Social Engineering Attacks: A Phishing Case Simulation

Ammar Naser, Mahmoud Jazzar, Derar Eleyan, Amna Eleyan

Abstract: In this paper, we discuss phishing as one of the attack types used in social engineering. Phishing attacks will be discussed by simulating a process between two different devices in two different networks. An experimental penetration test was performed on one of the local network devices to obtain data and information of the victim. The experiment involves sending fake email containing a link to a fake website in order to persuade the victim to enter personal data logs into the fake website. The experiment illustrates the ways in which an attacker may defraud the victim. In addition, the experiment contributes to the protection from and avoidance to exposure of this type of attack.

Index Terms: Phishing, Phishing Cyber Attacks, Phishing Simulation, Social Engineering, Social Engineering Virtualization, Social Engineering Attacks, Social Engineering Tools.

1 INTRODUCTION

THE availability and accessibility of the Internet has contributed to the development of many software tools related to all facilities of human life. As such, many issues have become easier and more flexible to deal with through the Internet. This is evident in the field of scientific research, industries, electronic commerce, medicine, shipping, aiding and services remotely. The unlimited presence of services provided by many organizations and companies over the Internet has become something that cannot be ignored and is necessary for many individuals and companies. The spread of the Internet globally, has turned the world into a small virtual community. For example, individuals can access the Internet from anywhere at any time. This include working remotely, shopping from homes, delivery, ordering services, and requesting information and data through the Internet. Information and data are the most important things that organizations and companies deal with these days. They rely on this information in order to make important decisions and market products based on this information. Therefore, Internet must be maintained and protected because of the spread of this information which may leads to major problems. Many organizations and companies offer several standards to protect their information and data. One of the most important of these standards is ISO27002, ISO27001. Despite of many measures and procedures that companies undertake, information and data are sometimes penetrated and stolen. As such, individuals are considered the weakest link. This paper contributes to such issue and illustrate by experiment on how to protect and avoid the exposure to this type of attacks and penetration on individual and organisational machines.

- *Ammar Naser is currently pursuing masters degree program in Cybercrime and Digital Evidence Analysis in Palestine Technical University - Kadoorie, Palestine, E-mail: aydawabsheh@gmail.com.*
- *Mahmoud Jazzar, Faculty of Graduate Studies, Palestine Technical University - Kadoorie, Palestine, E-mail: mjazzar@ptuk.edu.ps.*
- *Derar Eleyan, Faculty of Graduate Studies, Palestine Technical University - Kadoorie, Palestine, E-mail: d.eleyan@ptuk.edu.ps.*
- *Amna Eleyan, Department of Computing and Mathematics, Manchester Metropolitan University, E-mail: a.eleyan@mmu.ac.uk.*

The purpose of this experiment is to illustrate on how social media users, and secure website users may request user-name and password for login. In addition, to illustrate the danger of phishing and for the awareness of the misuse of online links, strange messages and pay attention to the sources and senders. Furthermore, caution is required while browsing websites to anticipate the worst events when providing the username and password to any destination. The rest of the paper is organized as per the following: next section illustrates the related research works and background on social engineering attacks which can be understood as a technique to manipulate people, by deception, into giving out information, or performing particular action [1]. The next section discusses social engineering types followed by the methodology, experiment details and overall discussion. Finally, the concluding remarks are presented.

2 RELATED WORK AND BACKGROUND

2.1 Related works

According to [2], information can be considered such as lifeblood of organizations and individuals. On the other hand, threats to information systems have existed for a long time, however, the means by which a threat is made may differ as if the threat is through the local network. In general, there are many threats used against information systems to be considered such as phishing. Some of these threats are internal and others are external, i.e., as that they come from outside the network of the organization. Threats can arise from one person or from a group of people internal or external such as malicious or ignorant employee who may destroys the organization without intention [2]. Nowadays, cybersecurity has become of critical importance for the global economy because there are many areas and businesses that rely mainly on computer and Internet systems. As example, the trade via the Internet, vehicle engine systems, smart phones, e-mail, the development of the Internet of Things, and many other areas. Cybersecurity will become more important in all areas worldwide. Reports of threats and attacks through security companies indicate increasing attacks whether on individuals or on organizations and companies who lose large sums of money due to these attacks. Social engineering attacks use various possible technologies to extract sensitive information from the victim. The aim of social engineering

attacks is to obtain information regardless of the method. In this research, we will discuss one of the most famous attacks known as Phishing Attack and will simulate this type of attacks as social engineering attack. Experimentally, we will simulate phishing as it happens in real life using virtual machine (VM ware). Few researches work discussed the simulation of phishing attacks. However, most of the available literature proposed simulations tests are applied locally and barely applied on different networks such as in [3] using local IP address for experimentation. In this paper, the focus is on attacks on victims in different network connections with different Internet service providers (ISPs) in order to mimic real case scenario. There are few researches works use Spear-Phishing attack for phishing simulation. This type of simulation demonstrates on how to specially craft email messages and send them to a large (or small) number of people with related attached malicious files [4]. In this paper, the experiment focusses on the use of the website attack vector module as example on using Internet pages to compromise particular target. As such, a module was chosen for the triggered severity. Plus, the hacker may build trust relationship with the victim tracks, manipulate the victims' data through fake sites similar to the original site using several methods.

2.2 Social Engineering

Social engineering can be defined as the ability and the behavior of attacker to convince the victim toward fake connection. According to [5], the attacker can manipulate the victim by making relationship based on trust. As such, attackers can easily access vital human information due to the weak security measures. A social engineer manipulates and deceives people by using any available technique in order to influence people's minds and deceit by changing their thinking and opinions on specific scenario with specific aims. Many social engineering hackers succeed in their different ways by changing the belief of many people on many issues. Social engineers can provide victims with false information similar to the information that leads to confusing and thinking properly. They also take advantage of the fact that people can bypass procedures in emergencies and necessities. The social engineer can use the technique of urgency and intimidation to get clients to act quickly. Cyber criminals may use many methods of deception on victims such as emboldening click on certain links without thinking. Figure 1 below illustrate the stages of social engineering attacks. The process of collecting information is the basic stage of any social engineering attack. In general, social engineering attacks can be classified according to different goals. As such, each attack has different goals depending on determining the correct target and the appropriate sources of data and information. The first stage of the attack usually includes gathering correct information and the proper purpose of the target. In addition, this stage includes the mission and the validity of the information associated with the target. The goal is usually chosen based on investigation techniques and on building relationships with the target audience to gain confidence. For example, it is easy to obtain information about an organization such as general information obtained from official websites and relevant social media accounts. This information includes and not limited to the number of employees, job opportunities, job location, department managers, email addresses, and upcoming events.

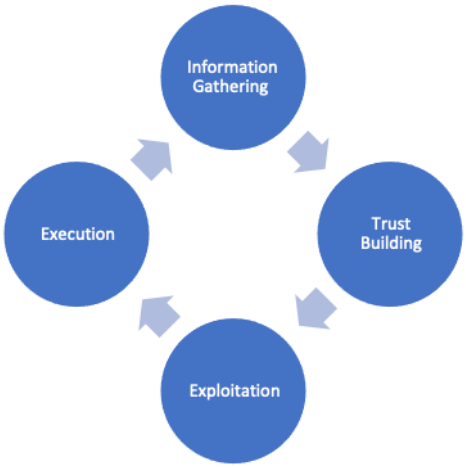

***Fig. 1**. Stages of social engineering attacks.*

Social media is considered as gold mine to obtain information about cyber users. This is an easy and ideal source for obtaining information about victims' personal information's such birthdays, legal names of family members and friends, identities and images that can be accessed using social media sites such as (Facebook, Twitter, and LinkedIn). On the other hand, attackers may use available tools for information gathering such as Maltego [6] which is nothing but an open-source intelligence software for data mining and knowledge discovery. The tool can be used professionally for link analysis and data forensics.

2.3 Types of Social Engineering

As illustrated in Figure 2 below, human-based social engineering and technology-based social engineering are considered as major types of social engineering. Human-based social engineering is achieved based on human-to-human connection and on relevant relationship. This can include attacks based on dumpster diving and shoulder surfing. On the other hand, technology-based social engineering is achieved using an electronic connection such as email, web, and social media connection. Generally, the demand on human based social engineering is on the rise due to the continuous protection improvements against technology-based threats [7]. Dumpster diving: It is the process of sifting waste for individuals and companies in order to find any neglected items that contain important information to be used such as usernames and passwords or any other sensitive information's [8]. Shoulder surfing: The purpose is to monitor and directly to obtain information such as looking from the back of a person for viewing the machine screen or keyboard [8]. Baiting attack: Attackers may leave the storage media containing malware located in someplace reachable by victims. The media is just like "road apples" such as leaving USB drive containing Trojan horse at the entrance of a company to attract any staff member to insert it into the organization computer [8].

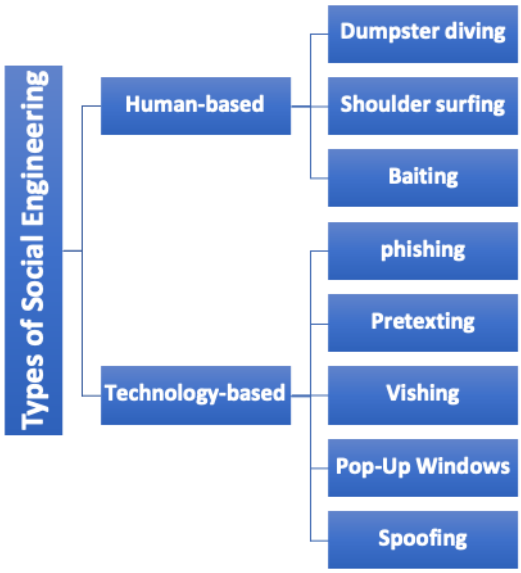

***Fig. 2**: Types of social engineering*

Phishing: The practice of collecting data and information illegally by sending fake messages through email or through any other type of electronic communication. The electronic connection usually appears to be from a reliable and legitimate source. The issue here is when the victim will be directed to use a fake link designed specifically to obtain the victim personal and confidential information [5]. Pretexting: This is usually based on the principle of simple scenario. The scenario is usually presented to the victim to participate in a vague work that urges the victim to participate indirectly in providing free information hastily [9]. Usually, this scenario is well prepared and carefully considered to impersonate the victim. Such information includes date of birth, legal name, social number etc. Vishing: A type of phishing attack which is usually done via Internet Protocol (VoIP) to manipulate the victim and urge to provide sensitive and private information [10]. For example, well-known bank calls and official institutions calls prepared interactively to encourage the victim to respond. Pop-up window attacks: This type of attacks refers to the pop-up window that appear on the victim's screen to report lost connection to run malware directly on the victim's device remotely based on the consent of the victim [10]. Sometimes they come in the form of text messages addressed to the victim to inform about viruses or the like to attract the victim to interact, download harmful programs and run such programs on the victim's machine with the help of the victim himself. An example on this type of attack includes informing the victim about the available storage space or the necessity of updating certain programs in order to access and activate malicious codes on the victim device. Spoofing: This type of penetration and fraud attacks relies on more than one way to reach the source machine [11]. Attackers may present themselves in smart way to camouflaging the victim through e-mail and or other means of electronic communication. There are different means in which attackers may think in order to perform such fraud attacks such as by altering and fabricating the IP address, DNS, and more.

3 METHODOLOGY

Experimental experience using sophisticated tools would highlight the importance of information for social engineering and phishing attacks. Nevertheless, the aim is to increase the awareness of social engineering attacks and phishing attacks by illustration and simulation of real-life scenario for such attacks. On the other hand, there are many security risks associated with phishing attack, which are likely to lead to huge losses for an organization or a person. Therefore, it is necessary to take many precautions to avoid this type of attacks [3]. For example, suppose that there is a financial manager working in a financial institution such that the manager uses similar password through his personal accounts and the accounts of the institution. In case that this person is exposed to fraud through his personal account and his password stolen, the accounts of the institution may also be at high risk. Such credentials are used to steal some customer data and even financial assets. The following diagram summarize the proposed experiment and steps as shown in Figure 3.

***Fig. 3**. Experimental stages.*

4 IMPLEMENTATION AND DISCUSSION

In the proposed experiment, we will use Kali Linux Virtual Machine (VMware) as experimenter tool [13]. Microsoft Windows 10 with latest update for victims' network, and Twitter website. Kali Linux is very popular, free and available social engineering tool kit. Kali Linux is an open-source operating system. Given an advantage to any user to develop his own tested phishing code with suitable internal security supported by Kali. The following illustrate the step-by-step experimentation scenario:

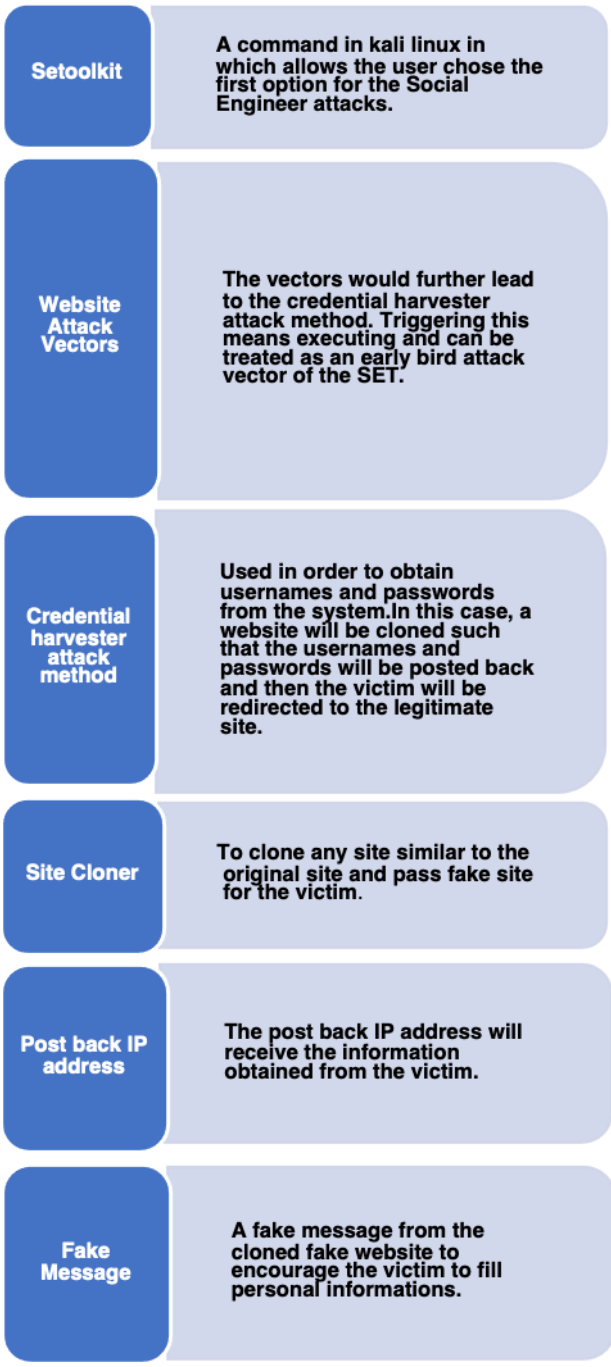

***Fig. 4**. Experimentation scenario.*

Setoolkit command was used in order to reach the Social-Engineer Toolkit (SET) interface as shown in Figure 5 below. The first option was elected in order to proceed.

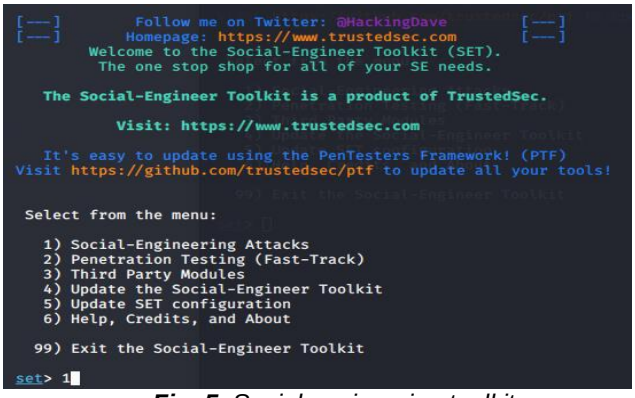

***Fig. 5**. Social engineering toolkit.*

The website attack vectors are available in stage two. The vectors would further lead to the credential harvester attack method. Triggering this means that we are executing and can be treated as an early bird attack vector of the SET. The credential harvester attack method is used when we do not want to specifically get a shell but perform phishing attacks in order to obtain usernames and passwords from the system. In this attack vector, a website will be cloned, and when the victim enters the user credentials, the usernames and passwords will be posted back to attacker machine and then the victim will be redirected back to the legitimate site [12]. The template and the site cloner to indicate the next move. The template can be accessed through the credential harvester attack menu. By choosing the site cloner, the toolkit asks the user to enter the IP address for the post back in the planned attack as well as to enter the web site in which we want to clone. This step may take several minutes according the chosen website. Initially, the choice was on twitter website as one of the most popular and famous websites. To implement the previous steps, i.e., in order to provide the toolkit with a public IP, we need to change some settings in TCP and UDP protocols in present router. At this stage, a fake e-mail needs to be prepared in order to lure the victim. As such, variety of social engineering methods and information gathering tools can be used to perform the job. An email should be delivered by the time in order to reach the victim screen. As such, a fake twitter website will appear to the victim screen for registration/login. Once confirmed, the browser redirects the victim to the original page of cloned twitter page and ask the user to login another time. The victim may think that there is an error in the data and would login again normally. Whether the victim was logged in or not, the username and password of the victim already set to the attacker as illustrated in the earlier steps. Figure 6 below demonstrate on the attacker authorisation for the victim data transfer.

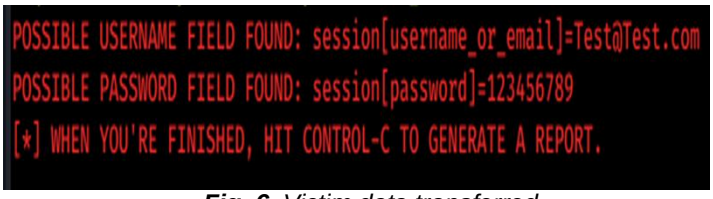

***Fig. 6**. Victim data transferred.*

It is important to mention that phishing can be carried out more professionally. As such, demonstrating real-life scenario would

be really harmful. It is possible to reserve a domain and a fake website similar to the original site with changing letters and more in site name such as in “Twittar.com”. However, convincing the victim by one of the methods of social engineering to enter and submit logging data is the issue. Experimentally, we have tested a fake e-mail in order to redirect the victim to fake site. As example, the experimental demonstration on how to manipulate the victim to enter Twitter account and then redirect the victim to the original Twitter website. In addition, it is important to note that most of the previous research work focus on local network environment for running experimental testing with relevant scope. However, very few research works have used public network and different Internet service providers in order to demonstrate real-life scenario for simulating a phishing case.

5 CONCLUDING REMARKS

Experimental demonstration illustrates that victim’s data can be successfully and easily reached on different network locations. However, the awareness of the user remains the issue. The outcome and the main purpose of this research work is to put hands on how the cyber world is very powerful and close to the user demand. The benefits and harms are varying. Furthermore, the tremendously rapid and dramatic technological development enabled social engineers to develop their methods and strategies. Therefore, there is no ideal hundred-percent solution against attacks that depend on social engineering. Users must be aware of the harms and benefits, organizations must develop their own polices, and have sufficient updated experience on how to identify any potential social engineering attack. Therefore, the ultimate organizational need is to increase cybersecurity professional population and focus on staff training and policy understanding. Future works should focus on dynamic policy development in order to stop or reduce this type of fraud attacks.

ACKNOWLEDGMENT

The authors wish to thank Palestine Technical University-Kadoorie (PTUK) for supporting this research work as part of PTUK research fund.

REFERENCES

[1] M. Mannan and P. C. Oorschot, "Security and Usability: The Gap in Real-World Online Banking," Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07. doi:10.1145/1600176.1600178

[2] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," 2015 International Conference on Cyberspace (CYBER-Abuja), Abuja, 2015, pp. 91-100, doi: 10.1109/CYBER-Abuja.2015.7360515.

[3] A. Pandey, “Phishing and Social Engineering Techniques,” Ethical Hacking- CC6051NI Final Report, 1998.

[4] TrustedSec, “The Social-Engineer Toolkit (SET),”Open Source Tools, https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/. Retrieved July 13, 2020.

[5] H. Aldawood and G. Skinner, “An Advanced Taxonomy for Social Engineering Attacks,” International Journal of Computer Applications, 177(30), 1-11, 2020, doi:10.5120/ijca2020919744.

[6] Maltego, https://www.maltego.com, Retrieved July 13, 2020.

[7] M. N. Sadiku, A. E. Shadare, and S. M. Musa,”Social Engineering: An Introduction,”Journal of Scientific and Engineering Research, 3 (3), 64-66, 2016.

[8] K. Krombholz, H. Hobel, M. Huber, and E.R. Weippl, “Advanced social engineering attacks,” J. Inf. Secur. Appl., 22, 113-122, 2015.

[9] C. K. Joe-Uzuegbu, U. C. Iwuchukwu and L. C. Ezema, "Application virtualization techniques for malware forensics in social engineering," 2015 International Conference on Cyberspace (CYBER-Abuja), Abuja, 2015, pp. 45-56, doi: 10.1109/CYBER-Abuja.2015.7360508.

[10] F. Salahdine and N. Kaabouch, “Social Engineering Attacks: A Survey,” Future Internet, 11(4), 89, 2019, doi:10.3390/fi11040089

[11] I. Belcic, “What is Spoofing and How Can I Defend Against it?,” https://www.avast.com/c-spoofing, Retrieved July 13, 2020.

[12] P. Boyanov and Z. N. Savova, “Implementation of Credential Harvester Attack method in the Computer Netwrok and Systems,” International Scientific Conference "Defense Technologies", Faculty of Artillery, Air Defense and Communication and Information Systems, Shumen, Bulgaria, Oct. 2019, ISSN 2367-7902.

[13] Kali, “Kali Linux Downloads,” https://www.kali.org/downloads/ Retrieved July 20, 2020.