IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 01-08
www.iosrjournals.org

Phishing-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation

Phirashisha Syiemlieh[1], Golden Mary Khongsit[1], Usha Mary Sharma[2], Bobby Sharma[3]
Department of CSE & IT, Assam Don Bosco University, India

Abstract: *Phishing is a scam that has evolved many years ago and it has been growing ever since. In this study we have collected much information regarding its new and improvised way of scamming the users without their knowledge and concern. Some case studies are also included based on real life events. According to the report received from Home Depot Company, the United States and Canada had encountered a loss of $62 million where only $27million was covered by the insurance company but the rest is yet to be recovered. Our main aim is to let the users be informed of all the malicious crime created by the attackers. We have also listed out some of the preventive measures that a user should follow in order to prevent such crimes. Knowingly or unknowingly theusers are trapped by using this kind of attacks and the hackers always succeed to outsmart them by using new and different scams. This paper is an attempt to bring an awareness on the phishing types, causes and various preventive measures that can change the way how people reason about the hackers and their perception towards them.*

Keywords: *Phishing, Spoofing, Pharming, Spamming, Scams, Crook.*

I. INTRODUCTION

The word "phishing" originally came from the analogy of early internet criminals using lures to "fish" for passwords and financial data from a large sea of unsuspecting internet users. The use of the "ph" in this terminology has been forgotten about over time. It was most likely linked to hacker naming conventions such as "phreaks". [1]

Phishing refers to the process where a targeted individual is contacted by email or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details and passwords. The personal information is then used to access the individual's account and can result in identity theft and financial loss.[2] Phishing is the act of sending email that falsely claims to be from a legitimate organization. It is usually combined with a threat or request for information like that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the website to conduct fraud. It can also be defined as an act of circumventing or entrap security with an alias[2]

II. LITERATURE REVIEW

The word phishing itself has many meaning some say it is a brand-spoofing, carding, pharming, fraud attack, semantic attack but all in all it comes to the same thing that is it is an objective of the phisher to succeed in tricking the victims into giving away their password or account number or any kind of personal information which will be useful to the phisher.

According to the author in [3] on Phinding Phish, phishing has been described as a **semantic** attack where victims are being tricked into giving out their personal information to an illegitimate site. A solution to this has been created by creating toolbars which will give certain results as to whether the site is a legitimate one or not. So many types of anti-phishing toolbars have been developed and they are as follows:

- Cloudmark Anti-Fraud Toolbar
- Earthlink Toolbar
- eBay Toolbar
- GeoTrustTrustWatch Toolbar and many more.. [3]

[4]Phishing has even become like a business as the phishers earn millions of dollars by stealing from the victims and there are many groups of this abhorrence scam and mostly in Eastern Europe, Asia, Africa and the Middle East.

III. HOW DOES ONE START PHISHING?

- The attacker creates his or her own fake websites, taking the example of creating a fake facebook website phishing.php file which will collect all the form of data and index.html page.[5]
- The attacker will go to the Facebook page without logging in .[5]
- The attacker inorder to find a link will look for word action .[5]

Example:

- [1]Action=https://www.facebook.com/login.php? Login_attempt=1
- Then the attacker create an account on free hosting website like [5]
- ***http://www.ttt.com
- Then the attacker uploaded the php file and html page with his name then the phishing website is created.[5]
- The attacker can now start phishing.

IV. TYPES OF PHISHING

There are different types of phishing which have evolved during the past few years in which the attackers find new ways and means to scam the users with their innovative ideas and update themselves with the latest technology emerge in the market so as to make their sites look more convincing and certain than ever. The examples are as follows:

- **[6]Deceptive Phishing-** This will cause the user to be misled and make them believe what is not true. The attacker will proceed by sending an email to the user regarding their financial accounts and the problems they are facing in which they are not aware of sending them a link to update their passwords and other personal information and with this information they can now use it against the user.
- **[6]Malware-Based** Phishing- This will harm the software of the user especially if it is software used in a small firm when the software is not updated for a long time. The attacker does not gain anything by doing this but only filled his desire of watching others suffer often called as a malicious crime.
- **[6]Keyloggers and Screenloggers-** This is also a malware attack where the attackertracks the inputs from the keyboard which he will send the relevant information through the internet to the hacker on the other side.
- **[6]Session Hijacking-** It is a type of malware attack where the attacker has track the system of the user and everything has been monitored so when then user is log in to bank details or other information useful for the attacker it will then be taken over by the malicious software and used the information in transferring funds without the knowledge of the user. It is called session because it only takes place by sessions and not the whole time.
- **[6]Web Trojans-** Almost same as session hijacking but it is invisible to the user and pops up when the user logs in to any important website or performing any transactions and collects all the information that the user has filled and transmit them to the attacker.
- **[6]Hosts File Poisoning-** This will trick the user into thinking that they are logging into the correct website without knowing that they have been trick into logging into a fake website which looks exactly the same as the original website. This is done by poisoning the host file where theattacker had stolen the information.
- **[6]System Reconfiguration Attacks-** The settings in the system of the users are being modified intentionally so as to change the URL names present in the users favourites so that when they try to login to the required website they are actually logging in to a fake look alike site.For example, if the name of the site is statebankofindia.com it will be changed to statebangofindia.
- **[6]Data Theft-** As we can understand from the name itself it is the stealing of data from the system of any users most probably those working for the government or any competitive source in which the information stolen will harm the users when it is leaked publicly or cause financial loss. It can also be define as an act or practice of spying or in this case using technical spies to obtain secret information as about another government or a business competitor.

- **[6]DNS-Based Phishing ("Pharming") -** Domain name system also known as pharming is the kind of attack where users can identify websites with human readable names (e.gwww.gmail.com) and the system will take them as IP addresses. This DNS will uphold the mapping which includes the domain names and the IP addresses which can be traced everywhere.

- **[6]Content-Injection Phishing-** This is another form of phishing will insert harmful contents to a genuine site or network in which it will redirect the user to another fraud site or it can install a malware content which will direct the users to the attacker website.
- **[6]Man-in-the-Middle Phishing-** This is the type of phishing that is very hard to detect. In this case the attacker is between the user and the website and when the user is doing any transaction online that is when they take over and copy all the information and credentials of the user but they still provide the users with all the steps needed to be go through by the user so that they would not get suspicious and they will use the information later usually it is link with credit cards details, bank account details, etc..
- **[6]Search Engine Phishing-** Nowadays everything can be done online whether shopping, booking travelling tickets, advertising, etc. So e-commerce also takes place in the malicious tricks of the attackers they create these fake websites of different banks and giving attractive offers and when the users tried to take the offers displayed on the screen they have to fill all their personal information without knowing that they are actually being framed by the attackers.

V. DYNAMIC FEATURES FOR GROWING OF PHISHING ATTACKS

- [7]Lack of awareness among the users- Users is not so much aware of the sneaky and devious ways of the attackers.
- [7]Lack of knowledge towards policy- Users is not so familiar with the policies of online transactions which makes it more prone to phishing scams despite the technical elegance.
- [7]Technical modernization- The attackers always seem to upgrade themselves with the newest technology available in the market. Even if the users are very much aware of phishing the attackers are one step ahead of the users by developing new innovative techniques to counter this awareness.

VI. CAUSES OF PHISHING

According to the author of paper [8] the major cause of phishing has tremendously affected the innocent people as a whole with regards to accessing of different secret information that one has. It has results to one of the cause and this cause is known as damage CAUSE of phishing .It is known that in the year between 2004 and 2005 of May around 1.2 million of people in United States of America suffered from a great loss of business, which also states that in the year 2007 they have suffered up to $2billion losses annually and 3.6 million people lost US$3.2 billion in August 2007 as their workers become victims .[8]In the United Kingdom Microsoft declares that a major losses cause by fraud bankers almost from phishing is twice to GB£23.2million in the year 2005 and GB£12.2m in the year 2004.The cause of damage includes loss of important accounts e.g. online banking, online shopping, online investment, online payments of different bills etc. Phishing has spread widely with the rising number of unsuspected people which can be easily influenced by the agents of the attackers.[8]

The significant information consists of their card numbers, mother's name and other secret records. Thieves can gained more information through phishing because of easy retrieval of public information. Once the phishes have received proper information, they can use the details for creating any kind of fake accounts according to the victim's information, which in turn results blocking of the victim's account. Therefore it is very important that almost all common users should have some knowledge about "**Phishing"** so that no one would get trap by the attackers.

VII. PREVENTIVE MEASURES

Here are some tips which are useful for prevention from scams in which it should be taken seriously so as to avoid circumstances such as losing your money to an unknown site or being framed for any kind of fraudulent incident because sometimes even after knowing what is best we still make wrong choices when deciding upon things. [9]

a. Keep your personal information private. Stuffs like bank account number, telephone number, address, passwords, etc.[9]
b. Do not fall for e-mails received from an unknown site enquiring about your personal information and giving you a strict deadline as to it should be filled within a period of time.[9]
c. Do not trust such e-mails or messages which say that you have won a big amount of money from some legitimate site and telling you to response to them along with your bank account and some other personal information.[9]

d. Update your system with the newest promising security software like anti-virus, anti-spyware, firewall, spam filters, etc.[9]
e. Pop-up messages are not to be acknowledged as they are mostly like the fishing rod of the fraudsters. Once you are hooked, there is no looking back.[9]

VIII. STATISTICS ON PHISHING ATTACKS

[10]Arecent study was made by the security specialist Kaspersky lab called the **"Financial Cyber Threats in 2014"**. In this study we found that about 30% of the phishing attacks target the online customers.[10]As we have described earlier that Phishing is an act of online fraud where customers are being lured to provide confidential or secret information regarding their accounts in order to perform this criminal act called Phishing scam.

We found that from their recent study Kaspersky exposed that about 16% of phishing crook uses the names of several banks recognized by customers to perform the crime which is very less compared to the previous year which is just 6% from 2013. But it got augmented by using the popular online shopping websites by 1% and it becomes twice by using the online payment which falls tobe 5%.[10]Specifically, banks mentioned that in 29 percent of attacks, online payment systems is 11 percent and online shopping sites is about 8 percent of attacks, Kaspersky said.

Cyber crooks mostly target and aimed at customers secret details and information like Visa card which is 31% of the attacks which is more than Paypal 30% and American Express is 25% which was attacked by the crooks. [10]It is found that the financial phishing on Mac systems occurred in about 48 percent of all instances,which results to an increase of 9.6 percent compared to 2013, Kaspersky reported.

In this paragraph the Kaspersky web content analyst revealed that "The rise in financial phishing that they saw in the past has naturally drawn a response from the brands most frequently abused in phishing scams," said NadezhdaDemidova, Kaspersky. [10]Here the company is trying to find ways and means to decline the purpose of phishing "They are beginning to tackle phishing distribution channels, especially email spam, more actively. That leads to a decline in the levels of phishing that targets some of the larger brands."[10]Cybercrooks responded to an increased awareness by name brands, Demidova said, by aiming at new markets, such as websites that sell plane tickets, which used to be an afterthought in phishing scams, she said.

IX. STATISTICS BY PHISH TANK COMMUNITY

[11] This statistics is for the month of November 1, 2013 through November 30, 2013.It is calculated that the total number of suspected phishes is 47,492. Phishes are described into two categories:

a. Valid Phishes: It is defined as the number of total submissions verified by the phish tank community. The phish tank community states that around **26,966** phishes are declared as valid phishes.
b. Invalid Phishes:It is defined as the number of total submissions verified by the phish tank community as well. The phish tank community states that around **648** phishes are declared as invalid phishes.

Many phishing emails were offline at the time of submission to Phish Tank. Offline phishes cannot be voted on, and therefore cannot be verified.[11]The Phish Tank community also prepared a questionnaire in order to get the total number of votes whether "is a phish," "is not a phish," and "I don't know" , is the question and the number of votes altogether made by the Phish Tank Community is 177,367. In order to verify this statistics the Phish Tank Community also at the same time calculates the time slot taken by the user's to answer the question which is known as the Median Time. The amount of time taken is 09 hours, 48 minutes.This results that the median time is the time taken by the Phish Tank community to verify submissions as valid or invalid.[11]Out of the more than 20,000 members of the Phish Tank community, these members were the most active participants in November 2013.

Table 1: Phish Tank

Top 10 Submitters	Vote of submissions	Top 10 Verifiers	Votes of Verifiers
Cleanmx	(24,507)	Andrea78vr	(47,515)
PhishReporter	(9,475)	Knack	(42,200)
Knack	(1,928)	Paulch	(23,864)
Cyscon	(1,635)	buaya	(20,531)

Andrea78vr	(982)	Andreil	(12,119)
Alsf78	(981)	NotBuyingIt	(8,401)
Billwake	(677)	ANTUNES	(3,160)
Tjatatt	(640)	phishphucker	(2,686)
ZRSABUSE	(507)	Dareks	(1,896)
Demartin	(498)	heymoe	(1,702)

X. NEW PHISHING STATISTICS

[12] A new phishing statistics was evaluated in the year 2014 25thof April by researchers in which they found that 1/3 of phishing attack last year is on bank credentials or financial records purposely. It was known that from 2012 there is an impact on the rise of 8.5% in financial attacks, which shows the highest effect compared earlier. The fraudulent which acts as one of the well known organization uses MasterCard, Visa, ATM's, American Express or PayPal's name in order to divulge into the business. Mostly Phishing attackers damages the volubility and reliability of the brand products which is very difficult for the end user's to either differentiate or distinguish real and fake emails. Example is the Amazon which is used as a cover by attackers to fool the customers or end user's in which Apple and E-Bay was also used.

[12]With effect to this most of the attackers have made an effort to take advantage of people who are interested for participating in any kind of talks, discussions, seminars, conference etc, just by pretending for helping them like reservation of hotels, transportation, hospitality and so on by pretending as one of the conference manager . the In addition to these, recent phishing attempts have tried to exploit conference attendees by posing as hotels or travel agencies representing the conference organizers by asking the participants to enrolled themselves by following the links and rules provided on the websites .[12]It is advisable that we should never fall into unwanted emails or fake calls asking for important information. We should keep in mind by having a doubtful thought whenever we are asked to reply any emails or to fill up any kind of online forms that asks for secret information like financial credentials, pin numbers , usernames, address, parents name and passwords because it might be a phishing crack .

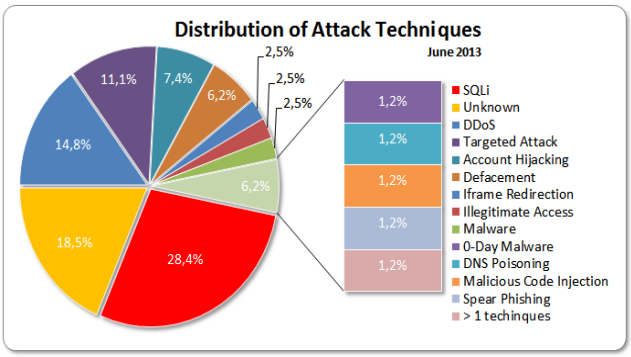

Fig 1: Distribution of attack techniques.[13]

XI. RESULTS AND ANALYSIS OF EXISTING WORK

According to the author in paper[3] the number of phishing sites out of 50 correctly and incorrectly identified by anti-phish toolbars is listed in the table below:

Table 2: Phishing sites identified by anti-phishing toolbars.

	Sites correctly identified as Phishing	Sites for which toolbar made no determination	Sites incorrectly identified as safe
Cloudmark	0 (0%)	50 (100%)	0 (0%)
Netcraft	48 (96%)	2 (4%)	0 (0%)
TrustWatch	34 (68%)	16 (32%)	0 (0%)
SpoofGuard	31 (62%)	12 (24%)	7 (14%)

The table below is the result of the number of phishing sites correctly identified and legitimate sites falsely identified as phishing sites by anti-phishing toolbars according to paper[3].

Table 3: Identification of legitimate sites by anti-phishing toolbars

	Time since phishing site URLs were extracted					Legitimate sites	
	0 hours	1 hour	2 hours	12 hours	24 hours	Falsely identified as phishing	Unsure
Netcraft	81 (81%)	80 (81.6%)	79 (89.8%)	67 (91.8%)	38 (95%)	0 (0%)	0 (0%)
TrustWatch	59 (59%)	59 (60.2%)	53 (60.2%)	45 (61.6%)	32 (80%)	0 (0%)	8 (8%)
SpoofGuard	93 (93%)	93 (94.9%)	85 (96.6%)	67 (91.8%)	38 (95%)	37 (37%)	55 (55%)
Cloudmark	40 (40%)	38 (38.9%)	35 (39.7%)	34 (46.6%)	13 (32.5%)	0 (0%)	84 (84%)
Google	53 (53%)	52 (53%)	48 (54.5%)	42 (57.5%)	30 (75%)	0 (0%)	0 (0%)
Active URLs	100	98	88	73	40	100	100

Table 4: Number of phishing sites initially identified incorrectly that were later identified correctly by ant-phishing toolbars.

	Time since phishing site URLs were extracted			
	1 hour	2 hours	12 hours	24 hours
Cloudmark	0	1	0	0
EarthLink	0	0	0	0
eBay	0	0	0	0
IE7	0	1	0	0
Google	0	1	4	5
McAfee	0	0	0	0
Netcraft	0	1	0	4
Netscape	2	0	0	7
SpoofGuard	0	0	0	0
TrustWatch	0	0	0	0
Active URLs	100	98	93	70

According to the authors in paper [16] they have made their study on the efficiency and usefulness of using phishing toolbars and blacklisting, in which the author in Nov 2006 used 10,000 phishing URLs from Phish tank to examine the efficiency of the black-lists maintained by Google and Microsoft. They found that Google blacklist enclosed more than 90% of the live phishing URLs, while Internet Explorer enclosed only 67% of them.In this study the author tested the efficiency of 10 popular anti-phishing tools in November 2006, where the data are generated in the table below.

Table 5: The top 10 brands that appear in our data set. Total phish: 191

Institutions Victimized	# of phish	Percentage
Abbey	47	24.9%
Paypal	21	11.1%
Lloyds TSB	17	9.0%
Bank of America	14	7.4%
Halifax	13	6.9%
Capital One	11	5.8%
New Egg Bank	11	5.8%
HSBC	7	3.7%
eBay	6	3.2%
Wachovia	6	3.2%
Wellsfargo	6	3.2%

The authors concluded that blacklist-based solutions are quite efficient in protecting users against phishing attempts.

Another important study made by the same authors [16] on Length of a Phishing Campaign (LPC) defines as the time lapse between the first time a phish appeared in their source report and the last time that phish appeared in their source report. In which these reports was received by them from their source every 4minutes.

In the above study they have made out of 191 phish which were used to test phishing blacklists, 127 of them, 66%, had an LPC less than 24 hours, indicating that their corresponding phishing campaign lasted less than 24 hours. A total of 25 URLs had an LPC between 24 and 48 hours, and the remaining URLs had an LPC between 3 and 23 days. Examining the first day's data more closely, they found that 109 URLs were spammed only in a two-hour period, accounting for 63% of the URLs in this dataset.

Table 6: Website takedown rate vs. length of phishing campaign (LPC)

Hours	% of website taken down	% Phishing Campaign Finished
0	2.1%	0%
2	7.9%	63%
4	17.8%	67%
5	19.9%	70%
12	33.0%	72%
24	57.6%	75%
48	72.3%	90%

Website takedown rate at each hour is measured by the number of phish taken down at that hour divided by total phishing users initially, as most of them caught less than 20% of phish at hour zero. They also found that blacklists were updated at different speeds, and varied in coverage, as 47% to 83% of phish appeared on blacklists 12 hours from the initial test in October.

At any given hour, they define the coverage of the blacklist as: No: of phish appearing on blacklist

Total phish that were taken down

They have found that the coverage rates of some of the blacklists were highly correlated, where Firefox 2, 3 and Google Chrome appear to use the same blacklists. Internet Explorer 7 and 8 also share a blacklist. In their analysis, they have combined the results for those tools that use the same blacklists.In their October test, they enclosed that all of the blacklists contained less than 20% of the phish initially. New phish appeared on the blacklists every hour, suggesting that the blacklists were updated at least once every hour.

XI. CASE STUDIES

A. Case 1

- [14]One of the best known and well populated site of the world **Google.com** was also recently under phishing attack where the subscribers of Google were given notice to update their personal information within the period of seven days and if they failed to do so their account will be terminate from the site permanently. This has left the subscribers in a state of confusion whereby later the matter is being denied by the spokesperson of the respected site and claims it to be a phishing attack which intends to collect personal information popularly known as **spoofing** or password **phishing**.

A. Case 2

- [14]**Reserve Bank of India under attack!!!** This information appears to be true when the attackers have the nerves to create a fake website which is a clone of the RBI website in which they send e-mails to the

users informing them regarding the prize money of Rs.10lakhs that they had won which will definitely caught the attention of the users and giving them a link of the look-alike site enquiring the users with their personal details like passwords, I-pin number and savings number. In spite of this the RBI has warned its users concerning the counterfeit scam of the bank's original website.

B. Case 3

- [15]In Nov 8th2014, Home Depot a home-improvement chain company said 53 million e-mail addresses are being violated due to the attack caused by the hackers whereby 56 million payment cards were disclosed. The hackers somehow manage to utilize a third party vendor's username and password and gain the company's rights to traverse the systems. It uses a custom-built software of the company's self checkout terminals to retrieve customers data especially in the United States and Canada which causes the company the loss of $62 million to recover in which the amount of $27 million will be covered by insurance. It was reported that the malicious software used by the hackers was designed in such a way that it can escape the detection of the anti-virus software of the company's systems.

XII. CONCLUSION

In conclusion to this study about phishing we have seen some interesting facts about how far an attacker would go in order to fulfill his desirable needs. We have also witness a huge loss of money globally which results to under-achieving productive goals and development of the society. But the most dreadful loss are the common users who are the victims of phishing for without their knowledge their personal information are being used against them for some kind of fraudulent acts, or even their bank accounts are being robbed without their concern. In spite of this now the organizations are taking an initiative move of spreading an awareness statement to be more cautious and precise regarding the fake information (like winning lottery of undeniable prize, reservation of hotels at a cheap rate, travel agencies offering less expense, etc..) which alerts the users from getting phished.

REFERENCES

[1] http://www.theemailadmin.com/2009/02/history-of phishing/
[2] http://www.phishing.org/what-is-phishing/
[3] Lorrie Cranor, Serge Egelman, Jason Hong, Yue Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars,"Carnegie Mellon University, November 13th2006, CMU-CyLab-06-018,P:1-3.
[4] Anthony Elledge, "Phishing: An Analysis of a Growing Threat," GIAC Security Essentials Certification(GSEC) Practical. Version 1.4b, January 2007, P:3.
[5] http://www.facebook.com
[6] http://www.innovateus.net/science/what-are-different-types-phishing-attacks
[7] NeerajAarora,"Phishing Scams in India and Legal Provisions, Cyber forensics, cyber lawyer, cyber offenses / contravention, information technology act, other laws," March 14, 2011, 2.
[8] RachnaDhamija, J.D. Tygar, "The Battle Against Phishing:Dynamic Security Skins,"University of California, Berkeley.In SOUPS 2005: Proceedings of the 2005 ACM Symposium o usable security and privacy, ACM International Conference Proceedings Series, ACM Press, July 2005,P:1.
[9] http://blogs.wit.edu/security/new-phishing-statistics
[10] http://thevarguy.com/business-technology-solution-sales/022215/kaspersky-nearly-30-percent-phishing-attacks-target-financial-inf
[11] http://www.phishtank.com/stats/2013/01
[12] http://www.symantec.com/security_response/publications/threatreport.jsp
[13] file:///E:/phishing/APWG_GlobalPhishingSurvey_2H2013.pdf
[14] AtulKahate, "Cryptography and Networking Security," Second Edition, Tata McGraw Hill,2008.
[15] http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html.
[16] Steve Sheng, Brad Wardman, Gary Warner, Lorrie Faith Cranor, Jason Hong, Chengshan Zhang, "An Empirical Analysis of Phishing Blacklists," Carnegie Mellon University Engineering and Public Policy Pittsburgh, PA 15213, University of Alabama Computer Science Birmingham, Alabama 35294, P:3-5.