentiate phishing emails from legitimate business correspondence. In the MailFrontier survey and test people misidentified fraudulent emails at a rate of over 31 percent. Recipients of phishing emails will likely not respond if they are not customers of the spoofed company. However, those that are customers may be fooled at an even higher rate than the survey and test respondents because of the social engineering tricks employed by the fraudsters.

We need to significantly diminish the effectiveness of phishing to discourage fraudsters from sending these emails. No single solution in this paper will end phishing. We must work together – technology providers, the legal system, businesses, and consumers – to safeguard Internet users and restore our faith in e-commerce.

References

1. Anti-Phishing Working Group (January 2005). Phishing Attack Trends Report – December 2004. Retrieved from http://antiphishing.org/APWG%20Phishing%20Activity%20Report%20-%20December%202004.pdf
2. Drake C.E., J.J. Oliver, and E. J. Koontz (July 2004), Anatomy of a Phishing Email. *Proceedings of First Conference on Email and Anti-Spam (CEAS), Mountain View, CA, July 30 and 31, 2004.* Retrieved from http://www.ceas.cc/papers-2004/114.pdf
3. EarthLink Aims to Block 'Phishing Scams (19 April 2004). *CNET News.com*. Retrieved from http://zdnet.com.com/2100-1105_2-5194778.html
4. Gilbert, Alorie (17 August 2004). Anti-Phishing Software Detects Fraudulent Lures. *CNET News.com.* Retrieved from http://news.zdnet.co.uk/internet/security/0,39020375,39163688,00.htm
5. Keizer, Gregg (19 August 2004). Do-It-Yourself Phishing Kits Lead to More Scams. *InternetWeek.com.* Retrieved from http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=29111947

6. Koontz, Eugene, Jonathan Oliver and Andrew Klein (January 2005). Bayesian Spam Classification Applied to Phishing Fraud. *Proceedings of Spam Conference, Cambridge, MA, January 21, 2005*. Retrieved from http://www.spamconference.org/abstracts.html#Koontz
7. Lebihan, Rachel (26 August 2004). Still Fishing for Answer to Internet Scam. *Australian Financial Review*. Retrieved from http://afr.com/articles/2004/08/25/1093246607260.html
8. Litan, Avivah (14 May 2004). Phishing Victims Likely Will Suffer Identity Theft Fraud. *Gartner*.
9. Litan, Avivah and John Pescatore (8 June 2004). Catching Phishers Requires More than Bait. *Gartner*. Retrieved from http://www.protectingthenet.com/archives/Phishers.pdf
10. mi2g (20 October 2004). Q3 2004: The Rise of Islamist Hacking and Criminal Syndicates. Retrieved from http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/201004.php
11. Monosson, Rich (14 August 2004). Life Span of a Phishing Site Averages 54 Hours. *Netcraft*. Retrieved from http://news.netcraft.com/archives/2004/08/14/life_span_of_a_phishing_site_averages_54_hours.html
12. Munro, Jay (31 August 2004). Security Watch Alert: Bagle AI Spreads Fast While Rbot.GR Hijacks Webcams. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,1759,1641759,00.asp
13. Ponemon, Larry (24 August 2004). Phishy E-mails and Web Sites: What's Your Responsibility?" *Computerworld*. Retrieved from http://www.computerworld.com/managementtopics/management/story/0,10801,95461,00.html?f=x25>
14. Ramasastry, Anita (16 August 2004). Hooking Phishermen. *CNN.com*. Retrieved from http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing/
15. Rusch, Jonathan J. The 'Social Engineering' of Internet Fraud. *United States Department of Justice*. Retrieved from http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm
16. United States. Cong. Senate. 108th Congress, 1st Session. H.R. 1731, A Bill to Amend Title 18, United States Code, to Establish Penalties for Aggravated Identity Theft, and for Other Purposes [introduced in the House of Representatives April 10, 2003]. 108th Congress. Congressional Bills, GPO Access. Retrieved from http://frwebgate.access.gpo.gov/cgibin/useftp.cgi?IPadress=162.140.64.88&filename=h1731ih.txt&directory=/diskb/wais/data/108_cong_bills>
17. United States. Cong. Senate. 108th Congress, 2nd Session. S. 2636, A Bill to Criminalize Internet Scams Involving Fraudulently Obtaining Personal Information, Commonly Known as Phishing [introduced in the U.S. Senate; July 9, 2004]. 108th Congress. Congressional Bills, GPO Access. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=s2636is.txt&directory=/diskb/wais/data/108_cong_bills
18. Van Dyke, James (March 2004). Online Account Management as the Antidote to Fraud: Financial Institutions and Billers Must Revamp Their Web Features and Messages. *Javelin Strategy & Research*. Retrieved from http://www.javelinstrategy.com/rp.html
19. Varghese, Sam (10 May 2004). Phishing Spreads in Europe. *smh.com.au*. Retrieved from http://www.smh.com.au/articles/2004/05/10/1084041315645.html?oneclick=true
20. Vijayan, Jaikumar (16 August 2004). Antiphishing Tool Adopted by eBay Now Available to the General Public. *Computerworld*. Retrieved from http://www.computerworld.com/securitytopics/security/story/0,10801,95280,00.html
21. Warner, Bernhard (6 May 2004). Billions of "Phishing" E-mails Sent Monthly. *Reuters*. Retrieved from http://www.ladlass.com/archives/002196.html