ISSN: 2321-7782 (Online)
Volume 1, Issue 7, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Phishing: A Computer Security Threat

Aryan Chandrapal Singh[1]
Assistant Professor
Department of Computer Engineering
Jaihind College of Engineering, Kuran
Pune – India

Kiran P. Somase[2]
Assistant Professor
Department of Computer Engineering
Jaihind College of Engineering, Kuran
Pune – India

Keshav G. Tambre[3]
Assistant Professor
Department of Information Technology
Dnyanganga College of Engineering
Pune – India

Abstract: ***In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes.***

There are many variations on this scheme. It is possible to Phish for other information in additions to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage caused by phishing ranges from denial of access to e-mail to substantial financial loss.

This report also concerned with anti-phishing techniques. There are several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing. No single technology will completely stop phishing. However a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. Anti-phishing software and computer programs are designed to prevent the occurrence of phishing and trespassing on confidential information. Anti-phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported and even reviewed as a report after a period of time.

Keywords: Network Security, Internet Fraud, Identity Theft, Phishing Techniques, Social Engineering, Hacking tool.

I. INTRODUCTION

In the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes. There are many variations on this scheme. It is possible to Phish for other information in additions to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss.

This report also concerned with anti-Phishing techniques. There are several different techniques to combat Phishing, including legislation and technology created specifically to protect against Phishing. No single technology will completely stop Phishing. However a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of Phishing and the losses suffered from it. Anti-Phishing software and computer programs are designed to prevent the occurrence of Phishing and trespassing on confidential information. Anti-Phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported and even reviewed as a report after a period of time. This also includes detecting Phishing attacks, how to prevent and avoid being scammed, how to react when you suspect or reveal a Phishing attack and what you can do to help stop Phishers.

The simplified flow of information in a Phishing attack is-

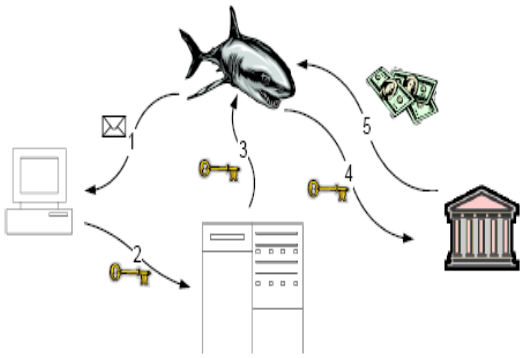

Figure 1.1

1. A deceptive message is sent from the Phishers to the user.
2. A user provides confidential information to a Phishing server (normally after some interaction withthe server).
3. The Phishers obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishers obtains illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute Phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

II. PHISHING TECHNIQUES

Phishers use a wide variety of techniques, with one common thread.

LINK MANIPULATION:

Most methods of Phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by Phishers. In the following example, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the yourbank website; actually this URL points to the "yourbank" (i.e. Phishing) section of the example website.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password. For example, http://www.google.com@members.tripod.com/ might deceive a casual observer into believing that it

will open a page on www.google.com, whereas it actually directs the browser to a page on members.tripod.com, using a username of www.google.com: the page opens normally, regardless of the username supplied.

FILTER EVASION:

Phishers have used images instead of text to make it harder for anti-Phishing filters to detect text commonly used in Phishing e-mails.

WEBSITE FORGERY:

Once a victim visits the Phishing website the deception is not over. Some Phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

PHONE PHISHING:

Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the Phishers) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

III. PHISHING EXAMPLES

PAYPAL PHISHING:

In an example PayPal phish, spelling mistakes in the e-mail and the presence of an IP address in the link are both clues that this is a Phishing attempt. Another giveaway is the lack of a personal greeting, although the presence of personal details would not be a guarantee of legitimacy. A legitimate Paypal communication will always greet the user with his or her real name, not just with a generic greeting like, "Dear Accountholder." Other signs that the message is a fraud are misspellings of simple words, bad grammar and the threat of consequences such as account suspension if the recipient fails to comply with the message's requests.

Note that many Phishing emails will include, as a real email from PayPal would, large warnings about never giving out your password in case of a Phishing attack. Warning users of the possibility of Phishing attacks, as well as providing links to sites explaining how to avoid or spot such attacks are part of what makes the Phishing email so deceptive. In this example, the Phishing email warns the user that emails from PayPal will never ask for sensitive information. True to its word, it instead invites the user to follow a link to "Verify" their account; this will take them to a further Phishing website, engineered to look like PayPal's website, and will there ask for their sensitive information.

RAPID SHARE PHISHING:

On the RapidShare web host, Phishing is common in order to get a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cool down times between downloads. Phishers will obtain premium accounts for RapidShare by posting at warez sites with links to files on RapidShare. However, using link aliases like TinyURL, they can disguise the real page's URL, which is hosted somewhere else, and is a look-a-like of Rapid Share's "free user or premium user" page. If the victim selects free user, the Phishers just passes them along to the real RapidShare site. But if they select premium, then the Phishing site records their login before passing them to the download. Thus, the Phishers has lifted the premium account information from the victim.

Examples of Phishing E-mails:

Phishing e-mail messages take a number of forms. They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.

The main thing Phishing e-mail messages have in common is that they ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data. The following is an example of what a Phishing scam in an e-mail message might look like.

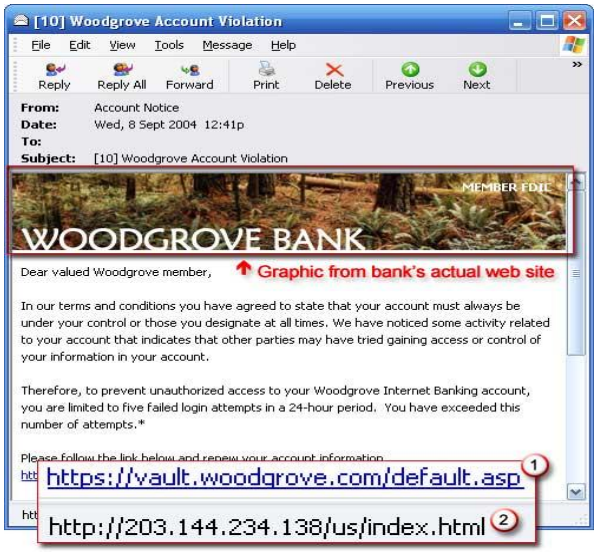

Figure 3.2.1

Example of a Phishing e-mail message, which includes a deceptive Web address that links to a scam Web site. To make these Phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

Phishing links that you are urged to click in e-mail messages, on Web sites, or even in instant messages may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate Web site.

Example of a masked Web address:

Notice in the following example that resting (but not clicking) the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.

Figure 3.2.2

IV. REASONS OF PHISHING

Let's consider some of the reasons people fall victim to Phishing scams.

TRUST OF AUTHORITY:

When a Phishing email arrives marked as "High Priority" that threatens to close our bank account unless we update our data immediately, it engages the same authority response mechanisms that we've obeyed for millennia. In our modern culture, the old markers of authority – physical strength, aggressiveness, ruthlessness – have largely given way to signs of economic power. "He's richer than I am, so he must be a better man". If you equate market capitalization with GDP then Bank of America is the 28th most powerful country in the world. If you receive a personal email purported to come from BOA questioning the validity of your account data, you will have a strong compulsion to respond, and respond quickly.

TEXTUAL AND GRAPHIC PRESENTATION LACKS TRADITIONAL CLUES OF VALIDITY:

Most people feel that they can tell an honest man by looking him in the eye. You can spot a "professional" panhandler before he gets to the fourth word in his spiel. Without clues from the verbal and physical realms, our ability to determine the validity of business transactions is diminished. This is a cornerstone of the direct mail advertising business. If a piece of mail resembles some type of official correspondence, you are much more likely to open it. Car dealers send sales flyers in manila envelopes stamped "Official Business" that look like the envelopes tax refund checks are mailed in. Banks sendcredit card offers in large cardboard envelopes that are almost indistinguishable from FedEx overnight packages. Political advertisements are adorned with all manner of patriotic symbols to help us link the candidate with our nationalistic feelings.

E-MAIL AND WEB PAGES CAN LOOK REAL:

The use of symbols laden with familiarity and repute lends legitimacy (or the illusion of legitimacy) to information-whether accurate or fraudulent-that is placed on the imitating page. Deception is possible because the symbols that represent a trusted company are no more 'real' than the symbols that are reproduced for a fictitious company. Certain elements of dynamic web content can be difficult to copy directly but are often easy enough to fake, especially when 100% accuracy is not required. Email messages are usually easier to replicate than web pages since their elements are predominately text or static HTML and associated images. Hyperlinks are easily subverted since the visible tag does not have to match the URL that your click will actually redirect your browser to. The link can look like

http://bankofamerica.com/loginbut the URL could actually link to

http://bankofcrime.com/got_your_login.

V. DAMAGES CAUSED BY PHISHING

The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss. This style of identity theft is becoming more popular, because of the readiness with which unsuspecting people often divulge personal information to Phishers, including credit card numbers, social security numbers, and mothers' maiden names. There are also fears that identity thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the Phishers may use a person's details to create fake accounts in a victim's name. They can then ruin the victims' credit, or even deny the victims access to their own accounts.

It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by Phishing, totaling approximately US$929 million.

VI. ANTI PHISHING

There are several different techniques to combat Phishing, including legislation and technology created specifically to protect against Phishing.

SOCIAL RESPONSES:

One strategy for combating Phishing is to train people to recognize Phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer Phishing tactic, which uses Phishing e-mails targeted at a specific company, known as Spear Phishing, has been harnessed to train individuals at various locations. People can take steps to avoid Phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by Phishers), it is a sensible precaution to contact the company from which the e-mail apparently originates to check that the e-mail is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected Phishing message.

Nearly all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to Phishers. Some companies, for example PayPal, always address their customers by their username in e-mails, so if an e-mail addresses the recipient in a generic fashion ("Dear PayPal customer") it is likely to be an attempt at Phishing. E-mails from banks and credit card companies often include partial account numbers. However, recent research has shown that the public do not typically distinguish between the first few digits and the last few digits of an account number—a significant problem since the first few digits are often the same for all clients of a financial institution. People can be trained to have their suspicion aroused if the message does not contain any specific personal information. Phishing attempts in early 2006, however, used personalized information, which makes it unsafe to assume that the presence of personal information alone guarantees that a message is legitimate. Furthermore, another recent study concluded in part that the presence of personal information does not significantly affect the success rate of Phishing attacks, which suggests that most people do not pay attention to such details.

The Anti-Phishing Working Group, an industry and law enforcement association has suggested that conventional Phishing techniques could become obsolete in the future as people are increasingly aware of the social engineering techniques used by Phishers. They predict that Pharming and other uses of malware will become more common tools for stealing information.

TECHNICAL RESPONSES:

Anti-Phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

a. Helping to identify legitimate sites

b. Browsers alerting users to fraudulent websites

c. Augmenting password logins

d. Eliminating Phishing mail

e. Monitoring and takedown

LEGAL RESPONSES:

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected Phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information. In the United States, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005.Companies has also joined the effort to crack down on Phishing.

VII. DEFEND AGAINST PHISHING ATTACKS

PREVENTING A PHISHING ATTACK BEFORE IT BEGINS:

A Phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposal have been made to institute a “holding period” for new domain registration during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go “live,” but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest.

DETECTING A PHISHING ATTACK:

Many different technologies may be employed to detect a phishing attack, including providing a spoof reporting E-mail address that customers may send spoof emails to. This may both provide feedback to customers on whether communications are legitimate, and provide warning that an attack is underway. Monitoring "bounced" email messages. Many Phishers email bulk lists that include nonexistent email addresses, using return addresses belonging to the targeted institution. Establishing "honeypots" and monitoring for email purporting to be from the institution. There are contractors that will perform many of these services. Knowing when an attack is underway can be valuable, in that it may permit a targeted institution to institute procedural countermeasures, initiate an investigation with law enforcement, and staff up for the attack in a timely manner.

PREVENTING THE DELIVERY OF PHISHING MESSAGES:

Once a phishing attack is underway, the first opportunity to prevent a phishing attack is to prevent a phishing message from ever reaching a user.

PREVENTING DECEPTION IN PHISHING MESSAGES AND SITES:

There are two different points to thwart phishing presentation deception: at the message, and at the site to which the message points.

VIII. CONCLUSION

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. Phishing attacks can be detected rapidly through a combination of customer reportage, bounce monitoring, image use monitoring, honeypots and other techniques. Email authentication technologies such as Sender-ID and cryptographic signing, when widely deployed, have the potential to prevent phishing emails from reaching users. Personally identifiable information should be included in all email communications. Systems allowing the user to enter or select customized text and/or imagery are particularly promising. Browser security upgrades, such as distinctive display of potentially deceptive content and providing a warning when a potentially unsafe link is selected, could substantially reduce the efficacy of phishing attacks. Information sharing between the components involved in a phishing attack – spam filters, email clients and browsers – could improve identification of phishing messages and sites, and restrict risky behaviour with suspicious content. Anti-phishing toolbars are promising tools for identifying phishing sites and heightening security when a potential phishing site is detected. Detection of outgoing confidential information, including password hashing, is a promising area of future work, with some technical challenges.

References

1. Mutton, Paul. "Fraudsters seek to make phishing sites undetectable by content filters". Netcraft. Archived from the original on 2011-01-31. Retrieved July 10.
2. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter.Handbook of Information and Communication Security. Springer. ISBN 9783642041174.
3. Mutton, Paul. "Phishing Web Site Methods". FraudWatch International. Archived from the original on 2011-01-31. Retrieved December 14, 2006.
4. "Internet Banking Targeted Phishing Attack".Metropolitan Police Service. 2005-06-03. Archived from the original on 2010-02-18. Retrieved 2009-03-22.
5. "Phishers target Nordea's one-time password system". Finextra. October 12, 2005.
6. Cleber K., Olivo , Altair O., Santin , Luiz S., Oliveira (July 2011). "Obtaining the Threat Model for E-mail Phishing"(PDF). Applied Soft Computing. Archived from the originalon 2011-07-08.
7. "Anti-Phishing Working Group: Vendor Solutions". Anti-Phishing Working Group. Archived from the original on 2011-01-31. Retrieved July 6, 2006.
8. Landing another blow against email(Google Online Security Blog)
9. Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)"
10. Felix, Jerry And Hauck, Chris "System Security: A hacker's Perspective"

AUTHOR(S) PROFILE

Prof. Aryan Chandrapal Singh, received his B.Tech degree in Computer Science & Engineering from IIMT Engineering College (UPTU, Lucknow), Meerut in 2005. Also currently pursuing the M.Tech in Computer Science & Engineering from Rajasthan Technical University, Kota. He is having 8 years of experience in teaching and also presently working as an Assistant Professor at Jaihind College of Engineering, Kuran (Pune University, Pune).

Prof. Kiran P. Somase, received the Diploma in Computer Technology from K.B.P. Polytechnic, Kopargaon in 2006 and B.E. degree in Computer Engineering from SRES College of Engineering, Kopargaon in 2009. Also currently pursuing the M.Tech in Computer Science Engineering from Rajasthan Technical University, Kota. He is having 4 years of experience in teaching and also presently working as an Assistant Professor at Jaihind College of Engineering, Kuran (Pune University, Pune).

Prof. Keshav G. Tambre, received the B.E. degree in Computer Engineering from Terna College of Engineering, Osmanabad in 2006. Also currently pursuing the M.E in Software Engineering from Dr.Bhimrao Ambedkar Marathwada University, Aurangabad. He is having 6 years of experience in teaching and also presently working as an Assistant Professor at Dnyanganga College of Engineering, Narhe (Pune University, Pune).

