Analysis of user Responses to Phishing Attacks

Ms. Daljit Kaur [1] , Dr. Parminder Kaur[2]
[1]Department of Computer Science and IT, [2]Department of Computer Science Engineering

***Abstract*-** **Phishing, the act of stealing personal information via the internet for the purpose of committing financial fraud, has become a significant criminal activity on the internet. The term "phishing" has origins in the mid-1990s, but now days the term has evolved to encompass a variety of attacks that target personal information. This paper gives brief about phishing , its techniques, and maps them to anti–phishing techniques. Furthermore , we analyzed the anti-phishing databases and conducted survey to know the awareness of phishing among internet users.**

1. INTRODUCTION

Phishing is a form of social engineering attack 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].It is the act of attempting to acquire information such as usernames, passwords, credit card details or other personal details by sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations. Tricking others into giving out passwords or other sensitive information has a long tradition in the attacker community. The first recorded term "phishing" is found in the hacking tool AOHell, which included a function for stealing the passwords or financial details of America Online users [2]. A complete phishing attack has three steps for phishers as shown in figure1.

Send out a large number of fraudulent emails which direct users to fraudulent websites. Set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. [3]

According to a research report, phishing attacks cause extensive collateral financial damages such as ruining brands'

reputation after hacking. These damages continue to rise with increasing sophistication[4].

This research paper is about phishing , it gives brief of phishing and anti-phishing techniques available to both attackers and users of the Internet. Also it shows the analysis result of anti-phishing databases, survey results from internet users. This paper is structured as follows:

Section 2 describes the types of phishing attacks, Anti phishing tips and their mapping to phishing attacks. Section 3 shows the Anti phishing database analysis and survey results. Section 4 gives information about anti phishing reporting and Section 5 concludes the paper and briefs future work that could be done.

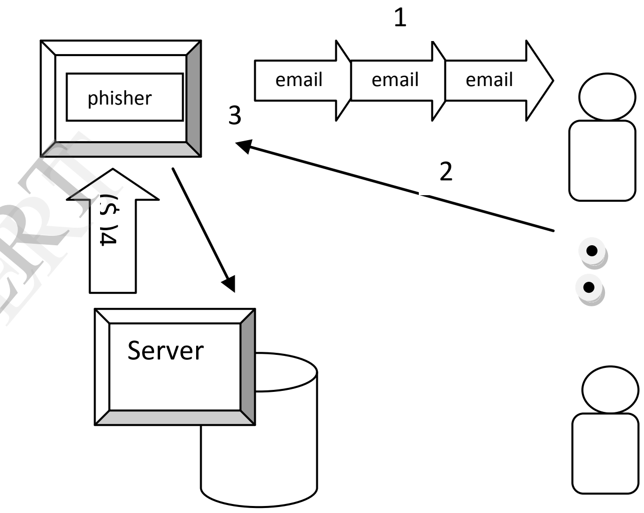


Figure1:Phishing process

2. PHISHING AND ANTI-PHISHING TECHNIQUES

Different techniques have been developed to conduct phishing attack and to make them less suspicious. Such techniques make the recipient believe in the fraud message and take action according to its instructions. Malware are installed into victims' computer to collect information directly or aid other techniques [3,15]. Phishing has spread to emails, VOIP, SMS, instant messaging, social networking sites and even multiplayer games. Some major categories of phishing are discussed below:

1)Spear Phishing : In this type of phishing attack, phisher focuses on a single user or department within an organization and requesting information such as login IDs and passwords. Such scams often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. [3,5]

Once phisher get this data he can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can thieve data [6,14]. Spear phishing attacks often target high profile individuals within organizations who typically have extensive or deep access to sensitive information. This is known as "*Whale Phishing*" or *"Whaling"*. Sometimes, the whaling email claims to be from the Better Business Bureau, seeking to confirm a complaint against the target company. [6]

2)Clone Phishing: In this phishing attack a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken by phisher and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a re-send of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email [3,7].

3) Deceptive Phishing: In this technique, phishers use social engineering to steal victims' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails to lure unsuspecting victims into counterfeit Websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers [8]. 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.

4) Malware-Based Phishing : This type of phishing involves 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 [9]. *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.[9,10]

5) Session Hijacking: In this type of attack, 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. [9]

6) Web Trojans: Web Trojans pop up invisibly when users are trying to log in. They collect the user's credentials locally and transmit them to the phisher [5].

7) Hosts File Poisoning: Pharming is the other name given hosts file modification or Domain Name System *(DNS)-based phishing*. 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 to a fake "look alike" website. [3, 10]. As a 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 [3].

8) System Reconfiguration Attack: This attack modifies settings on a user's PC for malicious purposes [9]. For example: URLs in a favorites file might be modified to direct users to look alike websites.

9) Data Theft: Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors [10]. sInsecure PCs that contain subset of sensitive information are used to access servers and can be more easily compromised.

10) Content-Injection Phishing: In this type of phishing technique, phishers 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.[10] They may insert malicious code to get user's credentials or an overlay which can secretly collect information and deliver it to the phishing server.

11) Man-in-the-Middle 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]. This type of attack is harder to detect than many other forms of phishing.

12) Search Engine Phishing: In this technique, 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[10].

2.1 Anti-Phishing Techniques

Phishing scams are more dangerous than the social ones [12]. Phishing can be prevented by following few anti-phishing techniques. Information about known phishing attacks is available online from groups such as the Anti Phishing Working Group (APWG). Report phishing to such anti phishing groups (shown in section IV). The Anti-Phishing Working Group, a group of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing. Below are few anti phishing techniques, and also mapping of phishing attacks to anti phishing is shown in table1.

a. Check the Sender's Full Email Address
b. Check the Attachment File Type Closely
c. Check for Vague Filenames
d. Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.
e. Beware of links in emails that ask for personal information
f. Never enter personal information in a pop-up screen
g. Be skeptical of any unsolicited electronic requests for you to verify or update account information, or to click on or download information – even if it appears to come from a known business or organization
h. Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
i. If you are suspicious of a website, close it and contact the company directly.
j. Do not click links on social networking sites, pop-up windows, or non-trusted websites. Verify the web address begins with “https://” (the “s” is for secure) rather than just “http://”
k. Avoid using websites when your browser displays certificate errors or warnings.
l. Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don’t ask for sensitive information through email or text messages.
m. Beware of visiting website addresses sent to you in an unsolicited message.
n. Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
o. Try to independently verify any details given in the message directly with the company.
p. Utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.
q. Do not open attachments received from unknown senders or unexpected attachments from known senders.
r. Be cautious of the amount of personal information you make publicly available through social networking sites and other methods. The more information publicly available Communicate personal information only via phone or secure web sites. Never email personal or financial information, even if you are close with the recipient
s. Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software
t. Keep a clean machine.
u. Having the latest operating system, software, web browsers, antivirus protection and apps are the best defenses against viruses, malware, and other online threats.

PhishingTechnique	*Anti Phishing Technique*
Spear Phishing/ Whaling	a,o,p,q
Clone Phishing	a,e,h,i,o,p
Deceptive Phishing	e,f,p,s,l
Malware-Based Phishing	b,c,r,t
Session Hijacking	d,u
Web Trojans	f,g
Hosts File Poisoning/ Pharming	f,g,h,j,m,n
System Reconfiguration Attack	t,u
Data Theft	t,u
Content-Injection Phishing	f,g,,j,k
Man-in-the-Middle Phishing	s,d
Search Engine Phishing	o,p

Table 1: Mapping of Phishing to anti-phishing

3. ANALYSIS, SURVEY AND RESULT

We analyzed phishing database "*PhishTank", "FraudWatch*" for 30 days continuously. PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, it provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge [11]. It offers a community-based phish verification system where users submit suspected phishes and other users "vote" if it is a phish or not. Whereas FraudWatch is a privately owned Internet Security company. Each month, FraudWatch takes down thousands of phishing sites, Malware sites, fake Domains, Social Media Profiles and fake Mobile Apps. It provides the best site take down times in the industry [16]. It lists small subset of some recent phishing attacks.

From these databases we analyzed that most targeted brands are related with the financial transactions. The result is shown in table 2.

Top Ranking	*Brand Name*	*Sphere of activity*
1	PayPal	Internet Payment
2	Bank (Bank Of America, Union Bank of Philippines, Chase Bank, others)	Financial Transactions
3	Amazon	Online retailer
4	ebay	Online shopping

Table 2: Most Targeted Brand

Other key finding was that on average 1,752 links are submitted to verify it as a Phish on PhishTank and for most of the phishing websites, it takes not more than 2 days downtime.

Survey was launched on *www.esuveysPro.com* for 30 days and it got 65 responses in total which tells that only 20% people know the term phishing though they are well qualified and daily use Internet for different purposes. 80% people said that they receive spam e-mails in their inbox (as shown in figure 2) and among those 41.67 % said that such emails contain the links which contains some IP address and special characters like % , @,etc.

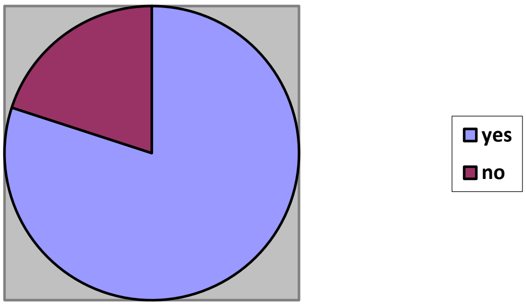


Figure 2: Receive spam emails in inbox

Also a study was designed for the participants and 26 participants took part in it. We presented participants with websites that appear to belong to financial transactions, retailing, social networking some spoofed and some real. The participants task was to identify fraudulent and legitimate sites and mention their decision, rate their decision and describe the reasoning for their decision. We presented 10 websites and among those only 2 were legitimate but many participants were found wrong in this study, and result are shown in table3.

Website	*Real or Spoof*	*Participants Decision(%ge)*	
		Real	*Spoof*
http://clientesfilesminersmi.zz.mu/	Spoof	12	88
http://www.onlinepnb.net/	Spoof	77	23
https://www.paypal.com/webapps/mpp/paypal-payments-advanced/	Real	72	28
https://twitter.com/i/redirect? url=https%3A%2F%2Ftwitter.com%2Fi%2F387….	Spoof	88	12
http://paypal-challenge.net/63645/index.php	Spoof	37	63
http://www.sicherheitpaypal.de.vu	Spoof	28	72
https://www.onlinesbi.com/	Real	80	20
http://paypal-challenge.net/63645/index.php	Spoof	25	75
http://finance-reports.com-nbc24.com/business/2013/..	Spoof	23	77
http://www.faceb0ok.com	Spoof	10	90

Table3: website study

When the participants were asked to ranked their decision, none was very confident and most of the participants were not sure about their judgment about the websites legitimacy as shown in figure 3. Many participants reported experiencing confusion about whether a site is legitimate or not.

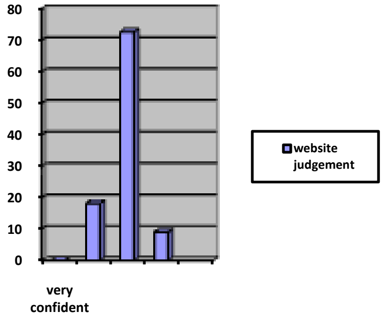


Figure 3: judgment confidence

Phishers use various strategies to deceive users and the users use different techniques to determine the legitimacy of the websites. But the users who lack technical knowledge or/and who lack attention get fooled easily. When participants were asked that what method they used for determining the legitimacy, their responses were as shown in figure-4.

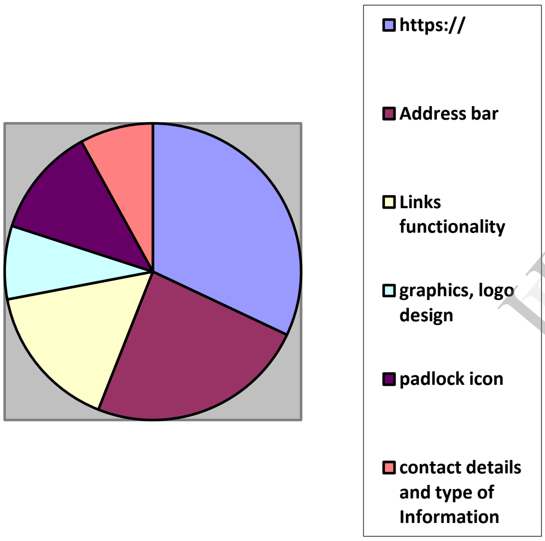
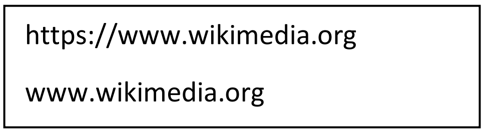


Figure4: website legitimacy techniques

Maximum participants (32%) consider that when browser send request beginning with "https://", it is the indication of a secure site, but only 24% said that they pay attention on the address bar which shows the lack of attention. In total 16% participants check for the functionality of the links on site and content, which means 84% can be fooled very easily even with partially functioning site or little efforts. 8 % participants said that they assume a site legal if it has original looking logos, images and graphic design, which indicates their lack of technical knowledge that how attackers can mimic original website. 88% do not know that closed padlock icon in the browser indicates that the page they are viewing was delivered securely by SSL(Secure socket Layer) and even they are not aware about its correct position in browser. So designers can easily fool users by placing padlock icon in the content of webpage. Figure 5 shows the google chrome's address bar when visiting the wikimedia's page with or without padlock icon. Only 27.27 % participants were aware that their browser has the functionality to prevent phishing.


https://www.wikimedia.org

www.wikimedia.org

Figure 5: Wikimedia site

In other research, it was found that, 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time [13]. It was surprising fact that only 18.18% strictly do not open a link or site when it prompts some kind of warning or error message but rest of the users sometimes or many times ignore warnings and continue with suspicious links. More surprisingly, there are 37% users, who use same password for multiple sites. They admitted it for their yahoo, gmail, facebook, and other social networking sites, which makes attackers task easier as just knowing one password can give them lots of personal information. 36. 4 % users assume that any link if it asks for only username and password, it can not be fraud but 54.5% users consider a site fraud only when it asks for credit card information, 36.4% said that it creates a doubt in their mind about the site legitimacy but they are not sure.

When people receive suspicious emails in their inbox, 87% of them said that they open when it seems from a known person and 50% said that they open it even it is from unknown sender but the subject is very interesting. Figure 6 shows the user' actions with the suspicious e-mails in their inbox.

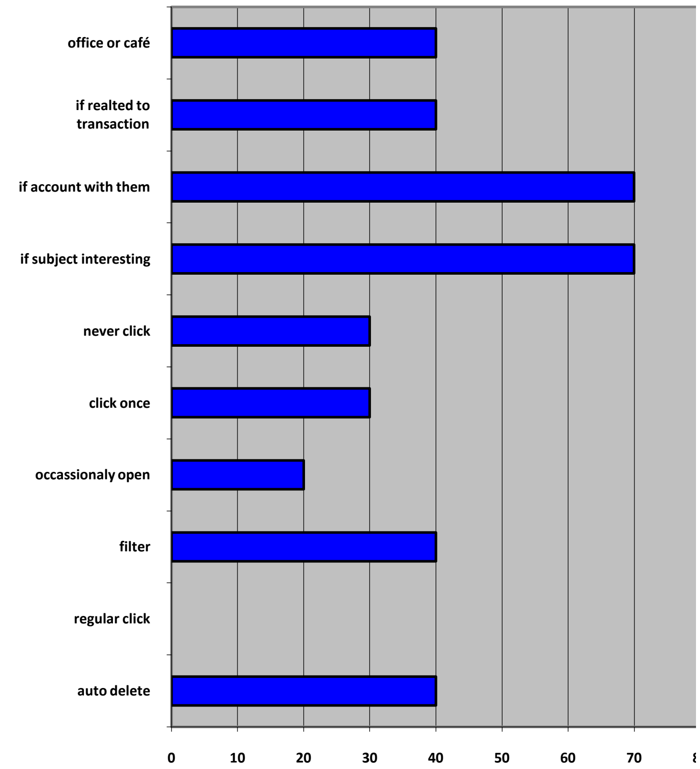


Figure 6: Actions with suspicious e-mails

4.ANTI PHISHING REPORTING

If anyone faces some phishing attack or finds some phishing site or link, it should be reported to some anti-phishing group. Such Anti-phishing groups brings that site or link down and save the others from getting deceived. Information about known phishing attacks is made available online on these groups. So do report phishing to any of these anti phishing groups as these groups, ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing . List of few Anti-Phishing groups is as below:

www.antiphishing.org(APWG)
www.phishtank.com (Phishing Tank)
www.digitalphishnet.org (Digital Phishnet)
www.onguardonline.gov/phishing
www.us-cert.gov/report-phishing
www.submit.symantec.com/antifraud/phish.cgi
www.netcraft.com/
www.consumer.gov/idtheft/ (Federal Trade Commission)
www.ic3.gov (Internet Crime Complaint Center - a joint project of the FBI and the National Collar Crime Center)
antifraud@support.trendmicro.com (Trend Micro Anti-Fraud Unit)

5. CONCLUSION AND FUTURE WORK

Mostly users get deceived because of their lack of technical knowledge and lack of awareness and attention. In order to prevent phishing, users need to adopt best techniques, more awareness, educate themselves about phishing and anti-phishing techniques, use current security protection in browsers and protocols, and report suspicious activities to anti phishing groups. By doing so, they can reduce their exposure to fraud and identity theft, safeguard their confidential information, and help fight one of today's most serious and ongoing threats of phishing. The most effective solution is to educate users not to blindly follow links to web sites where they have to enter sensitive information such as passwords or other personal information and users must be paranoid. The final technical solution to phishing involves significant infrastructure changes in the Internet that are beyond the ability of any one institution to deploy.

6. REFERENCES

[1] M.Jakobsson, S.Myers, "*Phishing and countermeasures: understanding the increasing problem of electronic identity theft"*, John Wiley & Sons, Inc., 2007.

[2] Langberg and Mike," AOL Acts to Thwart Hackers", *San Jose Mercury News*. September 8, 1995.

[3] J Shi, S.Saleem , "Phishing", research report published *in CSc 566, Computer Security Research Reports*, University of Arizona, April 2012

[4] White paper-"The Cost of Phishing:Understanding the True Cost Dynamics behind phishing Attacks", *A Cyveillance, Report,* January 2010.

[5] Phishing and Pharming: A guide to understanding and managing Risks by *CPNI (Center for the Protection of National Infrastructure),* July 2010.

[6] "Phishing" article retrieved from *http://en.wikipedia.org/wiki/Phishing*.

[7] "Types of phishing", retrieved from *http://www.phishingbox.com/typesofphishingdefined.htm*

[8] H Huang, J Tan ,L Lui, "Countermeasure Techniques for Deceptive Phishing Attack" published in *International conference on New Trends in Information and Service Science, 2009. NISS '09*

[9] J Milletary, "Technical trends in Phishing attack", published in US-CERT, June 2012.

[10] Courtsey. ,Article on "Types of Phishing attack", September 2007 retrieved from *http://www.pcworld.com/article/135293/article.html*

[11] "What is phistank", retrieved from *http://www.phishtank.com/*

[12] A Ameen , Talab S.,"The Technical Feasibility and Security of e-voting", I*nternational Arab journal of Information Technology. July 2011*

[13] R. Dhamija, J. Tygar, M.Hearst , "Why Phishing Works", *CHI (Conference on Human Factors in Computing System), April 2006*.

[14] A Khan, "Preventing Phishing attack using one time password and user machine identification", *International Journal of Computer Applications* Vol. 68, issue 3, April 2013.

[15] J. Chhikara , R. Dahiya , N. Garg , M. Rani., "Phishing and Anti-Phishing Techniques: Case Study", *International Journal of Adnavce Research in computing science and Software Engineering* , Vol. 3 Issue 5, May 2013.

[16] Report retrieved from http://www.fraudwatchinternational.com