International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 189-191 www.ijaem.net ISSN: 2395-5252

Social Engineering Attacks and their mitigation solutions

Deepak Singh Malik
University Institute of Computing (UIC), Chandigarh University

Submitted: 01-11-2022 Accepted: 12-11-2022

ABSTRACT — We can see the exponential growth of internet usage in today's world. Each one of us has our day-to-day activities stored in electronic devices (smartphones, mobiles, or other electronic gadgets) whether it's a personal conversation or financial information everything is there on these devices. That's why hackers have always their eyes on our devices. One of the human approaches to hack our data is usually termed "Social Engineering".
This paper provides you the information on "How Social Engineering has emerged as a serious threat in today's world". You would find the different techniques of Social Engineering attacks and the means to counter these attacks. Also, this document highlights the role of advanced technologies like Artificial Intelligence (AI), Machine Learning (ML) in preventing these attacks.
Keywords – Social Engineering, Phishing, Hacking, Artificial Intelligence, Machine Learning

I. INTRODUCTION

Social Engineering is one of the simple methods for hackers as it depends on the attackers how they manipulate the individual or exploit the individual weakness to get access to their personal information. This method aims to access their private information and try to harm the individual or organization by making them download malicious files and software, or by clicking malicious links that provide the attacker to capture the individual data. It is a collection of all the methods used to manipulate the individual into performing actions or revealing confidential information.

II. SOCIAL ENGINEERING ATTACKS

Social Engineering attack is one of the most difficult ones to be dealt with. This is one of the foremost serious and exponential growing attacks in cyber security. Attackers collect personal and sensitive data through social engineering, then use this information to exploit the individual like blackmailing or marketing it on the black market. Social Engineering Attackers usually follow four basic steps. The very first step is collecting information about the victim and then the second is the development of the relationship with the aim. The third is to use the information which the attacker collects in the first two steps to exploit and start carrying out the attack. Last Fourth step is the attacker's exit without the traces. These are basically the four major stages of the social engineering attackers.

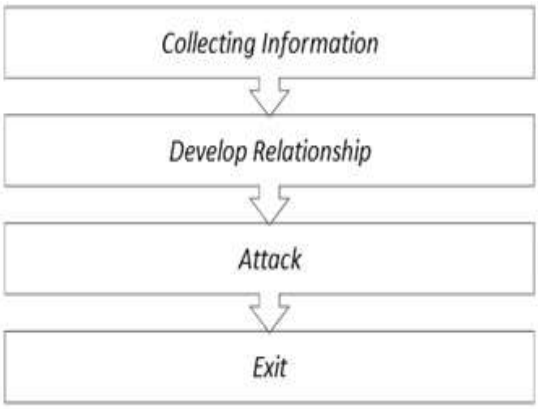

Fig.1 Four Stages of Social Engineering Attacks

III. SOCIAL ENGINEERING ATTACKS CLASSIFICATIONS

Based on how attacker executes the attack, we are classifying Social Engineering Attacks in two types:

A. Human Based:
In this attacker executes the attack in person by directly interacting with the person to collect his/her desired information. This way attacker influence very limited number of individuals.

B. Computer Based:
In this attacker executes the attack using the electronic devices to collect the target desired information. This way attacker may impact many victims at a time.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 11 Nov. 2022, pp: 189-191 www.ijaem.net ISSN: 2395-5252

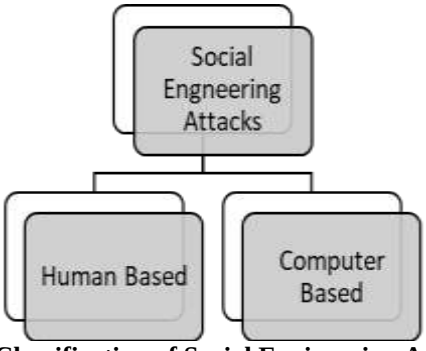

Fig.2 Classification of Social Engineering Attacks based on how attacker executes the attack

All Based on how attacker conducts the attack, we are classifying Social Engineering Attacks in three types:

A. Technical Based

Technical Based attacks are conducted through internet via social networks and online services websites, and they gather desired information such as passwords, credit card details and security questions.

B. Social Based

Social-based attacks are performed through relationships with the victims to play on their psychology and emotion. These attacks are the most dangerous and successful attacks as they involve human interactions. Examples of these attacks are baiting and spear phishing.

C. Physical Based

Physical-based attacks refers to physical actions performed by attacker to collect information about the target. An example of such attack is searching dumpster for valuable documents.

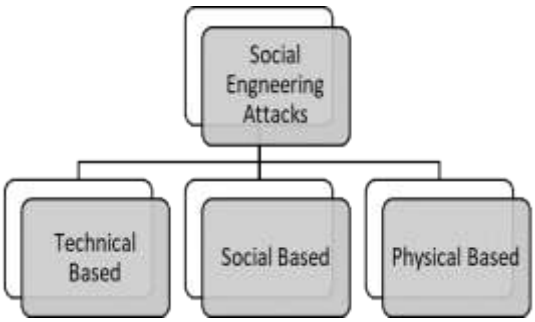

Fig.3 Classification of Social Engineering Attacks based on how attacker conducts the attack

Let's have a look at few types of Social Engineering Attacks:

1. Phshing Attacks:

One of the most popular and frequently utilised social engineering techniques is phishing. While attempting to fall into a fishing net in order to get personal data, phishing occurs when a phisher sends an email or telephone call, or when they create a malicious website, fake prize announcements, fake offers, fake online shopping sites, and other types of trickery and chicanery. To nab a victim, the attacker might send a phony message, claiming he won an award with them and must claim it. You can then give away your bank card and secret numbers, in addition to secret numbers, to receive the award, or you can include any sensitive or confidential information that benefits the attackers and is accessible online.

2. Robocalls Attacks:

A robocall is a call from a computer to a targeted individual that rings their cell phone, residential, and work phones. It is often a computer program that automatically dials a list of phone numbers to deliver pre-recorded messages. A robocall is a VoIP technology that is used to enable voice response, voice over internet protocol (VoIP), and text-to-speech features. It is used to deliver information or sell products. For example, helping people to solve tax issues has become more intense in recent years. When someone answers the phone, the number is stored in the attacker's database. Even if they are blocked, the attackers' systems keep calling other numbers. The only way to stop these calls is to ignore unknown telephone numbers, which has become a serious problem in the USA and other countries.

3. Email/Phone Scams Attacks:

- Bluejacking:

Constant Bluetooth connectivity allows hackers to bluejack you (sending spam text messages), bluesnarf you (accessing your email and other personal information on your phone), and even bluebug you (taking full control of your phone).

- Juice Jacking:

Those USB charging ports at airports or other public places can be tempting if your phone battery is running low. However, be cautious. Malware on the ports may expose your information to criminals. Only use charging cables from reputable sources in order to avoid this.

- Public Wi-Fi:

Your phone's rules are the same as for your laptop, Siciliano says; your personal information may be at risk when connected to Wi-Fi in a coffee shop or other public venue.

4. Malware and Ransomware Attacks:

An attacker can use viruses, worms, Trojans, and other types of malicious software in this attack. It

rides in a risky link or a risky software installation to target software components and propagate to other systems. The victim must then complete any amount of money or work demanded by the attacker in order to return the computer or device to a stable condition. This is an example of Malware.

5. Pretexting Attacks:

Pretexting is a technique of creating a situation to persuade victims to reveal information they should not persuade victims. It is frequently used to obtain client information from businesses, such as banks, credit card firms, utility providers, and transportation companies. Individuals impersonate clients to acquire data from businesses, typically over the phone. Pretexting takes advantage of a flaw in voice transaction recognition technology. Businesses must rely on other methods to identify their customers, since it is impossible to physically identify them. Businesses usually ask for personal information, including addresses, dates of birth, mothers' maiden names, and account numbers in order to verify their identities. Pretexters can get all this information from social networks or trash diving. Pretexting is a critical component of almost any successful social engineering attack, but its definition is confusing, resulting in more uncertainty.

IV. CONCLUSIONS

This paper highlighted the significant aspects of social engineering attacks and provided suggestions for avoiding them. It also emphasized the significance of recognizing social engineering attacks. Despite the fact that humans are one of the weakest links in cyber security, several social engineering approaches were discussed to prevent themselves from being suckered. Zero trust architecture and its implementation were also discussed. Various architectures and implementations of ML or AI in cyber security were also discussed.

REFERENCES

[1] Social Engineering Attacks: A Survey Fatima Salahdine and Naima Kaabouch School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, ND 58202, USA.
[2] A STUDY ON SOCIAL ENGINEERING ATTACKS: PHISHING ATTACK (Article in International Journal of Recent advances in Physics · January 2021)
[3] https://learn.saylor.org/mod/book/view.php?id=29612&chapterid=51674
[4] A Review of Social Engineering Attacks and their Mitigation Solutions (International Journal of Engineering Research & Technology (IJERT))
[5] https://www.imperva.com/learn/application-security/social-engineering-attack/
[6] https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html
[7] https://www.itgovernance.co.uk/social-engineering-attacks
[8] https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
[9] Wikipedia - https://en.wikipedia.org/wiki/Social_engineering_(security)
[10] https://www.webroot.com/in/en/resources/tips-articles/what-is-social-engineering
[11] https://www.trendmicro.com/en_in/what-is/phishing/types-of-phishing.html
[12] https://www.ncsc.gov.uk/guidance/phishing