Phishing: A Technology Trap

Gagandeep Chawla
Research scholar, Punjab Technical University, Kapurthala, India.
Contact number: 9988750200 E-mail: gagan.rang@gmail.com

Dr.Neeraj Sharma
Dean & Professor, Gian Jyoti School of Management, Banur, District Patiala, India.
Contact number: 9814837880 Email: nrjsharma@yahoo.com

Abstract

"Phishing" is a social engineering attack and the panic word that scares every internet user, banks, companies and many other organizations. Internet fraudsters imitate a website or business to trick the people into giving out their personal, banking, and other credential information. Once they succeed to get users credentials and sensitive information they can misuse it by any mean. Legitimate businesses never ask anybody to send sensitive information through insecure channels. Due to lack of awareness and knowledge the graph of phishing scams and malware attacks is increasing dramatically, resulting financial and emotional loss and affects psychologically also. However, today more and more ways are trying to be found and new technologies are being devised to deal with the phishing and malware attacks. This is being achieved through the use of various legislations and cyber laws along with training people how to detect and deal with such attacks.In this paper the best available detection and prevention techniques are being proposed to prevent from becoming the victim of phishing or a malware attack.

Keywords: Phishing, APWG, CERT, Phish Tank, Phish Guru.

I. Introduction:

After decades of having the Internet, surprisingly most of the e-mails and information is being sent and received insecurely through the World Wide Web. This negligence and insecurity over the internet is the main cause of phishing and malware attacks. Online frauds and scams is a growing problem on the Internet as people are tricked into providing personal information including credit card numbers, passwords, bank account numbers and ATM pass codes. The most common way that phishers attempt to gain access to the sensitive information is by creating "look-a-like" websites that resembles like the original websites or by sending an email or instant message to the Internet or mobile users [14]. Recipients of these fake e-mails are requested to click on these links and to

provide their personal and credential information. After getting the enough personal information from victim, cyber criminals then can commit a variety of fraudulent and other criminal activities in the victim's name. Phishing is a global problem now and number of anti-phishing activities and awareness camps are going on to reduce its graph.The best way to someone can protect himself from phishing scams is to avoid supplying personal information to an email request. In order to avoid being victim, user should take proper security precautionsevery timehe/she on the Web [8]. Virus protectors and firewalls do not catch most phishing scams because they do not contain suspect code, while spam filters let them pass because they appears to come from legitimate sources[16].

II. Phishing scams; some illustrations:

Given below are the few cases demonstrating phishing scams. They basically make us aware of the said pattern mails which could be a sign of phishing. So the user should always be careful and cautious whenever he/she come across such types of mails.

(i) Case 1: In this example a forgery email is received from Income tax department of India for the settlement of refund and asking to click on the link "CLICK HERE" to submit a request.

As Part of Our Duty to Usher You, we have reviewed your tax fiscal payment for previous years and have resolved that you are qualified for a refund settlement of the sum of 36,120.25 INR which is your accumulated tax excesses. Please submit a tax refund request and allow us to process it within 7(seven) working days.

To submit a request CLICK HERE
Refund can be delayed for some reasons:

- Applying after deadline of notification.
- Submitting incorrect account information.

Tax Refund Department
Department of Revenue,
Ministry of Finance,
India.

(ii) Case2: Another very popular e-mail scam received by almost every e-mail user is Lottery scam. You might receive messages that claim that you have won the lottery of $50,000. These messages might even look like they come from a legitimate source. So if ever you receive these kinds of e-mails, delete themimmediately. A demonstration of such type of e-mail is given below.

THE LOTTERY DEPARTMENT BMW Automobiles
22 Garden Close, Stamford,
Lincs, PE9 2YP, London
United Kingdom

Dear Winner,

This is to inform you that you have been selected as a winner for a cash prize of £450,000.00 (Four hundred and fifty thousand Great British Pounds) and a brand new BMW 5 Series Car from International programs held on the 8th of 2012 in London Uk. Description of prize vehicle is given below;

Year: 2009
Model: 530iA
Colour (exterior/interior): Black Sapphire Metallic/Black Leather
Mileage: 5
Transmission: Automatic 6 Speed
The selection process was carried out through random selection in our computerized email selection ballot system from a database of over 250,000 email addresses from which you and nine others were selected as the winners.To begin the processing of your prize you are to contact our fiduciary claims agent for more information as regards procedures to claim your prize.

BMW LOTTERY DEPARTMENT UK
7 DOCK WAY, SEFTON BUSINESS PARK
LONDON, T40 4RT
United Kingdom

Contact him by please providing him with your secret pin code x7pwyz2005 and your Reference Number BMW: 2551256003/23.You are also advised to provide him with the under listed information as soon as possible:

1. Name:
2. Address:
3. Contact number:
4. Name of Bank:
5. Bank account number:
6. Netbanking password:

III.Facts and Figures:

(i) Phishing sites detected from October – December 2014: According to the APWG (Anti Phishing Working Group) reports of 4th quarter of 2014, total 46,824 phishing sites were observed in 4th quarter. This number is comparatively lower than in Q3 by roughly half. The following chart shows the unique phishing sites detected from October to December 2014. There has been a recent increase in Potentially Unwanted Programs such as spyware, adware and other such type of programs.

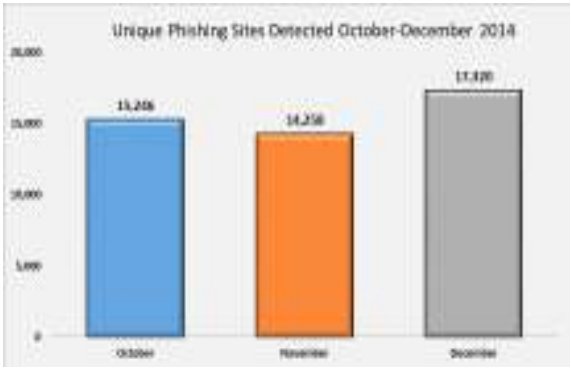

Figure 1- Source: Anti Phishing Working Group.

The Anti-Phishing Working Group continues to enhance its tracking and reporting methodology to overcome phishing related problems. APWG additionally tracks crime ware instances as well as unique sites that are distributing crime ware. The APWG Phishing Activity Trends Report also includes statistics on rogue anti-virus software, desktop infection rates, and related topics. [2]

(ii) Statistical Highlights for 4th Quarter 2014:

	October	November	December
Number of unique phishing websites detected	15,246	14,528	17,320
Number of unique phishing e-mail reports (campaigns) received by APWG from consumers	68,270	66,217	62,765
Number of brands targeted by phishing Campaigns	271	273	300
Country hosting the most phishing websites	USA	USA	USA
Contain some form of target name in URL	44.88%	50.40%	50.37%
Percentage of sites not using port 80	0.72%	0.35%	1.04%

Table 1 - Source: Anti Phishing Working Group.

(iii) Most Targeted Industries: The following Pie chart shows that the most targeted industries. Retail Service was the most-targeted industry in the fourth quarter of 2014, with 29.37% of phishing sites. The United States again continued to be the top country in hosting phishing sites during the third quarter of 2014. This is mainly due to the fact that a large percentage of the world's Web sites and domain names are hosted in the United States.

Figure 2 - Source: Anti Phishing Working Group.

IV. Major factors for increase in Phishing Attacks:

Presence of phishing has been around for over 18 years now, and yet, the world has not been able to rid itself of this phenomenon [14]. There have been major increases in phishing attack volume in some countries, while slight declines were recorded for others. One of the most significant increases was seen in Canada, where phishing increased nearly 400% in

the first half of 2012. Main reason is simply economics – fraudsters follow the money. With the Canadian and U.S. dollar being exchanged at nearly a 1:1 ratio, Canada has become a lucrative target for cybercrime. There are another three major factors behind flourishing the phishing attacks worldwide aregivenbelow. [13]

(i) Unawareness among public: Worldwide, particularly in India, there has been lack of awareness regarding the phishing attacks among the common masses. The users are unaware that their personal information is actively being targeted by criminals and they do not take proper precautions when they conduct online activities. [13]

(ii) Unawareness of policy: The fraudsters often count on victim's unawareness of Bank/financial institution policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation. Customers unaware of the policies of an online transaction are likely to be more susceptible to the social engineering aspect of a phishing scam, regardless of technical sophistication. [13]

(iii) Technical sophistication: Fraudsters are now using advanced technology that has been successfully used for activities such as spam, distributed denial of service (DDoS), and electronic surveillance. Even as customers are becoming aware of phishing, criminals are developing techniques to counter this awareness. These techniques include URL obfuscation to make phishing emails and web sites appear more legitimate, and exploitation of vulnerabilities in web browsers that allow the download and execution of malicious code from a hostile web site. [13]

V. Tools and tips to protect people from Social engineering and phishing scams:

Phishing scams are usually presented in the form of spam or pop-ups and are often difficult to detect. Once the fraudsters obtain users credential information, they can misuse it by any mean. Because phishing is one of the most errant forms of identity theft, it is important for user to become familiar with various types of phishing scams as well as to learn how to guard against them. To help protect the people from phishing, following tips are offered:

(i) If ever a person receive an e-mail that asks to enter or update information and it seems to be from some legitimate source, go to the website by typing the URL in browser's address field instead

of clicking the link in the e-mail. For example, go to https://www.onlinesbi.com" instead of clicking the link in an e-mail that appears to come from SBI bank.

(ii) If a person uses netbanking, online shopping or makes any online transactions, look for a lock sign on the left side of the address bar and it always appears "https:" rather "http:" in the URL whereby the "s" stands for "secure".

(iii) Never reveal personal, banking or credential information over the phone until unless a user initiates the call and be cautious of any emails that ask to call a phone number to update account and any other information.

(iv) To avoid malware attacks do not open or download files, attachments in emails from unknown senders. It is best to open attachments only when user is expecting them and know what they contain.

(v) If someone frequently uses netbanking or makes online transactions, try to use virtual browsers which are easily and free of cost available online.

(vi) Adopt proper defence system such as anti-phishing tools, firewall, spam filters, anti-virus and anti-spyware software's. Update them all regularly to ensure blocking of new viruses and spyware.

(vii) Beware of submitting name, email address, or other personal information on a website, look for the site's privacy policy. This policy should state how the information will be used and whether or not the information will be distributed to other organizations.

(viii) To protect attackers from hijacking the information, any personal information submitted online should be encrypted so that it can only be read by the appropriate recipient. Many sites use SSL, or secure sockets layer, to encrypt information.

(ix) Check online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.

(x) Change the net banking and other valuable passwords regularly.

VI. Anti-phishing organizations:

Number of national and international consortiums is there to fight phishing and malware attacks. These groups are working for welfare of internet users and developing a way to freeze e-crimes. The challenge which these organizations are facing is a lack of a coherent reporting system.

(i) Anti-Phishing Working Group: Founded by Tumbleweed Communications in 2003 is an international consortium operates as a tax-exempted and non-profit global organization to fight against phishing and on-line frauds. The APWG provides a forum of opinions as well as mechanism for the dissemination of best practiceswhich can be deployed against phishing. As online criminals seek new ways to gather personal information, the APWG holds summit to counteract the latest trends. In June, 2004 APWG was incorporated as an independent corporation controlled by its board of directors, its executives and its steering committee. APWG publishes monthly reports containing statistics on phishing aiming at measuring the scale of the threat. [2]

(ii) Phish Tank: PhishTank is another consortium and a free community website where anyone can submit, verify, track and share phishing data. Also, PhishTank provides an open API (Application Programming Interface) for developers and researchers to integrate anti-phishing data into their applications at no charge.PhishTank is an information clearinghouse, which helps to pour sunshine on some of the dark alleys of the Internet. PhishTank is free to everyone, both the website and the data (via the API) and registration with phish tank helps make the data better. After completing the free registration, net user can send emails to phish@phishtank.com from the registered email address. It is important to include as much information as possible, including mail headers if possible. For that reason, we suggest redirecting any suspected phishes to PhishTank.

(iii) PhishGuru: PhishGuru is a software-as-a service product developed by Wombat security technologies founded in June 2008 used to assess and train employees with simulated phishing emails.Scientific studies show that employees don't pay attention to classroom or video security training and they don't retain the information learned. That's why PhishGuru is uniquely effective. PhishGuru lets the company to assess and train their employees by sending simulated phishing emails. When an employee falls for the simulated attack, it creates a unique "teachable moment" when employees are open to learning. Employees are immediately presented with training that explains what happened and how to avoid similar attacks in the future. PhishGuru anti-phishing training simulations have been able to reduce the likelihood of a user falling for an attack by 60% in just one campaign.The latest version of PhishGuru also reveals whether an employee fell for an attack through a mobile phone, a tablet, or their computer, and specifically what type of device or browser they were using.

VII. Reporting phishing attempts:

The www.apwg.org and www.phishtank.com are two most common anti-phishing websites who collects, analyses, and exchanges lists of spoofe-mails, websites or any criminal activities. One easy way to do this is to simply forward the suspected phishing email to reportphishing@apwg.org or phish@phishtank.com. Apart from this net user can also follow the following written steps to report phishing attempt

(i) User can report a phishing scam attempts or malware attack to the company directly that is being spoofed.

(ii) If a user receivesfake e-mail or any type of offer which ask to provide credential information, the message can be forwarded to the Federal Trade Commission at spam@uce.gov.

(iii) US-CERT (United States Computer Emergency readiness team) also collects phishing email messages and website locations to avoid becoming victims of phishing scams.User can report phishing US-CERT by sending email to phishing-report@us-cert.gov

(iv) If the suspicious mail in question includes a file attachment, it is safer to simply highlight the message and forward it. Some configurations, especially in Windows environments, may allow the execution of arbitrary code upon opening and viewing a malicious email message.

(v) If a net user is using Internet Explorer and is on a suspicious site, click the gear icon and then point to Safety. Then click Report Unsafe Website and use the web page that is displayed to report the website.

(vi) Depending on location, some local authorities also accept phishing scam reports

VIII. Actions followed after being a victim of a phishing attack:

If the user suspects that he/she have responded to a phishing scam with personal or financial information, take these actions to minimize any damage and to protect identity.

(i) Immediately change the passwords or PINs of all online banking accounts that might be compromised.

(ii) Contact the bank or the online merchant directly. Do not follow the link in the fraudulent email message.

(iii) Place a fraud alert on credit reports. Check with bank or financial advisor if someone not sure how to do this.

(iv) If any account that was accessed or opened fraudulently, close that account.

(v) Routinely check bank and credit card statements monthly for unexplained charges or inquiries that a user didn't initiate.

IX. Cyber Offences and Laws:

Under the Information Technology Act, 2000(as amended by Information Technology (Amendment) Act 2008), Ministry of Law, Justice and company affairs of India provides the legal provision for any unfair means conducted by an individual or company. Anyone who destroys deletes or alters any information by any meanswith intent to cause damage to the public or private system commits cybercrime.The person who commits cybercrime or hacking shall be punished with imprisonment up to three years and fine according to crime committed. According to the National Crime records bureau, 233 people were arrested in 2010 under this information technology act with majority of these crimes beingthat of forgery or fraud.

X. Conclusion:

Technology makes the things easier but a user has to be aware of the threats and dangers that can be paused by the misuse of technology and hence cause financial and other loses. This paper shows that phishing, a type of network attack poses similar threats to network users. Though the service providers are finding ways to safeguard their users from getting befooled by the phishing attacks, but all these methods prove no more useful if the user is not cautious. Awareness among users is must and they should put a cross to their curiosity factor that makes them open the phishing mails and hence become victim of these attacks. If somehow users have been trapped in this technology trap, awareness regarding the necessary actions and reporting to the anti-phishing organizations should be clear and followed. Technology like network is a boon for the users, but lack of awareness can turn it to a curse. So be aware for these kinds of attacks and surf the net safely.

References:

[1] "A new Anti-phishing method in Open ID" by Hwan Jin Lee. *IEEE 25-31 Aug 2008*.

[2] "Virtual Browser: An On-Demand Service to Prevent Phishing Attack" by Swapan Purkait.

[3] "Online detection and prevention of phishing attacks" by Juan Chen, Chuanxiong.

[4] http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

[5] "Technical trends in phishing attacks" by Jason Milletary.

[6] "Angeling for phishers: Legislative responses to Deceptive E-mail" by Jasmine E. McNealy

[7] "Textual and Visual Content–Based Anti-Phishing: A Bayesian Approach" by Haijun Zhang, Gang Liu.

[8] "Global Phishing Survey: Domain name use and trends in 2H2011" by Greg Aaron and Rod Rasmussen. Available athttp://antiphishing.org

[9] "Anti phishing Technology"Technical white paper by Kasper sky lab. Available at www.antiphishing.org

[10] "The cost of phishing: Understanding the True Cost Dynamicsbehind Phishing Attacks" by Cyveillance.Available at www.antiphishing.org

[11] "Botnet Threats and Solutions: Phishing" by TrendMicros's.

[12] "Vulnerability of First-Generation Digital Certificates and Potential for Phishing Attacks and Consumer Fraud" by GeoTrust

[13] "Phishing Scams in India and Legal Provisions" by Neeraj Arora.

[14] "The Perpetration and Prevention of Cybercrimes" by Stanley Kratchman , Jacob Lawrence Smith and Murphy Smith.

[15] "Legal risk for fishing researchers" by Christopher Soghoian.

[16] "Impact of Cybercrime on Virtual banking" by Subramoniam Arumuga Perumal.

[17] "Privacy and the information technology act in India" by Prashant lyengar.

[18] "A Review of the Economics of Information Security Literature" by Mike Hammock.

[19] "Phishing and Man in the Middle Attacks" by Adity Vinay Mahajan.

[20] "Spear-Phishing Email: Most Favored APT Attack Bait" by Trend Labs SM APT Research Team.

[21] "www.wikipedia.com" An online encyclopaedia.

[22] "www.apwg.org" An Anti-phishing working group.

[23] "www.esecurityplanet.com" A website which publishes e-security and IT related news.

[24] "www.phishtank.com" An open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

[25] "Strategies for Securing the Cyber Safety Netfor Terrorists: A Multi-Disciplinary Approach" by Doris Estelle Long.