www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 01, January 2023, pp : 18-20

e-ISSN : 2583-1062

Impact Factor : 2.265

SOCIAL ENGINEERING ATTACKS TECHNIQUES

Hassan Saad Fadhil[*1]

[*1]IT Engineer, Department of Computer Engineering, Mosul University, IRAQ

Email: computer.eng.hassan@gmail.com

ABSTRACT

The Social Engineering Attack is the most potent attack on systems because it involves psychology. Since neither software nor hardware can stop it or even defend against it, people must be trained to defend against it. Social engineering is quite possibly the greatest test confronting network security since it takes advantage of the normal human inclination to trust. The social engineering attacks, their classifications, and their strategies are all covered in depth in this paper.

Keywords: social engineering attacks, cyber security, phishing attack, social networks

1. INTRODUCTION

The term "social engineering" refers to a variety of methods that exploit the human vulnerability to obtain information and circumvent security systems. The human component of security systems is the "glitch," or vulnerable component, as various authors have stated clearly[1]. The art of tricking customers and employees into disclosing their credentials and then using those credentials to gain access to networks or accounts is known as social engineering. It is a hacker's skillful use of deception or manipulation to get people to trust, be cooperative, or just follow their curiosity and desire to learn. Systems cannot be shielded from what appears to be authorized access or from hackers using sophisticated IT security systems. Since people are easy to hack, they and the content they post on social media are prime targets for hackers. By luring computer users to spoof websites, tricking them into clicking on harmful links, and downloading and installing malicious software, backdoors, or applications, it is frequently simple to infect a company's network or mobile devices [2]. In the field of security, the term "social engineering" refers to a type of attack against the human element in which the perpetrator persuades the victim to divulge personal information or take actions they shouldn't [3]. Even though security measures to protect sensitive information are getting better, people are still easy to manipulate, so the human element is still a weak link [4].

2. SOCIAL NETWORKS

The Internet is now the most widely used medium for information and communication. In our day-to-day lives, we now communicate via a variety of online communication channels [5]. Social engineers now have a new disguise and become more "invisible" to victims and authorities in today's mobile and internet environments [6]. Social networking websites like Facebook, LinkedIn, and Twitter are unquestionably the online services that are expanding at the fastest rate right now. Today, social networks are among the largest and most rapidly expanding online services. Facebook, for instance, has been ranked as the second most popular website on the Internet and has reported weekly growth rates of up to 3% [7]. In addition to data exchange, social networks provide full support for making new friends. As a result, a brand-new resource is added to our knowledge [8].

3. ATTACKING STRATEGIES

Before launching an attack, attackers prepare their flow and identify a target during the information-gathering phase, also known as footprinting. The first phase includes more than just gathering information about the target; instead, it gathers additional (physical) attributes needed for the subsequent phases of the attack, such as recreating official document letterheads or learning target-related jargon and lingo. Different methods can be utilized by an aggressor to accumulate data about their objective. After this information has been gathered, it can be used to establish a relationship with the target or an important person, which can help ensure a successful attack (Figure 1). These might include disclosing information that, from a security standpoint, appears to be harmless but could be useful to the attacker [9]. Public sources like web pages, social media posts, phone books, and job portals, among others, can be used to gather information, as can previous social engineering attacks. The information from this step is used to build a relationship with the people who are being targeted [10].

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 01, January 2023, pp : 18-20

e-ISSN : 2583-1062

Impact Factor : 2.265

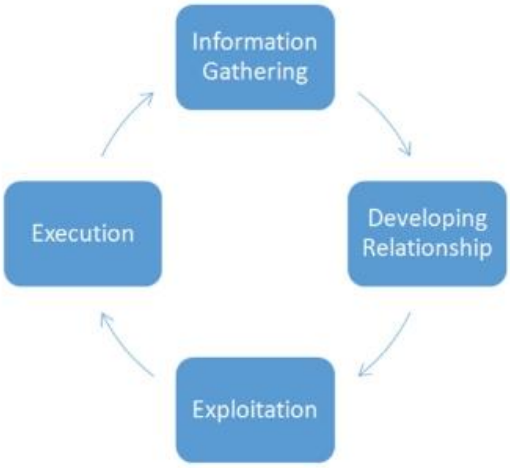

Figure 1: Attack Cycle of Social Engineering [9]

3.1 Attacks Classification

There are two main types of social engineering attacks: based on humans or computers, as shown in (Figure 2). In human-based attacks, the attacker interacts with the target in person to gather desired information. As a result, they can only influence a few victims. The targets of software-based attacks are obtained from them with the help of devices like computers or mobile phones. In a matter of seconds, they can attack many victims. One of the computer-based attacks used for spear phishing emails is the social engineering toolkit (SET) [11].

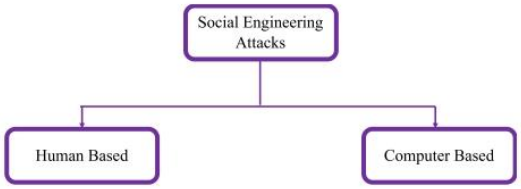

Figure 2: Attack Cycle of Social Engineering [11]

4. PHISHING ATTACK

The user is frequently referred to as the "weakest link" in information security since even the most robust technical safeguards can be circumvented if an attacker successfully manipulates the user into divulging a password, opening a malicious email attachment, or visiting a compromised website [12]. Phishing is an attack of the network kind in which a person pretends to be on a real webpage to get personal information from an online user. Phishing is using social engineering and technical means to get a user to give out personal information [13].

5. CONCLUSION

Information security is seriously threatened by social engineering attacks. They are used to get system access or information from employees who don't know about it. We gave an overview of the methods used in social engineering attacks in this paper. Unfortunately, technology alone cannot stop these attacks, and even a robust security system can be easily broken by a social engineer with no security expertise. People and businesses are suffering emotional and financial harm as a result of increasing numbers and intensity of social engineering attacks. As a result, programs to educate employees and novel detection and countermeasure strategies are in great demand. To produce trained and skilled individuals, nations must also make investments in cyber security education.

6. REFERENCES

[1] F. Mouton, L. Leenen, and H. S. Venter, “Social Engineering Attack Detection Model: SEADMv2,” Proc. - 2015 Int. Conf. Cyberworlds, CW 2015, pp. 216–223, 2016, doi: 10.1109/CW.2015.52.

[2] N. Y. Conteh and P. J. Schmick, “Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks,” Int. J. Adv. Comput. Res., vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/ijacr.2016.623006.

[3] M. Nohlberg, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks, no. 09. 2008. [Online]. Available: http://www.mendeley.com/research/securing-information-assets-understanding-measuring-protecting-against-social-engineering-attacks/

[4] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," Comput. Secur., vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.

[5] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," J. Inf. Secur. Appl., vol. 22, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.

[6] A. Yasin, R. Fatima, L. Liu, J. Wang, R. Ali, and Z. Wei, "Understanding and deciphering of social engineering attack scenarios," Secur. Priv., vol. 4, no. 4, pp. 1–17, 2021, doi: 10.1002/spy2.161.

[7] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6739 LNCS, no. March 2010, pp. 55–74, 2011, doi: 10.1007/978-3-642-22424-9_4.

[8] Y. S. Saini, L. Sharma, P. Chawla, and S. Parashar, "Social Engineering Attacks," Lect. Notes Networks Syst., vol. 491, no. 6, pp. 497–509, 2023, doi: 10.1007/978-981-19-4193-1_49.

[9] A. U. Zulkurnain, A. Kamal, B. Kamarun, A. Bin Husain, and H. Chizari, "Social Engineering Attack Mitigation," Int. J. Math. Comput. Sci., vol. 1, no. 4, pp. 188–198, 2015, [Online]. Available: http://www.aiscience.org/journal/ijmcs

[10] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 145–149, 2016, doi: 10.1109/FiCloud.2016.28.

[11] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Futur. Internet, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.

[12] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," ACM Comput. Surv., vol. 48, no. 3, 2015, doi: 10.1145/2835375.

[13] P. N. Astya, Galgotias University. School of Computing Science and Engineering, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section. SP/C Joint Chapter, and Institute of Electrical and Electronics Engineers, "Proceeding, International Conference on Computing, Communication and Automation (ICCCA 2016) : 29-30 April, 2016," pp. 1–4, 2016.