Phishing as a Strategy against Individuals and Organization

Prasanna. S[1] and Dr. V. Mariappan[2]

[1]*(Research Scholar, Department of Banking Technology, School of Management, Pondicherry University, India)*
[2]*(Associate Professor, Department of Banking Technology, School of Management, Pondicherry University, India)*

Abstract: *Technological advancement has brought lots of convenience to the human community, one such technology that has made a revolution in human life is the development of computer and its associated technologies which have shrunk the whole world into a global village. However, technological developments and advancements are not without concerns particularly the cybersecurity-related crimes are creating lots of worry among the entire stakeholders. One such form of cyber security related crime is phishing which is targeted against an individual, as well as organization, has generated a lot of discussions and focus in the recent years among the netizens. Hence, this paper attempts to analyze the recent developments in phishing as a strategy against individuals, successful organizations and nations.*

I. INTRODUCTION

In today 's environment, computer and smart device are omnipresent and has become an essential part of individuals and organizations to engage with various stakeholders. The smart environment is gaining importance among business houses as it supports them in achieving their objectives in a cost-effective way. Moreover, there is an increasing trend amongst the people in adopting smart systems which will continue in the near future too. Organizations are utilizing this development for their business success by incorporating innovative technologies to serve their clients better, but such opportunities are not without concerns. This includes various kinds of illegal or criminal activities happening in the electronic environment that is popularly known as cybercrime. One such form of cybercrime is phishing where user confidential information has been illicitly obtained by cyber criminals either for financial gain or other motives that have affected the privacy of individuals as well as institutions.

Phishing Attacks – An Overview

The anti-phishing working group has defined phishing as "criminal mechanism employing both social engineering and technical subterfuge to steal consumer's personal identity data and financial account credentials". Phishing is considered to be the serious cybersecurity problem today as such attacks get more sophisticated through the use of new techniques [1]. Phishing is an attempt by fraudsters to acquire confidential data such username, password and bank account detail of customer for the monetary gains. As per [2] phishing spoofs legitimate entity, uses the website to implore confidential information of the victim. Even though lots of techniques are used in phishing attacks, most of them happen through e-mails, social network sites and also instant messages. The message used in the phishing attacks is so designed in such a way that it entices the customer to share their confidential information [3]. The success of phishing attack depends on the sense of trust created by perpetrator on victims that allows them to obtain the confidential information which is then used for the personal gain [1], [4], [5]. The impact of phishing attack includes loss of intellectual properties right, financial loss and threat to national security [1]. As phishing crimes are reaching to a new high, a study about phishing and its various dimensions gains importance.

Types of Malware Attacks and the Infection Rate

Malware is malicious software created to access or damage a computer system without the knowledge of the owner. Malware includes viruses, worms, keyloggers, spyware, or any other type of malicious code that infiltrates a computer [6]. Trojan is a type of malware used to gain access by tricking the user to load and execute in their system which enables the cybercriminals to delete, block, modify or copy the data and disrupt the computer performance [7]. While worms are a standalone computer program that replicates itself to spread to another computer, a computer virus is a malicious program designed to spread from one computer to another and to alter the way a computer operates. The following table 2 list out various malware along with its infection rate.

Table 1: Type of Malware and Rate of Infection (Figures in percentage)

Type\ Year	2012		2013		2014		2015		2016	
	A*	B**	A	B	A	B	A	B	A	B
Trojan	76.49	77.09	72.32	77.19	72.58	73.53	66.53	72.81	69.57	69.84
Worms	10.22	6.48	13.61	5.82	9.83	3.27	7.46	2.7	10.26	2.69
Viruses	10.68	7.78	9.39	6.29	7.27	3.22	15.13	1.7	13.1	1.56

Others	2.61	8.65	4.69	10.71	8.06	14.31	10.9	22.08	7.06	25.91

Source: Data as compiled by a researcher from Anti Phishing Working Group Reports
* A-Average percentage of malware identified
** B-Average rate of infection from malware identified

It is seen from the table that trojans, worms, viruses, are major malware used for phishing attacks. The other malware includes adware, spyware, rogue ware and PUP used in attacks. Though attacker's used different malware to carry out the attack on their target, Trojans has been most popular among the cybercriminals as it was used extensively with an average infection rate of 74.50 percent followed by worm and viruses with 4.19 and 4.11 percent. The main reason behind the Trojan's high rate of infection is its ability to disguise as legitimate software [7]. The increase in the usage of the social network has paved the way for the perpetrator to gain access to other systems by tricking them to execute the malware like Trojans [7]. The development of various anti-malware programs by the expert has made the perpetrators to shift their focus to other malware such as Rogue ware, PUP etc due to the knowledge gained by the users over the years about the traditional malware. This is evident from the fact that the infection rate due to Rogue ware, PUP etc has doubled between the year 2012 and 2016 and a corresponding decrease in the infection rate of malware like worm and viruses.

Top Countries Affected By Phishing Attacks

The cyberterrorist uses phishing as a means to strategically destroy nation's development. The cybercriminals have not spared any single country in the universe and therefore every country today is a victim of the phishing attacks. The following data provides the top five countries that are being affected by the phishing attacks in the recent years that are between 2012 and 2016.

Table 2: Top Five Countries Affected by Phishing Attacks

Year \ Rank	1	2	3	4	5
2012	China	Turkey	Taiwan	South Korea	Bolivia
2013	China	Turkey	Peru	Taiwan	Russia
2014	China	Turkey	Peru	Bolivia	Russia
2015	China	Turkey	Peru	Russia	Taiwan
2016	China	Taiwan	Turkey	Ecuador	Russia

* Source: Compiled from various Anti Phishing Working Group Reports.

The analysis clearly reveals that most of the attacks have taken place in Asian Countries followed by Latin American countries. It is also seen that China has been continuously targeted by the attackers may be due to its economic position or a strategic move by rival countries. The data further shows that some countries have been repeatedly under attacks, for instance, Turkey which is rated less in the information processing skill according to OECD Studies [8]. The interesting point to be noted is that the western countries generally considered economically sound nations are not on the top list of affected countries. According to OECD report, the citizens of Western and European countries are far better on computer skill than their Asian counterpart [9] may also be the reason behind the lesser attacks on the western countries.

Sectors Targeted by Phishing Attacks

National economies of countries consist of different Sectors which are classified as primary, secondary, tertiary and quaternary based on the function they perform. Each sector refers to industry or a market that shares same operating characteristics [10]. While every sector has a unique role in the country's economic development, the role of the certain sectors like financial and payment are considered very critical for the nation. Hence, carrying out attacks on such sectors is almost weakening the country's economy. The following table 3 provides the sector-wise details of phishing attacks across the world in the recent years.

Table 3: Sector-wise Phishing Attacks (Figures in percentage)

Year \ Sector	Payment Services	Financial Services	Retail Service Sector	Internet Service Providers	Others Services
2012	29.45	35.33	9.11	6.93	19.18
2013	50.83	24.32	7.56	6.41	10.88
2014	35.88	22.03	17.68	8.12	16.29
2015	17.36	21.37	14.83	23.6	22.84
2016	12.27	18.82	42.64	12.15	14.12

* Source: Data compiled from Anti Phishing Working Group Reports

It is observed from the above table that there has been a consistent shift in the attack from payments and financial sector to retail services and Internet Service Providers (ISP). It is also a fact that the payments and financial service providers shifted their focus equally on the cybersecurity policy framework and investing heavily in software and installing strong security measures in the recent years. This may be the reason for the shift from these sectors to online retail which is a recent phenomenon that recorded a growth of almost four times between the year 2012 and 2016. Since online retail is an emerging sector with lesser security measures may have attracted the attention of the cybercriminals to move their focus from the traditional payments and finance sectors. To sum up, it is evident from the above data that more than two-thirds of the total phishing attacks are carried on payment, financial and retail service sectors across the globe.

Phishing Attacks on Major Brands

A brand is a name, symbol, term, design or other features that distinguish an organization or product from other similar product in the customer point of view. Customer’s perception of company services, reputation is represented by brand. It creates value for the business by improving recognition, creating trust, building financial value and through the generation of new customer [11]. Attacks on brand not only destroy the company image but also its’ value in the market thereby negatively affects the turnover and thus business prospects. According to FBI report, the attacks on brands may happen for a variety of reasons which includes intentional act by the business rivals to damage the reputation of the company or by the cybercriminal for monetary benefits. It may also be caused by disgruntled employees. The table below reveals the numbers of brands came under attack during the study period 2012 to 2016.

Table 4: Number of Brands Attacked

Year	No of Internet Crime Complaints	No of Brands under Attack
2012	289874	4840
2013	262813	4869
2014	269422	4029
2015	288012	4979
2016	298728	4521

* Source: Data from Anti Phishing Working Group Reports

It is seen from the above table, the average number of attacks in a year on brands stood at 4648 during the study period. Similarly, the average internet crime reported recorded is 281770. Both the number of internet crimes and brands under attack reported a fluctuating trend. The highest number of complaint is recorded in the year 2016 with 2.99 lakhs and the highest incident of brand attack is recorded in the year 2015 with 4979 attacks worldwide.

Phishing Attacks using Unique Websites

There are various techniques that perpetrator use in carrying out a phishing attack, one of such is the creation of a fake website that looks similar to the genuine site of an organization by which the fraudsters steals confidential information of individuals that is later used for the financial gain [12]. The fake website is a site that looks similar to the original site of an organization with minor / unnoticeable changes in the domain name which may fool the users to believe as original sites. Attacks of such nature seem to be increasing which may continue to increase in future as more and more people start adopting digital technology without proper knowledge about online security measures. The survey conducted among internet user in the U.K reveals that about 43 percent of new internet user have no idea on the firewall which is even worse in case of other security measures such as antispyware and deletion of cookies.

The following table 5 shows the number of unique phishing websites present in the internet space during the study period.

Table 5: Number of Unique Phishing Websites (Figures in lakhs)

Year \ Period	Quarter 1	Quarter 2	Quarter 3	Quarter 4	Total	Trend (%)
2012	1.64	1.75	1.48	1.42	6.30	-
2013	1.18	1.19	1.43	1.11	4.92	-21.92
2014	1.25	1.28	0.92	0.47	3.93	-37.64
2015	1.36	2.53	2.41	1.58	7.89	25.14
2016	2.89	4.66	3.64	2.77	13.97	121.65

* Source: Data compiled from Anti Phishing Working Group Reports

It is observed that the number of unique websites reported during the study period ranges from 3.93 lakhs in 2014 to 13.97 lakhs in 2016. When compared to the base year, it recorded about 122 percent during the last 5 years but overall it shows a fluctuating trend with a negative trend during 2013 and 2014. The phenomenal growth of fake websites in the cyberspace over the years is not a good environment for the internet users and also corporate and organizations. It exposes the unsuspecting users to greater risk and thereby pose danger to the netizens.

Phishing Attacks Using Emails

One of the most preferred techniques by the fraudster to carry out phishing attack is use of persuasive emails [12] to get information of customer which is then used for stealing customer’s information, data or money. Emails frauds include spoofing, bogus offers, and requests for help and email scam like investment offers, employment offers, health scams, Nigerian 422 and so on which is an unsolicited email that claims the prospect of something for nothing. The emails sent by the fraudster will be so unique such that the receiver of such message will be enticed to share their confidential information or transfer of money expecting the benefit of the offers made to them.

Table 6: Number of Unique Phishing Emails Reported (Figures in lakhs)

Year \ Period	Quarter 1	Quarter 2	Quarter 3	Quarter 4	Total	Trend (%)
2012	0.85	0.84	0.74	0.76	3.20	-
2013	0.74	0.53	1.80	1.60	4.67	46.21
2014	1.71	1.71	1.63	1.97	7.04	119.00
2015	2.21	4.17	3.95	3.80	14.13	341.74
2016	5.57	3.15	2.29	2.11	13.13	310.44

* Source: Data compiled from Anti Phishing Working Group Reports

A leading solution provider for phishing threat management, Phishme states that almost 91 percent of cyber attack starts with a spear phishing [13] and the top reason of people being duped includes curiosity, fear, and urgency followed by reward /recognition, social, entertainment or opportunity. The following table 6 shows the number of unique phishing emails reported during the study period. The above table supports the Phishme view mentioned above reflecting an increasing trend in spear phishing attacks. The period between 2012 and 2016 saw a total of about 4.2 million attacks. It is seen from the table that the number of email attacks increased over three times during the last five years. It increased from 3.2 lakhs to 13.13 lakhs between 2012 and 2016 accounting for a growth of 310.44 percent. The emails attacks increased continuously on year on year basis which is expected to continue in futures if proper awareness is not created among the email users, as the study by the Radicati group [14] has projected number of email user to reach 2.9 billion by the end of the 2019.

II. FINDINGS

The analysis of phishing data across the world in this study reveals many important findings. Most of the phishing attacks have targeted against financial and payment sector with almost half of the attacks are targeted against these sectors from the total phishing attacks. It is also found that fake e-mail and websites used to carry out phishing attack are on the increase with an average of 8.40 lakhs spear phishing emails per year and 7.40 lakhs fake websites per year. Trojan malware leads the list of total malware identified with an average of 71.50 percent with an infection rate of 74.50 percent.The analyses also reveal that the Asian and Latin American countries are most affected by malware infection with China has been the most favored location for the perpetrators of cybercrime.

III. CONCLUSION

The problem around the online security is getting complex day by day which will become even worse in the upcoming days to come if proper security measures are not adopted by all the stakeholders which include national governments, organizations and also the cyber community. All actors in the cyberspace are responsible for keeping the cyberspace threat free for which each and every one in cyberspace should perform their assigned duty as expected by the security framework. Even though the organization is adopting best of the class framework in its security, it will go into a vein if they are not properly adopted by its users. In order to reap the benefits of technology, the organization should not only incorporate high standards in their security but also make their users to adopt best security culture. The organizations should frame strategies to increase the awareness level of the user which is the foremost requirement for preventing cyber attacks.

IV. REFERENCE

[1] *I. Kirlappos and M. A. Sasse, "Security education against Phishing: A modest proposal for a Major Rethink," IEEE Secur. Priv., vol. 10, no. 2, pp. 24–32, 2012.*

[2] *Z. Ramzan and C. Wüest, "Phishing attacks: Analyzing trends in 2006," 4th Conf. Email Anti-Spam, CEAS 2007, 2007.*

[3] *Action Fraud, "Phishing, vishing and smishing." [Online]. Available: https://actionfraud.police.uk/fraud-az-vishing. [Accessed: 18-Jan-2018].*

[4] *N. L. Muscanell, R. E. Guadagno, and S. Murphy, "Weapons of In fl uence Misused : A Social In fl uence Analysis of Why People Fall Prey to Internet Scams 1," vol. 7, pp. 388–396, 2014.*

[5] *N. Costigan, "The growing pain of phishing: Is biometrics the cure?," Biometric Technol. Today, vol. 2016, no. 2, pp. 8–11, 2016.*

[6] *"Malware 101: What is malware?" .*

[7] *"What is a Trojan Virus Internet Security Threats Kaspersky Lab India." .*

[8] *OECD, "Adults' proficiency in key information-processing skills," OECD Ski. Stud., pp. 33–66, Jun. 2016.*

[9] *E. Ravenscraft, "This Chart Shows How Computer Literate Most People Are," Lifehacker. .*

[10] *"Sector Definition Investopedia." .*

[11] *"6 reasons why a strong brand is important for your small business," Deluxe Small Business Resource Center. Jan-2015.*

[12] *"Phishing," Wikipedia. Mar-2018.*

[13] *"Anti-Phishing Solution Threat Management," Cofense. .*

[14] *. The Radicati Group, "Email Statistics Report, 2015-2019," Email Stat. Rep., vol. 44, p. 4, 2015.*