International Journal of Computer Applications (0975 – 8887)
Volume 182 – No. 33, December 2018

Study on Phishing Attacks

Vaishnavi Bhavsar
Ajeenkya D Y Patil University, Pune

Aditya Kadlak
Ajeenkya D Y Patil University, Pune

Shabnam Sharma
iNurture Education Solutions, Bangalore

ABSTRACT
Now a day there is a lot of data security issues. Hackers are now very much expert in using their knowledge for hack into someone else's system and grab the information. Phishing is one such type of methodologies which are used to acquire the information. Phishing is a cyber crime in which emails, telephone, text messages, personally identifiable information, banking details, credit card details, password is been targeted. Phishing is mainly a form of online identify theft. Social Engineering is being used by the phisher to steal victim's personal data and the account details. This research paper gives a fair idea of phishing attack, the types of phishing attack through which the attacks are performed, detection and prevention towards it.

Keywords
Social Engineering, Phishing, Cyber Crime.

1. INTRODUCTION
Phishing is the act of attempting to payoff information such as username, password and credit card details as a trustworthy entity in an electronic communication. Communication purporting to be from popular social websites, auction sites, online payments process or IT administrator is commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware.

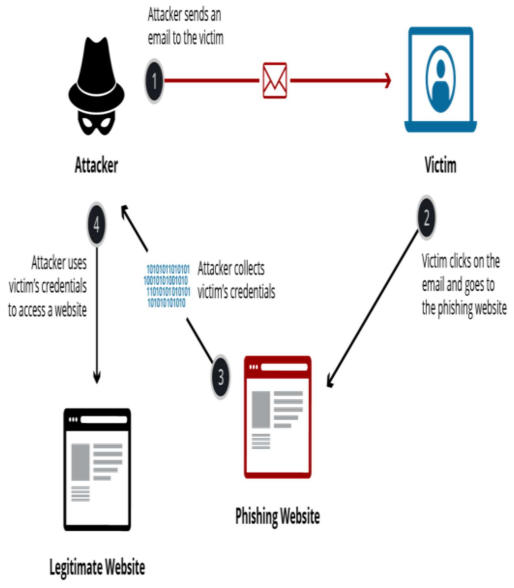

Fig.1

Phishing is an example of Social Engineering. Phishing is mainly used in email hacking, in email phishing the hacker send a link via mail to the user of let's say some bank details or any personal information, so now the user goes to that link and fills all the detail in that link and then the hacker gets all the information of the user. This is how phishing is done. As explained in the fig1.[11].

Phishing is explained step-by-step:

1. Attacker sends an email to victim.
2. Victim clicks on the email and goes to phishing website.
3. Attacker collects victim's credentials.
4. Attacker uses victim's credentials to access a website.

Fig.1

Phishing starts with an email or other communication type that designed to help in attacking the victim. The message is made as if that message is coming from a trusted sender. If it fools the victim, the victim is providing the personal information to a spam website. Sometimes malware is also downloading onto the target's computer.

2. LITERATURE REVIEW
The paper [1], phishing attack is being discussed in detail, history of phishing attacks and motivation of attacker behind performing this attack. Detection of phishing attacks with high accuracy has always been an issue of great interest. Recent developments in phishing detection techniques have led to various new techniques, specially designed for phishing detection where accuracy is extremely important. Phishing problem is widely present as there are several ways to carry out such an attack, which implies that one solution is not adequate to address it.

In paper [2], in this paper deceptive phishing attack is discussed. Deceptive phishing is the most common type of phishing scam. These scams occur when a recognized source emails you in order to compromise information. Typically, these emails request that you: Verify account information. Re-enter information, such as logins or passwords

In paper [3], here Deceptive Phishing Detection and prevention in Social Networking sites Using Data Mining and Word Net Ontology. Deceptive Phishing is the major problem in Instant Messengers, much of sensitive and personal information, disclosed through socio-engineered text messages for which solution is proposed[2] but, detection of phishing through voice chatting technique in Instant Messengers is not yet done which is the motivating factor to carry out the work and solution to address this problem of privacy in Instant Messengers (IM) is proposed using Association Rule Mining (ARM) technique a Data Mining approach integrated with Speech Recognition system.

In paper [4], here discussion is about Browser Vulnerabilities Browser, like any commercial software, is subjected to vulnerabilities, which can be exploited by the phisher to launch a phishing attack on the user. With every addition of new features and functionality to the browser, there are possibilities of introducing vulnerability to the software (Ollmann, 2004). Furthermore, the ability to install add-ons and plug-ins from third-party providers has led to more

vulnerability in the browser. Such phishing attacks through browser vulnerability are harder to detect and prevent.

In paper [5], in this paper the review of some recent attacks happened through the phishing techniques

In paper [6], in this paper, how to detect and prevent the phishing attacks online is discussed. . Lexically analyzing the URLs can enhance the performance and help to differentiate between the original email and the phishing URL. As assessed this study, in addition to textual analysis of phishing URL, email classification is successful and results in a highly precise anti phishing.

In paper [7], the article proposes and justifies a trial classification scheme. Requirements engineering is the branch of software engineering concerned with the real-world goals for, functions of, and constraints on software systems. It is also concerned with the relationship of these factors to precise specifications of software behavior, and to their evolution over time and across software families

In paper [8], Phishing is an email-based scam where a perpetrator camouflages emails to appear as a legitimate request for personal and sensitive information. This paper draws upon the theory of deception and the literature on mediated cognition and learning, including the critical role of attention and elaboration in deception detection.

In paper [9], in this paper a novel framework using a Bayesian approach for content-based phishing web page detection is presented. Their model takes into account textual and visual contents to measure the similarity between the protected web page and suspicious web page.

In paper [10], this paper the highlights of a user study which gauges reactions to a variety of common "trust indicators" principle result is the analysis of what makes phishing emails and web pages appear authentic.

After going through all the above research endeavors, various types of phishing attacks are explained, its prevention and detection.

3. TYPES OF PHISHING ATTACK

3.1 Deceptive Phishing

This is a most common type of phishing, in this type the attackers impersonates a legitimate company and try to steal people personal information or their login passwords. And then they blackmail the users to do as the hacker wants.

3.2 Spear Phishing

Wireless based Intrusion Detection Prevention System analyses the traffic of wireless network by analyzing wireless protocol activities and take appropriate actions. It detects unauthorized wireless local area network in use. It cannot identify suspicious activity in the application layer, transport layer and protocol activities. It is deployed in a particular range where the organization can monitor the wireless network.

3.3 Clone Phishing

Clone phishing is one of phishing attack where a legal or a previously gained email contains the attachment and link shared, recipients address (es) taken and used to create the same identical or cloned email. That attachment or link within the mail is replaced with some external malicious version and then sent it to the victim from email address spoofed to appear to come from the original sender. This technique can be used to pivot (indirectly) from the infected machine and take all the information or can gain a foothold on another machine.

3.4 Whaling

Whaling is one of the types of phishing, in this type of phishing the attacker aims at a wealthy and powerful status of the victim or user; the attacker takes out all the information of the victim using different medium such as social media accounts and then attacks the victim. The victims of this type of attack are also called as "*Whales*" or "*Big Phish*". Whale phishing involves the same tactics used in Spear Phishing.

3.5 Link Manipulation

Link Manipulation is a type of phishing attacks; in this type of attack the phisher send a link to a spoofed or malicious website. When the user opens that link, the link open ups in the phisher's website instead of opening it into the website mentioned in the link. Taking the mouse on that link to view the actual address stops users from falling for link manipulation.

3.6 Voice Phishing

Voice phishing is a form of phone criminal attack it is done using social engineering with the use of telephone system to look at to the private personal and financial information for the use of financial work it is also referred as "vishing".

4. PREVENTION OF PHISHING ATTACK

Phishing attacks are usually presented in the form of spam or pop-ups and are many times difficult to detect it. Once the attacker takes your personal information, they can use it for all the types such as identify theft, putting your good credit into bad once. Because phishing is one of the most devious forms of identity theft, it is important for us to become familiar with various types of phishing attacks and also know that what the prevention on it are. Some of them are explained in subsequent sections.

4.1 Guard against spam

In this type of prevention method, the attacker comes from unrecognized senders. They ask you for confirmation of personal or financial information over the internet and make requests for giving your information.

4.2 Communicate personal information only via phone or secure web sites

In this type of phishing prevention, the user should be aware of while conducting online transactions, look for the secured sign on the browser status bar or" https." URL where the "s" stands for "secure" rather than' http.".

4.3 Do not click on links, download files or open attachments in emails from unknown sender

It is always best to secure any data properly data such as bank details any social media details, in emails also open the attachment only if when you are expecting them and known what that attachment contains even if you the sender.

4.4 Sound security policies

In the big organizations or companies, you should set some rules as to how you should respond to strange or out of place emails and requests. Your company's policy should also show people what to do in case they see something out of place.

4.5 Security Awareness Training

Teach the employees about good emails look like, teach them and show them how a bad email looks alike. Mange and teach the staff about the phishing attack and their preventions. At the end the educating users is that going to reduce the success of attacks and testing will make sure security and management know how to respond.

5. DETECTION OF PHISHING ATTACKS

The internet is a wide source of mankind to do anything, but Facebook, Twitter, Gmail, Dropbox, PayPal, eBay, bank portals, and so many sites have twins that are actually phish. A "Phish" is a term for spoof websites which tries to look like as if it is an authorized website which you know well and often visit. Some of the methods for phishing detection are mentioned below:

5.1 Use a custom DNS services

In this type of the detection type the user can use theDNSresolution service so that user can access all the sites that he/she goes to. Your computer doesn't know where your Facebook is (as far as its Internet address, or IP address, goes), so it needs to ask a DNS resolution service for that IP address. Aside from name resolution, the DNS servers at ISPs do nothing else. However, there are some custom and independent DNS companies that do more than just name resolution. They filter the site on the bases of the content and malware or phishing concerns.

5.2 Use your Browser's phishing list

Now-a-days the modern browsers offer us a phishing list. In that list the browser checks the site you are visiting or you have visited, if possibly it is a phishing site. So, always check out before visiting any other sites.

5.3 Use sites to check links

Many a times when working on any site or any program there is a pooping of different kinds of links, or in case you're presented a link or which you are not so sure, you can copy and check it on a number of different sites. That can tell you whether there's something bad about that site, including malware and phishing.

5.4 Use your own Ninja skills

This may sound useless but use your own skills to detect the phishing attack, and may even prevent you from any mankind of malware or phishing sites that haven't made it in to your list the would throw an immediate flag. There are few things that should look for to see if you're being faked:

5.5 1 Look for secure connections

This is usually identified by a green area in the address bar, along with https in URL.

5.6 Look at the domain of URL

Look at the domain that it should not be modified or changed.

5.7 Look at the site itself

If it doesn't look exactly like the site, we are fa miliar with, then it is a scam. You can open that site in new tab and check out about it.

6. CONCLUSION

For Phishing attack, there are many ways to launch the attack. Here the research focuses on developing a detection and prevention techniques so that in future the client can take necessary actions to prevent phishing attacks. In this work, various types of attacks and their prevention and detection are studied. In future, focus is to compare various tools for phishing attack prevention.

7. REFERENCES

[1] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

[2] Huang, H., Zhong, S., & Tan, J. (2009, August). Browser-side countermeasures for deceptive phishing attack. In *2009 Fifth International Conference on Information Assurance and Security* (pp. 352-355). IEEE.

[3] Ali, M. M., Siddiqui, O. A., Nayeemuddin, M., & Rajamani, L. (2015, January). An approach for deceptive phishing detection and prevention in social networking sites using data mining and wordnet ontology. In *Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on* (pp. 1-6). IEEE.

[4] Raffetseder, T., Kirda, E., & Kruegel, C. (2007, May). Building anti-phishing browser plug-ins: An experience report. In *Proceedings of the Third International Workshop on Software Engineering for Secure Systems* (p. 6). IEEE Computer Society.

[5] Yadav, S., & Bohra, B. (2015, October). A review on recent phishing attacks in Internet. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1312-1315). IEEE.

[6] Chen, J., & Guo, C. (2006, October). Online detection and prevention of phishing attacks. In *Communications and Networking in China, 2006. ChinaCom'06. First International Conference on* (pp. 1-7). IEEE.

[7] Zave, P. (1995, March). Classification of research efforts in requirements engineering. In *Proceedings of 1995 IEEE International Symposium on Requirements Engineering (RE'95)* (pp. 214-216). IEEE.

[8] Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication*, *55*(4), 345-362.

[9] Zhang, H., Liu, G., Chow, T. W., & Liu, W. (2011). Textual and visual content-based anti-phishing: a Bayesian approach. *IEEE Transactions on Neural Networks*, *22*(10), 1532-1546.

[10] Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007, February). What instills trust? a qualitative study of phishing. In *International Conference on Financial Cryptography and Data Security* (pp. 356-361). Springer, Berlin, Heidelberg.

[11] https;//goo.gl/images/rGh3J8.