A Literature Survey on Social Engineering Attacks: Phishing Attack

Surbhi Gupta
Department of CSE
Amity University Uttar Pradesh
Noida, India.
surbhiamity15@gmail.com

Abhishek Singhal
Department of CSE
Amity University Uttar Pradesh
Noida, India
asinghal1@amity.edu

Akanksha Kapoor
Department of CSE
Amity University Uttar Pradesh
Noida, India
akankshakapoor75@gmail.com

Abstract— **Phishing is a network type attack where the attacker creates the fake of an existing webpage to fool an online user into elicit personal Information. The prime objective of this review is to do literature survey on social engineering attack: Phishing attack and techniques to detect attack. Phishing is the combination of social engineering and technical methods to convince the user to reveal their personal data. The paper discusses about the Phishing social engineering attack theoretically and their issues in the life of human Beings.Phishing is typically carried out by Email spoofing or instant messaging. It targets the user who has no knowledge about social engineering attacks, and internet security, like persons who do not take care of privacy of their accounts details such as Facebook, Gmail, credit banks accounts and other financial accounts. The paper discusses various types of Phishing attacks such as Tab-napping, spoofing emails, Trojan horse, hacking and how to prevent them. At the same time this paper also provides different techniques to detect these attacks so that they can be easily dealt with in case one of them occurs. The paper gives a thorough analysis of various Phishing attacks along with their advantages and disadvantages.**

Keywords—Phishing attack; Social engineering attack; spoofed email; Personal data;

I.INTRODUCTION

The main aim of information security is to protect the sensitive information from the social engineering attack such as phishing attack, and money laundering. Social engineering attack is an art of manipulating the people who have less knowledge about these types of attack. Every organization has security issues thathave been of great concern to users, site developers, and specialists, in order to defend the confidential data from this type of social engineering attack.

Phishing is a serious problem in the progressively limitless service of the internet. There are many ways to trick the people to disclose the information from the user by using social engineering attack [1]. Phishing attack is one of the common and popular amongst all. In this, the attacker bait the users by sending mails such as prize winning, send message from fake account on social networking sites, hacking password , send emails to victims which seems like it is sent by banks to disclose the information for financial gain. For Example, the attacker sends you an email such as "you have won a prize", in this mail they define some causes such as you have won the Rs.10000000 and your mobile number is selected randomly by the computer so fill the given information. Fake details such as, we will transfer the money directly in your account are given. They ask the account number, credit card number and the password etc. in order to capture our details. It uses social engineering techniques with brilliantly arranged tricks to bait users for elicit data. The bait can be delivered message, phone, and spoofed emails. Phishersend spoofed emails to millions of internet users in hope that at least a few of them might bite it. It targets the people who don't have Knowledge about online attack, Internet security and make them believe that the emails are coming from true organization. Phishing attacks main aim is to find the weaknesses of the target user. Attacker always finds the ways that causes users to visit a phishing website. The Spoofed emails are designed in such a manner that they often look professional and the users are easily targeted and befooled.

This paper consists of four sections. First section consists of introduction; section 2 illustrates Literature Survey and types of Phishing attacks, Section 3 explains widely Prevention from Social engineering attacks, Section 4 explains Analysis on social engineering attacks detection techniques, followed by Conclusion in Section 5.

II. LITERATURE SURVEY

Phishing attack is a cybercrime; the attacker manipulates people to elicit their personal data. It is a great security issue in the society. There are many techniques and numbers of solutions present today in order to prevent from these types of attack; however users are providing personal information on phishing webpage making it difficult for Programmers. Many toolbars are available for different browsers which attempt to warn the people of likely phishing sites, attempting users to further open them. Now this attack is known as spear phishing. It makes harder for users to distinguish between legitimate and spoofed email. Spoofed email being starting of Phishing attacks causes great harm to user's authentication.

ISBN:978-1-5090-1666-2/16/$31.00 ©2016 IEEE

Various types of Phishing Attacks are:-

*A. Spoofing email:*it is a type of phishing attack. Spoofing is when a spammer sends you an email using other email address. It seemslike that the message is for them, and tricks people into opening it [4].
Email spoofing is possible because of SMTP(simple mail transfer protocol), It is used in sending mail, doesn't include an authentication process.[12] So this type of attack can be manipulating user easily to disclose the secret information by reading (sometimes even clicking) that e-Mail.

B. Fake Social Network Accounts: The end users of social sites such as facebook, twitter, LinkedIn, orkut are not conscious about their accounts. A fake account is easily created on social networking sites [2] by the attacker. By these fake profiles, the attacker can access to secret data that the user discloses when he creates an account. These popular networking sites have policies against fake accounts however there are many fake accounts still available on these sites, because they have a lack of real system which determines the validity of user [7]. Eg: - The attacker creates a fake account with associative women name and her picture or famous athlete. This fake user sends the request to the target, fooling them and portraying her to be the popular athlete.

C. Hacking: A hacking is any technical effort to manipulate access the system or resources. A hacker is a person who engages in that process. Hacking and hacker are most commonly association with malicious programming attacks on the internet. Hacker can be motivated by a multiple of reasons such as challenge, profit and enjoyment [13]. Hackers use vulnerability scanner and port scanner to check computers on a network for known weaknesses [6]. In this type of attack, the hacker may use Brute Force attack, Password cracking, dictionary attack for obtaining passwords from data. In this, Social engineering is very efficient, because the users are most vulnerable part of an organization. If an employee reveals a password to an unauthorized person, No security device can keep an organization safe. So the user is the weakest point in the security.

D. Trojan horse: Trojan horse attack is the most deliberate threat to the system security. Trojan is the executable program, example: - when you click on any file, it will implement some action. There are many ways to fool someone easily. It is a set of line of code, contained inside apparently harmless programming which is harmful for the system. It is a type of program (code) designed in such a way that it can get control over the system, example: - running the file allocation table on your hard disk. There are many job offers present which requires the person to enter their personal information and their security numbers. Eg:- scammer use false banking sites to offer lower credit costs or better interest rate than other banks. Victims who fill the information with the dream to save money or make more from interest charges are encouraged to transfer existing accounts and fall prey to Trojan horse attack.

III. APPROACHES TO PREVENT PHISHING SOCIAL ENGINEERING ATTACK

A. Spoofed Email Detection: - There is no way to stop email spoofing. Only possible trick is to set your spam filtering to identify spoofed email. The best method to stop Phishing is to block malicious emails before reaching the customer with DMARC (Domain based message Authentication Reporting and conference)[14] by the company. Do not trust display name of the email because many attacker use brand name. Attacker also uses spelling mistake method to make a fake email. In this type of emails only "anchor test" is shown in the web browser but not URL. Link Guard algorithm [7] is used to solve that type of situations. The characteristics of links of phishing emails generate an algorithm with a set of rules such as finding hyperlinks with the difference of actual link.

B. Fake social networking accounts detection:
Social networking sites have many rules against creating fake profiles but there is lack of a right conformity to identify the user [8]. In, this attacker makes their fake account to manipulate someone. The user usually shares their personal information in their profile and status. They give chance to hacker to assemble the information about them in order to perform spear phishing. For example: if a user were to post something simple as "I Love Football" a potential hacker could take the information and make a unique spear phishing attack intended for the user[9]. To prevent this type of attack, the user should maintain a constant awareness of what they post, what they share, and user must be especially aware of media that they share with others through the use of links.

C. Hacking Detection: - Detection of hacking attack is not a simple task. Especially for that type of users who have no information about accounts security and no knowledge about internet attacks. The most important thing is that to keep your password as a secret. If you give your password to someone, you should change your password after they are done using its access. Our personal computers should not have any type of virus or key logger etc. for this one must download updated programs, software, and anti-viruses from a trusted site. One must keep upgraded versions of the latest anti-virus software for their computers and blogs[16].You should be aware while using internet; your email can be hacked if you click on a fraud link. Your password strength should be strong that can't be easily guessed by the attacker. It is especially important to keep your banking and other financial accounts password to be secure and secret. You have to use antivirus software to prevent from these types of attack. Antivirus software is crucial to keep your computer good and healthy. The password should be 3D; it can use numbers, alphabet and special character.

D. Trojan horse detection: -There are some points to prevent system from Trojan horse.

- You must be careful when you download a file from the internet, it is often just a matter of time before you fall victim to a Trojan horse.
- If a file comes from your office friend, you must be confident what the file is, before disclosing it because many Trojans will try to spread themselves in the friend list using an email address book.
- You should take care of hidden file extension, windows hides the last extension of a file by default. Eg: looking as "Susie.jpg" may be "Susie.jpg.exe"- it is an executable Trojan, this helps to reduce the chances of being tricked .

IV.ANALYSIS OF SOCIAL ENGINEERING ATTACK DETECTION TECHNIQUES

Other techniques to preventing phishing attack and their result, we discuss some technique which is used to prevent from social engineering attack as phishing attack. Now day's phishing have become too smart such that sometimes skillful people can't be able to distinguish between suspicious and legitimate pages then we used surf [9] technique to distinguish.

Sr. No	Techniques	Developer	Year	Methodology	Advantage	Disadvantage
1.	SURF(speed up robust Features)[11]	Herbert Bay	2006	It is a feature detector technique that can be used as object recognition, registration, and 3D reconstruction. We used this technique to compare the similar point between legitimate and suspicious pages.	Matching speed is good. It takes Less computation and it is short time consuming process.	There are more chances of false matching point and less accuracy in the surf process.
2.	SEADM(social engineering attack detection model)	Monique Bezuidenhout	2010	This model is based on decision tree by breaking the process into more manageable component and guidelines to make decision. In this, they describe the emotional state of the user when he takes a decision in the social engineering attack process.	To Be Experienced in this type of attack.	Less knowledge about this type of attack. Totally depend on mind making decision.
3.	Ontological model to detect social engineering attack[12]	Francois Mouton	2014	In this model we describe about an attack framework how the attacker easily targets the user and what is the process to be done by the attacker. The process of this model is based on kevinmitnick's social engineering attack cycle.	Provide depth knowledge about social engineering attack. This frame work is used for education and awareness purpose.	This model doesn't provide security to the information but its help us to how can I prevent our data.
4.	Anti Phishing tool	Jordan crain	2010	These tools are effective in identifying phishing websites but even if they were mostly correct, user ignore their warning anyway.	Protected from all attack factors, provide a reliable means of detecting phishing emails.	Lack of knowledge (many number of user can't understand that type of warning).
5.	Authentication technique to reduces phishing attack	SudanthaGunawardena	2013	In this we used steganography techniques to hide our profile. The password strength should not be weak. This methodology is that the user password may be an image that is the authentication process to identified user.	It is more secure technique to hide our password from the attacker.	For password securing no proper formwork is suggested in social engineering.
6.	Link Guard Algorithm[17]	NareshVidya Sagar	2013	This technique is used to analyzing the difference between visual and actual link. It is also used to calculate the similarities of a URI with a legitimate website(trusted site)	The false negative point is less in this technique and 95% phishing website is recognized by this algorithm.	The main disadvantage of this technique is that it works with windows XP. Now, many users are using widow's other version e.g. windows7, windows 8 and windows 10.

V. CONCLUSION

Social engineering attack as we discussed is a technique where attackers try to manipulate or fool users. Our paper dealt with one of the most common type of Social Engineering attack named Phishing Attack. Phishing attack is very difficult to detect because many people are unaware of it. There are many numbers of tools present to identify a phishing websites which warns the clients about the malware present in the website, but most of the users ignore the warning. There are many techniques to detect social engineering attack however we cannot stop it. We discuss in our paper types of phishing attack and how to prevent from it. How can people escape from attacks and what they can do in such type of situation?

One solution to these attacks is that the user should copy the linkand open it with a new browser; from this the user can recognize that the webpage is suspicious or legitimate. There are a number of open source websites available which identifies the authenticity of the link, website, or a webpage.

Apart from this there are many algorithms which can be used to detect Phishing attack, example: - link guard algorithm and surf detector. Though there is a weakness associated with these algorithms, they have been implemented up to windows XP only. In future we would like to implement it for the windows 7, 8, 10 and updated windows versions, since most of the users today use these versions.

REFERENCES

[1] F. Mouton, M. Malan, L. Leenen and H.S. Venter, "Social Engineer Attack Framework," IEEE Conference on Information Security for South Africa , 2014, pp. 1 - 9.

[2] J. Allen, L. Goman, M. Green, P. Ricciardi, C. Sanabria and Steve Kim, "Social Network Security Issues: Social Engineering and Phishing Attack ," CSIS, Pace University , 2012, pp. B1.1 - B1.7.

[3] M. Bezuidenhout, F. Mouton and H. S. Venter," Social Engineering Attack Detection Model: SEADM," IEEE Conference on Information Security for South Africa, 2010, pp. 1 - 8,

[4] S. H. Gunawardena, D. Kulkarni and B. Gnanasekaraiyer, "A steganography-based Framework to Prevent Active Attacks during User Authentication," 8thInternational Conference on Computer science & Education (ICCSE), 2013, pp. 383 - 388.

[5] R. S. Rao and S. T. Ali," A Computer Vision Technique to Detect Phishing Attacks," Fifth International Conference on Communication System and Network Technologies, 2015, pp. 596 - 601.

[6] C.handnogy and P.willson, "Social Engineering: The Art of Human Hacking," Wiley, 2010

[7] J. Chen and C. Guo, "Online Detection and Prevention of Phishing Attack", First International Conference on Communication and Networking in china, chinacom06, 2006, pp. 1 – 7.

[8] B. Zhang, Y. Jiao,Z. Ma, Yongchen Li and Junchao Zhu "An Efficient Image Matching Method using Speed Up Robust Features," IEEE international Conference on Mechatronicsand Automation(ICMA), 2014, pp. 553-558.

[9] H.Bay, T.Tuytelaars and L. Van Gool, "SURF: Speeded UP robust Features." European Conference on Computer Vision (ECCV), Springer Berlin,2006, pp. 400-417.

[10] F. Mouton, L. Leenen, M. M. Malan and H.S. Venter, " Towards an Ontological Model Defining the Social Engineering Domain" 11th Human Choice and Computers International Conference, Turku , pp. 266 - 279, July 2014

[11] M. Fujikawa and M. Nishigaki, "A Study of Prevention for Social Engineering Attacks using Real/Fake Organization's Uniforms," Sixth International Conference on Availability, Reliability and Security , 2011, pp. 597-602

[12] searchsecurity.techtarget.com/definition/email-spoofing{accessed.online 10 October, 2015}

[13] https://en.wikipedia.org/wiki/hacker {accessed. online 28 October, 2015}

[14] https://blog.returnpath.com/10-tips-on-how -to-identify-a-phishing-or-spoofing-email-v2 {accessed. online 2 December, 2015}

[15] searchsecurity.techtarget.com/definition/Trojan-Horse {accessed. online 12 November, 2015}

[16] [www.wikihow.com/prvent-hacking {accessed. online 12 January, 2016}

[17] U. Naresh, U. VidyaSagar and C. V. Madhusudan Reddy, "Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm" IOSR Journal of Computer Engineering (IOSR-JCE) 2013, vol. XIV, pp 28-36

[18] www.wikihow.com/Tell-if-Your-Computer-Is-Infected-by-a-Trojan-Horse {accessed. Online 17 January , 2016}