Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 3; April-June, 2017, pp. 161-165

http://www.krishisanskriti.org/Publication.html

The Security threat in Cyber World – cybercrime as PHISHING

Anu Yadav[1] and Jatin Gemini[2]

[1,2]University School of Information & Communication Technology, GGSIPU
E-mail: [1]noor4anisha@gmail.com, [2]aryankumar752@gmail.com

Abstract—*Since last decades, our financial as well as social activities depending on not only internet but on web applications also, the comfort provide by these online technologies almost revolutionized the modern world. The increase in user utilization of internet in everyday activities to a great extent that we explore our life and secrets to the world. The long time explore to internet of huge community for activities such that online services, ticket booking, sending important documents and information via email, online payment, online shopping, net banking and online trading drastically increasing risk of security threats and cybercrimes. Phishing is one of the cybercrimes that impact on user's personal information, damages brand reputation, damage financially and loss of customer by organization. Hence online transaction is doubtful and risky. The popular cybercrime is phishing that used to steal confidential and personal information by tricks and plague on internet users. The phishing is a combination of spoofing techniques as well as social engineering methods to deceive internet users by revealing their confidential and sensitive information. In this paper we discuss phishing and its forms, phishing types and damages caused by phishing, case study on real phishing crimes & laws for phishing and phishing statistics of 2016.*

Keywords*: Phishing, phreaking, social engineering.*

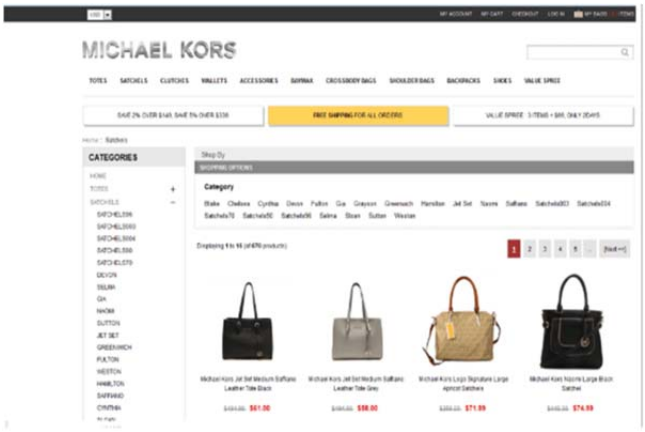
1. INTRODUCTION

The rapid increase of cyber world and frequently use of mobile, social media and web technologies increase risk of security threats- phishing. The popular cybercrime is phishing that used to steal confidential and personal information by tricks and plague on internet users. In this paper we studied the details of phishing like definition of phishing, origin of word phishing, phishing as a social engineering attack, how to avoid being a victim of phishing, important points of phishing, , forms of phishing, classification of phishing and case study on phishing crime. At last statistics of 2016 in worldwide is discussed with percentage of phishing record.

2. PHISHING

The phishing is a combination of spoofing techniques and social engineering methods to deceive internet users by revealing their confidential and sensitive information (security numbers & questions, bank details, credit card number, victim details, password of online accounts for shopping, username, passwords,) using impersonating a big, honest, and trustworthy 3rd party. The web technology based criminal act is phishing that is a fraudulent act by camouflaging as a trusted party to acquire secret information. Phishing is an art of cybercrime in cyber world that destroy connection and trust between organizations and customers with negative impact on organization. The Developing countries like India have recently facing Internet security threats such as phishing in cyber world with a rapid increase that used to steal information by tempting the victim (unaware of trap of phishing websites) with exciting and lucrative offers on the name of trusted organization, if victim click on links then they redirect victim to a fraud website and deceive victim by collecting sensitive information. The attacker of phishing websites fools the victim with techniques like SMS, DNS spoofing, chat rooms, website, voice, email (spoofed e-mails) and malware.

Recent example of phishing in Brazil Olympic Games. The phishers targeted both, ordinary citizens (who received fraud lottery win notifications) and Olympic game organizers, allegedly organized by the committee of Olympic and the government of Brazilian. Another example is holiday season sales in which phishers take advantages of busy duration of shopping period due to festival season and they create fraud websites of online stores and payment system and trap victims by giving discounts more than original websites. Example of such fraud website is shown in Fig. 1.



A fake online store page

Fig. 1: Example of phishing

2.1. Origin of word phishing

The security threat phishing is a combination of two English words, phishing derived from fishing & phreaking words each have meaningful definition that describe phishing. Fishing is a term used for a method in real life that used to attract fishes to bite the food that specially prepare to trap them & those fishes who bites that become victims, here online users are referred by fishes. Whereas phreaking is a term like slang, the term used to describe the overall activities of a particular culture of public who basically experiment, study, exploit as well as explore the telecommunication system (system or equipment that are connected to telephone network) to obtain the free call services.

2.2 Phishing as a SEA

As we know phishing cybercrime is a form of social engineering attack (SEA) method. Exactly what is a SEA method, the particular attacker uses social connection, media, and skills as human interaction to get information regarding particular person or organization or phone or computer system. According to victim attacker is a person with higher position, respectable, unassuming, researcher, or banker who asks questions in an art of getting small information that afterwards when combined attacker get full secret information to infiltrate an company or person. The attacker sometime elicitation from different sources (like contact each employee of company) of same company & piece together enough knowledge regarding particular company.

2.3. Important points regarding phishing

- The first cybercrime phishing case incident was reported in police first time as a crime in America in 2nd January 1996, AOHell UseNet newsgroup (America Online).
- The few of targets have highest priority by phisher (person who perform or carried out phishing crime), few attracting targets are social media, security companies, gaming industries, financial institutions, etc.
- The attacker mostly take the advantages of some scenario or situations like health scares or epidemics (swinflu, H1N1), holidays, big political election, natural disaster like tsunami/ earthquake and economic concerns (IRS scams).

2.4. Forms of phishing

- Create fraud URL and then upload it on cyber world using internet.
- The misspelled URL, we can detect such URL if we are aware of such cybercrime and pay attention to URL for example www.micosoft.com instead of www.microsoft.com.
- The manipulation of URLS using Java scripts a higher language of computer coding.
- When attacker getting a valid certificates for such fraud and illegal websites.
- Change of domain name in website such as www.microsoft.nic.in (fraud website domain .nic.in) where real website domain is .com (www.microsoft.com).
- The use of fraud SSL (Secure Socket layer – OSI network for transfer data) locks that show victims or users security and make them feel secured on that website but in reality it is fraud website.

2.5. Classification of Phishing

In cyber world there are huge number of different methods that used to obtain sensitive information from different users or victims. Phishing techniques used are more advanced as advancement in technology increases. To prevent cybercrimes, users should be aware of phishing techniques and anti-phishing techniques to prevent and secure themselves from being such cybercrimes victims. The types of phishing is described in this classification of phishing Fig. 2. And detail of techniques are below.

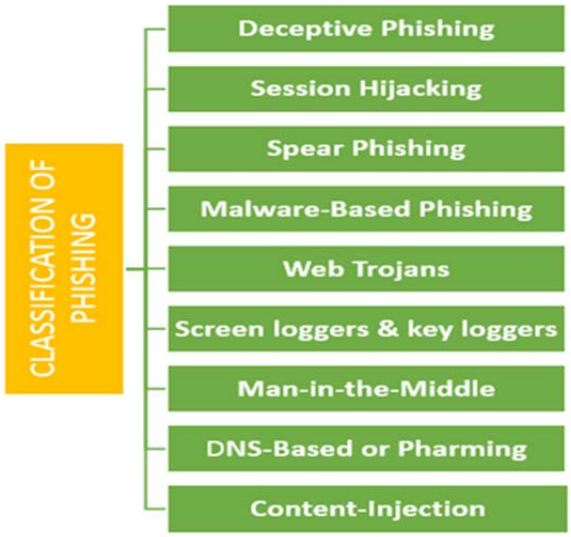


Fig. 2: The classification of phishing

The Deceptive Phishing: one of the most commonly occurring scam is deceptive phishing, attack to theft account or personal information (login details) by using instant messaging and attacker impersonate them as a legitimate organization. A phisher/attacker sends bulk email that contain a message too & users or victims are influenced (use to threat or scare user with sense of urgency) or attracted to click that link sended by phisher, for example new services for free that require quick action or updating, need to verify account details or undesirable changes required in account, account backend system failure hence require reenter important information, and change security question that require to enter previous security questions, etc. such messages are broadcast to a wide range of users with the chance or hope that unknowing unaware users may response by sing in (fraud website) or clicking that link sended by phishers and confidence to collect important information from that victim.

For example, paytm scam mail that instruct to click on link and sign in to verify their resent order or transaction. In reality the link is of fraud paytm URL that made by phisher to get victims details of paytm login. The success of such phishing is depend on user unaware of such phishing and that URL or message resemble to user (user order something on paytm).

The Session Hijacking: it a type of phishing attack that monitor the activities of victim or user until they login or sign in in particular account or website & link up their bona fide credentials. Now at such points the software called as malicious software used to takes over and perform unauthorized access like transfer money without the knowledge to victim.

The Spear Phishing: it is targeted attack like traditional phishing that uses a method of "spray and pray", in this method huge number of people get email but these people are targeted victims (group of same bank/ company customers/ employee). To increase victim trapped in their trap, phishers research on targets and make phishing more personalized.

The Malware-Based Phishing: it is a scam in which victim's computer/ laptop actually running on malicious software of phisher. The Malware or such situation can be introduced in victim PC due to downloaded file, email attachment, security application not up to date, or exploiting PC security vulnerabilities.

The Web Trojans: A Trojan horse is nothing but a type of malware that designed and use to mislead victim which look like legitimate, but it is doing unauthorized access in victim's account to collect information & credentials by use of local machine, then gathered information is transmitted to phishers. The web Trojans pop up but invisible to victim who are attempting to sign in.

The Screen loggers & key loggers: the varieties of malware in victim or users PC that track and identify each keyboard input and then all relevant information of victim are sended to hacker/phisher via internet where hacker decipher password and all useful information.

The Man-in-the-Middle: such Phishing are harder to detect & sophisticated technique, it is also known as Web based delivery phishing. In such attacks, phisher position is located between victim or phishing system and legitimate system (original website). The hacker/phisher traces and record the detailed information being enter during transaction between victims and legitimate without knowing the user regarding this trace but don't affect current transaction but later phisher use that information when victim is not active on its own system.

The DNS-Based Phishing: it is also known as **"**Pharming", DNS stands for Domain Name System based phishing (host file modification). Attacker tamper with organization's DNS or host files and request for fraud website URL and uses its name as well as services to communicate to fraud site. Hence victim or customer of organization unaware that sensitive information in website they are entering is actually controlled by phisher.

The Content-Injection Phishing: it is a phishing where phisher replace content part of legitimate website with wrong content designed & hence mislead the victim into giving up their sensitive information to phisher.

2.6. Prevent yourself from being a victim

- Never provide any kind of personal, secret or organization information like passwords as well as network or structure of organization until and unless you are dam sure about that particular person is authorized to have such information.
- Never ever send your secret information using internet without checking the security of website

- Always use anti phishing protection software's (AVG) install and maintain firewall, email filters, web browser, reducing spam and anti-virus software.
- Always take advantages from anti phishing features those are may be offered by your web browser or email client.
- Don't reveal financial and private information via email and never respond to email solicitations specially links sent in email (never click and go to fraud website).
- Be aware of URL of a website, there is little difference between legitimate (true/original) website and malicious (fraud) website, malicious website look like identical to original website but URL of fraud website may vary in spelling(instead of ICICI uses ICICII) or different domain (instead of .com uses .net).
- If you have doubt or unsure about suspicious email or call from original organization, instead of giving information try to find out and verify that person belong to legitimate company.

2.7. The Damages caused due to phishing attacks

The erosion of user trust on usage of internet and decrease public trust.

The financial loss is majorly occurring in cybercrimes such as phishing, aim of phishing is to get secret information (net banking login or transaction) hence victim loss the cash in their bank account.

Bad credit is another example in which phisher gets credit card and details of it (PIN number), some time they duplicate credit card by fitting some software in ATM machine.

3. CASE STUDY ON PHISHING IN INDIA

Here in this section we studied 4 biggest phishing cybercrimes recorded and solved by police.

ICICI Bank: the few members (customers) of ICICI bank registered a cyber-crime complain to police who are victim of phishing. The customers discovered that few emails can be extremely hazardous to their security and financial. These victims received an misleading email from phisher (perpetrators) who posed ostensibly emanating from bank's official ICICI email ID, when click on URL and connect them to website that resembled with original website of bank and asked for credential and secret information (like login id, username, PIN, debit card number, login name, password). It is called as banking scam. This scam discovered when bank's employee (assistant manager) received an email that is forwarded by some customer to crosscheck. The phisher accused is arrested from Vijaywada with the evidences of 1 laptop & 1 mobile phone, these evidences seized by police. To send emails attacker used OSC (open source code) Email application software as well as used VSNL Emails (service provider of such emails don't have spam box for blocking such unsolicited mails). This banking scam succeeds due to dynamic link (code handling by the IE onclick() event) on home page of fraud website, when victim submit sensitive information is received by accused on his Acer laptop through Reliance Wi-Fi internet connectivity. The accused is find guilty and registered a cybercrime against him under U/Sec. 66 of IT Act, sec 419, 420, 465, 468, 471 of I.P.C r/w Sections 51, 63 and 65 of Copyright Act, 1957, and get the punishment of 3 years imprisonment and fine up to 2 lakh Indian rupees.

The case of Bank NSP: one of the banks management trainee who is engaged to be married, using bank computer these couples exchanged so many emails but few months later they had break up relationship. The girl created fake email ids like "Indian bar associations" and email is sent to all foreign clients of that boy from whom she had break up using bank computer. As a result boy working in company undergo great loss, as company lost a large number of foreign clients and they took bank to court for such mails. The bank is liable because emails are sended by bank's computer system to important customers.

The case of AP (Andhra Pradesh) Tax: the hacker who find as guilty and accused in this case he actually plastic firm businessman in Andhra Pradesh submitted 6000 vouchers to prove it legitimacy of trade. Accused thought his crime will be undetected, but when careful examination of vouchers & seized computer from accused. The computer content revealed it is clear that accused running 5 business under the guise of one single company and used fraud/fake computerized vouchers to show fraud sales records to save his tax. From accused home 22crore cash recovered in investigation.

The case of jogesh vs. SMC Pneumatic: the case is of court of Delhi, the jogesh kwatra was employee of SMC Pneumatics India Pvt. Ltd. The jogesh want to defame Managing Director Mr. R K Malhotra and company by using Emails containing vulgar, obscene, abusive, humiliating, filthy, defamatory, intimidating, and derogatory contains. These emails are sended to all subsidiaries of company in all over the world as well as other employee of that company. The company who is plaintiffs cased against him to highly malign the reputation of company in all over the world, where legally employee had no permission to send mails and terminated the services of jogesh. The honorable judge of Delhi high court found him as guilty in case of cybercrime.

4. STATISTICS OF PHISHING IN 2016

In year 2015, 55.28% spam in emails which is increased by 3.03% points in 2016 and 58.31% spam in email flow is recorded in year 2016. The most popular security threat malware distributed via email is Trojan.Win32.Bayrob. Triggered 154,957,897 instances in 2016 that is 6,562,451 more times than in year 2015 of the Anti-Phishing system. In world, Brazil country suffered from the highest number of

phishing attacks that is 27.61% in year 2016. Percentage of unique users that attacked by phishers in year 2016 is 15.2%. In 2016, 47.48% cases phishers targeted victim belong to various financial organizations.

The top five countries who detected phishing in 2016 year are Russia, Brazil, USA, China, and India. The country that triggered highest in world for phishing is Russia with 16.12%. Brazil recorded 8.77% due to Olympic game and take second position in phishing cases. USA increased by 0.5% in 2016 from 2015 and recorded 8.01% with third position whereas china take fourth position and recorded 7.86%. At last fifth position held by India with 6.01%. Remaining countries percentage is shown in Fig. 3 that describe the statistics of phishing in the world recorded in year 2016.

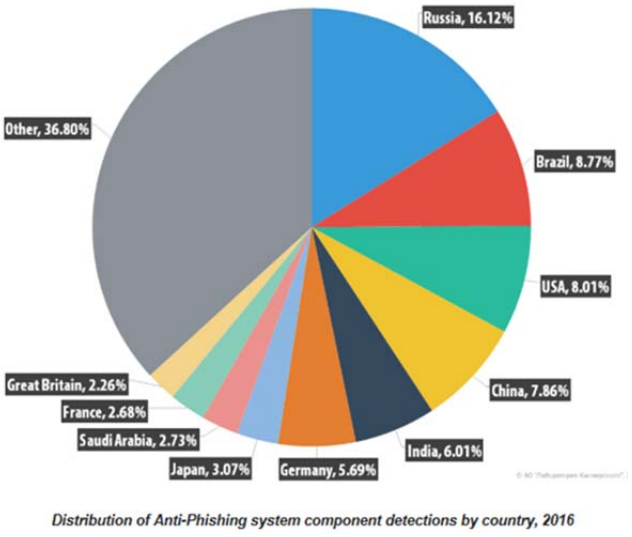


Fig. 3. The distribution of phishing detected by different countries in year 2016.

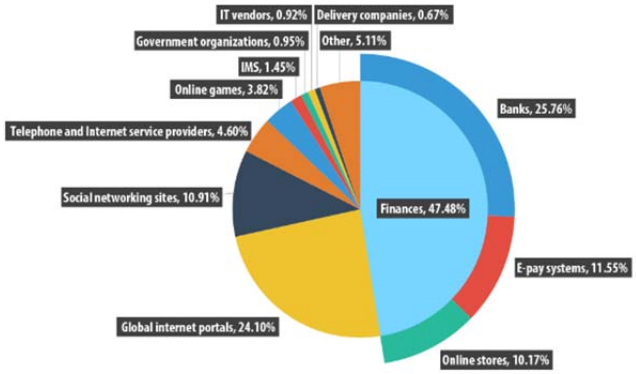


Fig. 4. organization under phishing attack by category.

The phishing attacks by category on particular organizations, mostly targeted group is financial sector. In Quarter 1 of 2016 detected 44.16% in financial sector and that increased in quarter 4 by 3.98% and it became 48.14%. In financial sector growth of phishing is detected continuously from year 2014. In 2014 it is 28.74% whereas in 2015, it increased and became 34.33% and in 2016 it was 47.47%. Similarly, there is increase in phishing attacks in online stores (10.17% in 2016 that increased by 1.09% from 2015) and payment systems (11.55% in 2016 that increased by 3.75% from 2015) sectors. Percentage of phishing occur in different organizations are shown in pie chart given in Fig. 4.

REFERENCES

[1] Varsharani Ramdas Hawanna; V. Y. Kulkarni; R. A. Rane, "A novel algorithm to detect phishing URLs", *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, 2016, Pp. 548 - 552.

[2] Xueni Li; Guanggang G.; Z. Yan; Yong Chen; Xiaodong Lee, "Phishing detection based on newly registered domains", *IEEE International Conference on Big Data (Big Data), 2016*, Pp 3685 - 3692.

[3] Christian Konradt, Andreas Schilling, Brigitte Werners, "Phishing: An economic analysis of cybercrime perpetrators", *Computers & Security, Volume 58, 2016*, Pp. 39-46.

[4] Ahmed Aleroud, Lina Zhou, "Phishing environments, techniques, and countermeasures: a survey", *Computers & Security, In Press, Accepted Manuscript, Available online, 2017.*

[5] Dongsong Zhang, Zhijun Yan, Hansi Jiang, Taeha Kim , "A domain-feature enhanced classification model for the detection of Chinese phishing e-Business websites", Information & Management, Volume 51, Issue 7, 2014, Pp. 845-853.