An Awareness towards "Phishing" Attack & its Counter-Measures

Sukhwinder Singh, Assistant Prof., Department of Computer Engineering, College of Technology, GBPUA&T, Pantnagar

Pragya Kamal, Assistant Prof., Department of Computer Engineering, College of Technology, GBPUA&T, Pantnagar

Deepak Kumar, Assistant Prof., Department of Computer Engineering, College of Technology, GBPUA&T, Pantnagar

[3] deepakchaudhary008@gmail.com

Abstract: Phishing is a method used by cyber criminals to acquire personal information such as passwords, debit or credit card details from net users. It is a general term used for creation and use of forged emails or websites that look amazingly real, designed to deceive users into revealing their personal information. Phishing is the commonest way used for fraud scams. Phishers use a variety of sophisticated skills to fool their victims. Even after so many years of phishing attacks and their publicity, they are still profitable to phishers. Phishing causes both an instant or short-term losses to victims and long-lasting damage to target organizations. Estimated losses from phishing are in billions of dollars all over the world, and that amount is growing as the phishing attacks are evolving. This paper covers the various techniques used by phishers and also the countermeasures against these attacks. By using this information, organizations and customers may aware about these kind of attacks or they might successfully defend many of the popular phishing attacks.

Keywords: phishing, Cross site scripting, Session Hijack, MITM, DDoS

I. INTRODUCTION

The convenience of e-commerce has been embraced equally by consumers and criminals. Identity theft has always been on top of a criminal's agenda. Phishing, the technique used by criminals to trick users into giving away their personal information has become a significant criminal activity on the Internet. Phishers design fake websites and emails that look like the legitimate ones and use them to acquire sensitive information from Internet users. In today's 21st century world, electronic identity theft has never been easier. Phishers simply use the acquired information such as login credentials or credit card details to make a transaction in a very small amount of time. Measures have been taken to prevent phishing attacks by educating the customers, but there has been an increase in the attack diversity and the attacks are becoming more sophisticated [1]. Phishing scams have evolved in recent years due to favorable technological and economic conditions. Phishing is a class of social engineering attacks, which uses technical deceit to exploit human behavior in certain conditions.

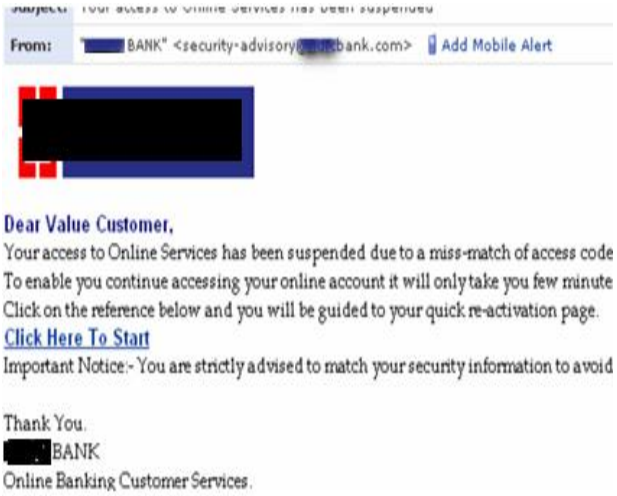

Fig: 1 Real life example of fake mail

The messages used by phishers in the fake emails create a sense of urgency such as a threat of account suspension, to motivate users to take action. The word Phishing came from the analogy that the criminals use email lures (fishing baits) to fish for passwords from a pond of unsuspecting Internet users. The use of 'ph' in phishing is due to the typical hacker naming conventions. The word 'phishing' was used for the first time in 1996 in the

alt.2600 hacker newsgroup, when the hackers were trying to steal AOL passwords [2].

II. PURPOSE & SCOPE

The purpose if a phishing attack has changed significantly over last ten years. In the beginning, the sole purpose of phishing was to acquire username and password of other customers. E-mail was used as the delivery method as well as acquisition method. After the popularity and awareness of fake e-mail, phishers developed more sophisticated delivery mechanisms. Unawareness of threat is the reason behind successful phishing. Today, phishers make use of e-mail, message boards, newsgroups, instant chat, social media sites and even internet telephony (VoIP) to attract users and steal confidential information. The most common method in use is the creation of fake websites which are a clone of the legitimate website. The user is tricked into visiting that cloned website where he unknowingly gives away his personal details. In the last few years, phishers have turned their interest to attachments to deliver Keyloggers or other malware to victim's computer. The purpose and motivations for phishing have changed and will continue to evolve due to advances in delivery techniques and sophistication of attacks. The financial rewards associated with phishing attacks have increased significantly. The most common purposes of phishing attacks are:

a. **Stealing Login Credentials –** The username and password combinations for online services such as Amazon, eBay, PayPal are used by phishers to make purchases or for online share trading and international money transfers.
b. **Stealing Credit Card Details –** The credit card details such as card number, card holder's name, expiry date, and CCV number are of great importance to criminals.
c. **Stealing Banking Credentials –**The username and passwords for online banking websites are used to access and transfer the funds.
d. **Stealing other personal information –** The other personal information particularly address information is sold out to direct marketing companies.
e. **Identity Theft –** Phishing can be used to steal personal information which is further used to create a fake identity, to commit another crime.
f. **Extending Botnets and DDoS Agents –** The phishers trick users into downloading malware, which turns the user's computer into a zombie machine that can be controlled by attacker. These computers can be used as DDoS [3] agents and are rented to other criminals.
g. **Attack Propagation –** Phishers may compromise a host and then use it as a sending machine for future attacks.

III. ATTACK EMPACT

Phishing causes both short-term losses and long-term damage. Following figures demonstrate the impact of phishing:

- If 2,000,000 phishing emails are sent.
- 5% get to the end user – 100,000 (APWG) [4]
- 5% click on the phishing link – 5,000 (APWG) [4]
- 2% enter data into the phishing site –100 (Gartner)
- $1,200 from each person who enters data (FTC) [5]
- Total damage due to phishing – **$120,000**

Phishing has following distinct types of impacts:

a. **Direct Financial Losses –** Consumers and businesses may lose up to thousands of dollars due to fraud committed using phishing. The Phishers can make purchases on your behalf or they can transfer funds from your account. Businesses face financial losses because of some credit card policies, which state that if a merchant accepts a credit card number that later proves to be acquired by fraud, then he is liable for the full amount of the fraudulent transaction [6].
b. **Erosion of Public Trust in Internet and e-Commerce –** The victims and witnesses of

phishing scams are less likely to use internet for business transactions. Phishing makes them uncertain about the integrity of the internet and e-Commerce. If a user cannot trust the address of the webpage he is presented with, he will hesitate using the internet for financial purposes.

c. **Difficulties in Law Enforcement Investigations –** Phishing can be conducted from anywhere in the world. A phisher in one country can use a controlled host in another country to send messages to unsuspecting users, which are redirected to the servers hosting fake websites in yet another country. This means that the phishers are less likely to get caught by the efforts of a single agency [7].

IV. PHISHING PROCESS

The phishers first select the victims and they decide the method to send them the phishing message. They can select Email, Message Boards, Instant Chat, Banners or Voice over IP depending on the situation. Phishers then decide the method for collecting data from victims, which can be done through embedded forms, Keyloggers, Interactive Communication or Fake Websites. The most common method used by phishers is redirecting the users to a fake website, where they are tricked into revealing their personal information.

The method in Fig.2 taken from [8] depicts that in this attack there are three phishers – Mailer, Collector and Casher devoted to handle specific tasks. The Flow of information is explained below:

1. An unsuspecting user receives a phishing mail sent by the phisher (Mailer).
2. The phishing mail prompts the user to click on a link. The phishing schemes rely on three elements.
   - These emails use familiar trademarks and official logos and recognized agency names.
   - Phishing emails create a sense of urgency by warning victims that if they do not follow the instructions, their account will be deactivated along with other negative outcomes. The fear developed because of these warnings further cloud the ability of the victim to judge the authenticity of the message. Even if a very small number of users respond, the ease with which the phishing messages can be sent to millions of people creates a large pool of victims. Sometimes messages offering positive incentives such as a reward are also used.
   - The phishers forge the email headers and subject lines to make message appear to come from trusted

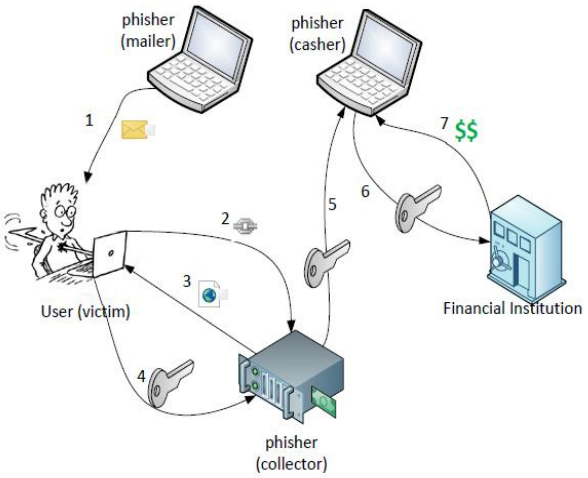

Fig 2: Information Flow in Phishing Attack.

3. The victim is then presented with a fake website, which is an almost exact replica of the corresponding legitimate website. Same graphics and fake validity signs are used to trick the victim.
4. The victim then unknowingly gives away his financial login credentials.
5. The Collector phisher then forwards the acquired information to the Casher fisher.
6. The casher phisher then impersonates as the victim using the stolen login credentials and authorizes himself with the financial company.

7. Once authorized the phisher (Casher) transfers or withdraws funds from the victims account [8].

V. PHISHING ATTACK VECTORS

For a phishing attack to be successful, a phisher has to adopt a number of methods to trick the victims to interact with the fake content. A combination of different attack vectors is used by the phisher according to the attack scenario and type of fraud being committed. The most common methods include:

a) *URL Obfuscation Attack:* It is the most common of all phishing attacks, in which the victims are made to follow a hyperlink (URL) to the phishing server without realizing that they are being fooled. It misleads the victims into thinking that the web site in their browser is the legitimate company website. The most common ways of doing this include - Registering Similar Domain Names, Use of Login URL's, URL Shortening Services, Use of actual URL within anchor tag of HTML, Abuse of International Domain Name Service and Use of alternate encoding schemes for URL's [9].

Fig.3: Use of actual URL within the anchor tag to fool users

b) *Man in the Middle Attacks:* In Man in the Middle attacks attacker situates himself between the victim and the real server. The attacker can use transparent proxies, DNS Cache Poisoning, or browser's proxy configurations to perform the attack. In this type of attack the even when the victim tries to visit the legitimate website, he is automatically redirect to attacker's server [10].

c) *Session Hijacking:* A Preset Session attack is possible when the web-based application allows client connection to define a session Id. In this class of attack the phishing link contains a preset session Id. The attacker sends this link to the victims and waits for one of them to authenticate the session Id. Once a session Id is authenticated, the attacker can use the same to gain access to the victim's account [11].

d) *Cross Site Scripting Attacks:* Cross Site Scripting Attacks [12], also called CSS or XSS make use of code injection into a valid web-based application URL or imbedded data field. These attacks occur because of vulnerabilities in the web servers or design of websites. User is made to click on a link which exploits XSS vulnerability in a server as shown in Fig 4.

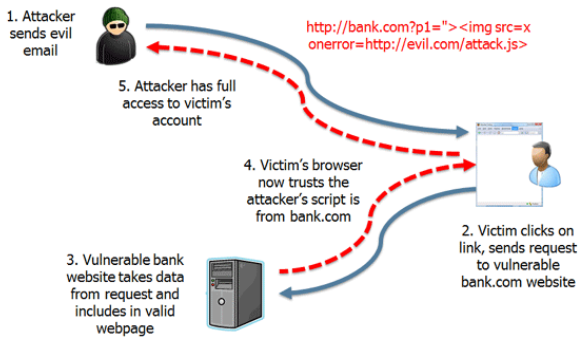

Fig 4: Cross site scripting attack

e) *Hidden Attacks:* The display of a web-page rendered by a web browser can be manipulated by using HTML, DHTML and other scriptable code that can be interpreted by the browser. Attacker can use these techniques in a Man in the Middle Attack, or in a fake website to disguise the fake content as coming from the real servers. Hidden frames of HTML are commonly used for this purpose. Attacker can also use some scripting languages (such as JavaScript and VBScript) to perform graphical substitution to fake the security indicators as shown in Fig. 5.

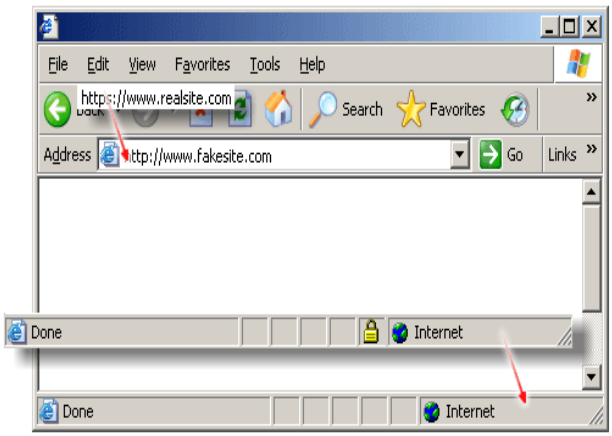

Fig.5 Positioning fake address and status bars on top of real ones

f) *Malware – Keyloggers and Screen Grabbers:* Keyloggers are old favorites of hackers and are becoming increasingly popular with phishers. The Keyloggers and Screen Grabbers can be used to capture information locally and send it to attacker using streaming, FTP, SMTP, etc. Keyloggers record the keys pressed by the user and Screen Grabbers take screenshots of the screen (or an application window) at regular intervals of time [13].

g) *Client Side Vulnerabilities:* The vulnerabilities in the web browsers used by the victims can be exploited by the attacker. The software vendors provide regular patches and fixes for the browsers but the home users rarely apply them. These vulnerabilities cam be exploited in a lot of ways and the attack is less likely to be detected by antivirus software. For Example: Microsoft Internet Explorer *window.createPopup()* method creates chromeless windows. Attacker can use the borderless window for graphical substitution.

VI. COUNTERMEASURES AGAINST PHISHING

Various solutions have been developed to defend against phishing attacks. But as shown in previous section, the phishers have a large arsenal of attack vectors at their disposal. Consequently no single solution can combat all those attack vectors. Using a mixture of defense techniques and applying defense mechanisms at different logical levels we can prevent current and future phishing attacks [5] .The measures to combat phishing must be deployed at Client side, Server-side and at Enterprise level as described below [14]:

A. *At Client-Side:* Client side includes the user's computer. This is where most of the countermeasures are applied. At Client-side protection can be ensured in following ways:

1) Using Anti-virus software: Anti-virus software provide local protection from common Malware. A personal firewall, IDS and Anti-spam functionality is included in most of the anti-virus software packages. Specific to Phishing attacks, the anti-virus programs have - Ability to detect and block attempts to install malware, Ability to identify common spam delivery techniques, Ability to detect and block un-authorized out-bound connections and Ability to identify common spyware installations.

2) Anti-phishing toolbars: Some plug-ins and toolbars that can be integrated into web browsers provide protection against phishing attacks.
Fig.6Browser Add-ins to identify phishing websites

3) Customer Vigilance: Customers may take a number of steps to avoid being a victim of a phishing scam by inspecting the content sent to them. Some general guidelines are:

- Be suspicious of any email that creates a sense of urgency, like giving warnings about account being suspended. Phishers generally ask for usernames, passwords, credit card numbers, etc.
- Never fill your details in forms embedded in emails or pop-up windows.
- While submitting financial details look for security indicators like the padlock icon. Also verify that the web address begins with 'https://' rather than just 'http://'.
- Phishing emails are typically not personalized, while valid messages from your bank or company are.
- Don't rely on links contained in emails to contact your financial institution. Call the company on official telephone or directly type the web address in the address bar.

B. *At Server-side:* Organizations can take an active role in protecting the customers from phishing attacks. At server side protection against phishing can be afforded by following methods:

1) Customer Education and Awareness:

Lack of education and awareness was originally the primary advantage for phishers. So to prevent phishing attacks the organization should educate its customers about the nature of attack. General information on phishing should be available at company website, Regular alerts should be sent to users to aware them of the phishing attacks, and security professionals should be invited to give seminars about phishing and the defense strategies. The organization should always use some personal information in the official e-mails.

2) Secure Web application Design: Design flaws in the web application can be used for phishing because of inherent trust relationships between users and website owner. The designers and developers must consider following factors:

- The web application should be immune to Cross Site Scripting attacks.
- Proper content validation should be in place.
- Session information should be handled carefully. It should never accept session information within URL's.
- Always maintain a valid list of redirection URL's, if web application needs to redirect users to other page locations or hosts.

3) Strong Authentication: The main purpose of all phishing attacks is to steal the victim's login credentials. To do this attacker monitors the authentication process.

Fig.6 Two phase authentication and virtual keyboard used by XY bank

A strong authentication process can make it difficult for attacker to capture all the information required for the phishing attack. The developers should adopt Two-phase authentication mechanisms along with techniques to avoid key-logging as shown in Fig. 6.

One time passwords and Token based authentication should be used for critical applications which work by generating single use or time-based passwords as shown in fig.8.

Fig.7 One time passwords used by XY bank

C. Enterprise Level

Businesses and ISP's can take enterprise level steps to combat phishing and protect customer and internal users. These solutions can be used to achieve defense-in-depth. At enterprise level, following steps can be taken to combat phishing [15].

1) Monitoring Domain Name registrations: When attackers spoof a target website they usually register similar domain names. Organizations should monitor the registration of domain names that are similar to theirs. Malicious domain should be taken down immediately after their discovery.

2) Mail server authentication: The sender's mail server should be validated by the receiving mail server. If the sending mail server address is not an authorized address for the email domain, then the email should be discarded. Validating emails can help reduce the volume of spam. Sender server can operate as an open relay server to overcome this problem. Also the enterprise mail servers should be configured to automatically validate digitally signed emails before they reach the user, and to automatically sign all outgoing e-mail.

3) Gateway Filters: Most phishing attacks make use of mass mailing as in case of spam. The Filtering techniques used to detect spam can also be applied to block phishing messages. The Gateway filters residing at the perimeter of the enterprise network can monitor all in-bound and out-bound traffic.

Apart from efforts to be taken at Client-side, Server side and at enterprise level a strong legislative framework is required to fight against phishing attacks. In India, phishing is treated as cyber-crime and sections 66, 66A, 66C & 66D of the Information Technology Act, 2000 are applicable to the phishing activities [16]. Also in some phishing investigations (involving two or more countries) a single government or agency might not be able to proceed by itself, so co -operation between multiple governments and agencies may be necessary for tracing the criminals.

VII. CONCLUSION

Phishing has significantly evolved over past few years. Phishers have successfully tricked users into revealing their financial details through cleverly designed fake web pages. A phisher don't need to be an expert to go phishing. Phishing kits are available for free download, which can be used by beginners to phish for passwords even without much knowledge of phishing attack vectors. With improvements in technology the phishing attacks are getting more and more sophisticated. No single technology will ever be able to take down phishing. However using a mixture of defense mechanisms at different levels as mentioned in this paper we can combat phishing effectively. We should know that the reasons of successful phishing are - Unawareness of phishing attacks, Unawareness of Policy and Technical sophistications. Enterprises should foresee the upcoming phishing attacks to prevent phishing before it occurs. An organization

should aim at protecting every user, even naïve users from phishing attacks.

REFERENCES

[1] TYRA, "resources.infosecinstitute.com," Phishing Definition, Prevention, And Examples, 2017. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/#gref. [Accessed 12 January 2019].

[2] R. Sherman, "Evolution of Phishing Attack," INFOSEC, 2016. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/evolution-of-phishing-attacks/. [Accessed 20 January 2019].

[3] G. A. K. a. M. R. N. R. Venkatesan, "A Novel approach to detect DDOS attack through VIRTUAL HONEYPOT 2018," in *IEEE International Conference on System, Computation, Automation and Networking (ICSCA).*, Pondicherry, India, 2018.

[4] APWGEU, Anti Phishing Working Group, 2013. [Online]. Available: https://www.antiphishing.org/. [Accessed 27 February 2019].

[5] F. T. C. C. Information, "Phishing," Federal Trade Comission Consumer Information, [Online]. Available: https://www.consumer.ftc.gov/articles/0003-phishing. [Accessed 12 February 2019].

[6] A. Gendre, "The Corporate Impact of Phishing," Vade Secure, November 2015. [Online]. Available: https://www.vadesecure.com/en/the-corporate-impact-of-phishing/. [Accessed 20 February 2019].

[7] H. Poston, "The Regulatory Impacts of Phishing Attacks," InfoSecInstitute, 31 October 2018. [Online]. Available: https://resources.infosecinstitute.com/the-regulatory-impacts-of-phishing-attacks/#gref. [Accessed 10 March 2019].

[8] S. S. Junxiao Shi, "Resources," 2013. [Online]. Available: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/index.html. [Accessed 12 February 2019].

[9] J. Rathod, "Anti-Phishing Technique to Detect URL Obfuscation," *International Journal of Engineering Research and Applications*, vol. 4, no. 5, pp. 172-179, May, 2014.

[10] N. D. a. V. L. Mauro Conti, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials* , vol. 18, no. 3, pp. 2027-2051, 2016.

[11] I. P. a. A. D. K. Suphannee Sivakorn, "The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information," in *IEEE Symposium on Security and Privacy*, New York, 2016.

[12] S. M. e. al., "A comparative analysis of Cross Site Scripting (XSS) detecting and defensive techniques.," in *Eighth International Conference on Intelligent Computing and Information Systems (ICICIS). IEEE*, Cairo, Egypt, 2017.

[13] S. Cooper, "Keylogger," Compaitech, 18 March 2018. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/what-is-keylogger/. [Accessed 21 January 2019].

[14] G. S. Bindra, "Efficacy of Anti-phishing Measures and Strategies-A research Analysis," in *World Academy Science, Eng. Technology 70*, 2010.

[15] L. L. Sullins, " "Phishing" for a solution: domestic and international approaches to decreasing online identity theft.," *Computer Crime. Routledge*, pp. 73-110, 2017.

[16] B. B. a. L. K. Bhagat, "Phishing and Its Indian Perspective," *The Internet Journal of Medical Informatics*, vol. 3, no. 2, 2008.