International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 608 – 612

Phishing: A Continual Threat for Cyber World

Somnath Basak
Computer Science & Engineering
Brainware Group of Institutions-Sabita DeviEducation TrustKolkata, India
somnath.basak30@gmail.com

Chandrani Ray Chowdhury
Computer Science & Engineering
Brainware Group of Institutions-Sabita Devi Education Trust
Kolkata, India
crc24jan@gmail.com

Abstract—Phishing is the act of attempting to acquire personal or sensitive information such as usernames, passwords, and credit card details, banking information detail. Phishing is usually done by sending emails that seem to appear to come from credible sources. Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal personal information. Email is the popular medium used in the phishing attacks and such email is also called as spams; however, not all email is spam emails. It is important to understand these types of emails with which we deal every day.

This paper gives brief information about phishing, its attacks, phishing techniques and steps that users can take to safeguard their confidential information.

Keywords-*cyber crime; spam; whaling; hoax mail; man-in –middle attack; website forgery.*

*****

I. INTRODUCTION

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life; on the other hand it also increases cybercrime. For this reason, we need improve the cyber security measures. For example all web browsers and servers take almost every care to make guarantee the safe business through internet. Still they are vulnerable to attacks such as phishing. Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion[1]. A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. 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 and it is a continual threat of cyber world.

II. TYPES OF PHISHING

There are basically four types of phishing.

A. Spam Email

Spam is most often considered to be electronic junk mail. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. It the main medium of speeding the phishing scams.

B. Hoax Email

An email hoax is a scam that is distributed in email form. It is designed to deceive and defraud email recipients, often for monetary gain. Commonly, the sender's name/address and the body of the message are formatted to appear from a legitimate source, as though the email came from a bank or a newspaper or legitimate company on the Web. Sometimes, the spoofer will make the email appear to come from a private citizen somewhere.

An email hoax is a commonly used Internet scam tactic targeted to specified demographics, markets or causes including:

1) Charities, such as missing children

The FBI has become aware of a spear-phishing e-mail made to appear as if it were from the National Center for Missing and Exploited Children. The subject of the e-mail is "Search for Missing Children," and a zip file containing

three malicious files is attached. E-mail recipients should never open attachments or click links in suspicious e-mails [2].

2) Nigerian scams

A scam is where the sender requests help in facilitating the transfer of a substantial sum of money, generally in the form of an email. In return, the sender offers a commission, usually in the range of several million dollars. The scammers then request that money be sent to pay for some of the costs associated with the transfer. If money is sent to the scammers, they will either disappear immediately or try to get more money with claims of continued problems with the transfer which is also known as "advance fee fraud".

3) Lottery scams

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery. The recipient of the message, the target of the scam, is usually told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but will never receive any lottery payment. Many email lottery scams use the names of legitimate lottery organizations or other legitimate corporations or companies, but this does not mean the legitimate organizations are in any way involved with the scams.

4) Chain letters

A typical chain letter consists of a message that attempts to convince the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible. In reality, the "chain" is actually a geometrically progressing pyramid that cannot be sustained indefinitely. Common methods used in chain letters include emotionally manipulative stories, get-rich-quickly pyramid schemes, and the exploitation of superstition to threaten the recipient with bad luck or even physical violence or death if he or she "breaks the chain" and refuses to adhere to the conditions set out in the letter. Chain letters started as actual letters that one received in the mail. Today, chain letters are generally no longer actual letters. They are sent through email messages, postings on social network sites, and text messages.

5) Fake security warnings

A tactic frequently used by criminals involves convincing users that a virus has infected their computer, and then suggesting that they download (and pay for) fakes antivirus software to remove it. Usually the virus is entirely fictional and the software is non-functional or malware itself [3].

C. Spear Phishing

"Spear Phishing" is a method of sending a phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; spear phishing describes any highly targeted phishing attack. Spear phishers send email that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look like as if it has come from your employer, or from a colleague who might send an email message to everyone in the company; it could include requests for usernames or passwords. Spear phishing scams work to gain access to a company's entire computer system. If you respond with a username or password, or if you click on the links or open the attachments in a Spear Phishing E-Mail, pop up window or website, then you might become a victim of ID theft and you might put your employer or group at risk. Spear Phishing also describes scams that target people who use a certain product or website. Scam artist use any information they can to personalize a Phishing scam to as specific a group as possible.

D. Whaling

Whaling is a form of phishing and spear phishing targeting executives from the top management in the organizations, usually from private companies. The objective is to swindle the executives into reveling confidential information. Whaling targets c level executives sometimes with the help of information gleaned through spear phishing, aimed at installing malware for key logging or other backdoor mechanisms. Emails sent in the whaling scams are designed to masquerade as a critical business email sent from a legitimate business body and business authority. The content of an email usually involves some kind of falsified industry wide concern and is meant to be tailored for executives.

III. PHISHING TECHNIQUES

A. URL manipulation

URLs are the web link (i.e., Internet addresses) that directs the netizens/users to a specific website. In phishing attacks, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com. Phishers use lobsterpot method of phishing and make the difference of one or two letters in the URLs, which is ignored by netizens. This makes a big difference and it directs users to a fake/bogus website or a webpage.

B. Filter evasion

This technique uses graphic (i.e., images) instead of text to obviate from netting such emails by anti-phishing filters. Normally, these filters are inbuilt into the web browsers. For example,

- Internet Explorer version 7 has inbuilt "Micro phishing filter." one can enable it during the installation or it can be enabled post installation. It is important to note that it is not enabled by default.
- Firefox 2.0 and above has inbuilt "Google Phishing filter," duly licensed from Google. It is enabled by default.

C. Website forgery

In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands. As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily. Another technique used in known as "clocked" URL domain forwarding.

D. Flash Phishing

Anti-Phishing toolbars are installed/enabled to help checking the webpage content for signs of phishing, but have limitations that they do not analyze flash objects at all, real website because anti phishing toolbar is unable to detect it.

E. Social Phishing:

Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.

- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.
- The victim calls the bank on the phone numbers displayed in the mail.
- The phone number provided in the mail is a false number and victim gets redirected to the phisher.
- Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank.
- Phisher gets the required details swimmingly.

F. Phone Phishing

We have explained "Mishing"- mobile phishing attacks ("Vishing" and "Smishing"). Besides such attacks, phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and password.

Numerous different types of phishing attacks have now been identified. Some of the more prevalent are listed below.

IV. TYPES OF PHISHING SCAM

A. Deceptive Phishing

The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

B. Malware-Based Phishing

Malware based phishing refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

C. Keyloggers and Screenloggers

Keyloggers and Screenloggers are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.

D. Session Hijacking

Session Hijacking describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

E. Web Trojans

Web Trojan is a pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.

F. Hosts File Poisoning.

When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of SMB users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen.

G. System Reconfiguration Attacks

System reconfiguration attacks modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankxyzb.com" to "bancxyzb.com"[4].

H. Data Theft.

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

I. DNS-Based Phishing ("Pharming")

Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's host's files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result: users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website.

J. Content-Injection Phishing

Content injection phishing describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

K. Man-in-the-Middle Phishing

Man in the middle phishing is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system [5].

L. Search Engine Phishing

Search engine phishing occurs when phishers create websites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.

V. PREVENTIVE MEASURES

The best way you can protect yourself from phony phishers is to understand what legitimate financial service providers and respectable online auction houses will and will not do. Most importantly, legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as email.

Follow these five simple steps to protect yourself from phishers:

A. Pick Up the Phone to Verify

Do not respond to any emails that request personal or financial information, especially ones that use pressure tactics or prey on fear. If you have reason to believe that a financial institution actually does need personal information from you, pick up the phone and call the company yourself — using the number in your rolodex, not the one the email provides!

B. Do Your Own Typing

Rather than merely clicking on the link provided in the email, type the URL into your web browser yourself (or use a bookmark you previously created). Even though a URL in an email may look like the real deal, fraudsters can mask the true destination [6].

C. Beef Up Your Security

Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for those who engage in online financial transactions. Make sure your computer has the latest security patches, and make sure that you conduct your financial transactions only on a secure web page using encryption. You can tell if a page is secure in a couple of ways. Look for a closed padlock in the status bar, and see that the URL starts with "https" instead of just "http."

Security Tip: Some phishers make spoofed websites which appear to have padlocks. To double-check; click on the padlock icon on the status bar to see the security certificate for the site. Following the "Issued to" in the pop-up window you should see the name matching the site you think you're on. If the name differs, you are probably on a spoofed site [7].

D. Read Your Statements

Don't toss aside your monthly account statements! Read them thoroughly as soon as they arrive to make sure that all transactions shown are ones that you actually made, and check to see whether all of the transactions that you thought you made appear as well. Be sure that the company has current contactinformation for you, including your mailing address and email address.

E. Spot the Sharks

Visit the website of the Anti-Phishing Working Group at www.antiphishing.org for a list of current phishing attacks and the latest news in the fight to prevent phishing. There you'll find more information about phishing and links to helpful resources.

Share personal E-Mail address with limited people and/or on public websites- the more it is exposed to the public, the more spam E-Mails will be received.

There is other some preventive measures are following:

- Never reply or open any spam emails. Any spam emails that are opened or replied to inform the phishers not only about your existence but also about validity of your email address.
- Disguise the email address on public website or groups by spelling out the sign "@" and the DOT (.); for example, TapasATgmailDOTcom. This usually prohibits phishers to catch valid email address while gathering email address through programs.
- Use alternate email address to register for any personal or shopping website. Never ever use business email address for these sites but rather use email address that is free from yahoo, Hotmail or Gmail.
- Do not forward any emails form unknown recipients.
- Make a habit to preview an email before opening it.
- Never use email address as the screen name in chat groups or rooms.
- Never respond to a spam email asking to remove your email address from the mailing distribution list. More often it confirms to the phishers that your email address is active.

VI. CONCLUSION

Phishing differs from traditional scams primarily in the scale of the fraud that can be committed.

In order to combat phishing, business and consumers need to adopt best practices and practice awareness, educate themselves about phishing and anti-phishing techniques, use current security protection and protocols, and report suspicious activities. By doing so, they can reduce their exposure to fraud and identity theft; safeguard their confidential sensitive data from cyber-criminal. The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy.

ACKNOWLEDGMENT

We would take the opportunity to thankAdvocate Rajarshi Rai Choudhury, LL.B (Cal) D.I.T.L (Pune) for providing us with all the necessary facilities to make our article work and of worth. We thank Birla Institute of Technology, Mesra, Kolkata Campus for paying a pivotal and decisive role during the development of the article.

REFERENCES

[1] Markus Jakobsson and Steven Myers.Phishing and countermeasures: understanding the in-creasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.
[2] http://www.fbi.gov/sandiego/press-releases/2013/fbi-warns-of-spear-phishing-e-mail-with-missing-children-theme.
[3] http://cybercrime.org.za/scareware
[4] http://www.sec.gov/investor/pubs/phishing. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
[5] http://www.pcworld.com/article/135293/article.html
[6] http://www.encyclo.co.uk/define/System%20Reconfiguration%20Attacks.
[7] https://www.tradestation.com/site-wide-items/disclaimers/legal/online-security/online-identity