ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 1, pp: (68-70), Month: January - March 2023, Available at: www.researchpublish.com

Social Engineering Attacks

Fahad Jasim Alanezi

Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7656021

Published Date: 20-February-2023

Abstract: **Growth of technologies, interconnected systems and digitalization, securing data becomes a vital concern to governments and organizations. The value of data enforces these governments and organization to implement huge number of security controls to safeguard their data. In fact, no matter of security controls implemented, there is another important factor might cause attacks, data leakage or service interruption which is "Human". Human is the main part of Social Engineering which is the art of manipulating people to obtain sensitive information. This type of attack is increasing across the world and impacting many organizations. This research paper is going to define certain aspects of social engineering, types of specific social engineering techniques and required security controls to prevent such social engineering attacks.**

Keywords: **Social Engineering, Attacks, Criminals, Phishing, Baiting, Tailgating, Should Surfing, Dumpster Diving.**

I. INTRODUCTION

Social Engineering is the art of manipulating people to obtain sensitive information. Depending on what attackers wants, they target human to steal sensitive information such as account's password and financial information including credit card numbers and security code. People are the main goal of cybercriminal to launch this type of attack since they exist in every single organization, and they have access to huge amount of data. Hence, attackers do not require to have advanced technical skills to phish people in order to respond to any social engineering techniques and disclose sensitive information. Organization should increase ethe level of awareness of their employees to realize the danger of cybersecurity attacks specifically social engineering since they are connected to the worldwide entities. Also, organization have to implement proper security controls to prevent such type of attacks, and harden their systems, hardware and data to prevent data breaches or data lose.

II. TYPES OF SOCIAL ENGINEERING

A. Phishing

Phishing is the most effective technique utilized by hackers to gather information about the target. Phishing attack is an attempt to steal sensitive information to exploit this information to carry out further attacks. The phishing attack occurs when a hacker sends a fraud email to a person which looks a legitimate email. The email message is designed to be real with well-known source in order to gain the victim's trust to click on the suspicious link or download the attachment.

B. Smishing

Smishing is a combination of SMS and Phishing. This type of attack occurs when a hacker sends a text message to the victim's mobile phone attempting to steal personal information.

C. Vishing

Vishing is a combination of Voice and Phishing. In this type of attack, a criminal uses the phone to call the victim aiming to trick the victim and get sensitive information or gain access.

D. Pre-texting

Pre-texting is a technique which manipulates victims into divulging sensitive information. This attack occurs when the perpetrator makes a phone call impersonating someone in authority and present a false scenario to gain victim's trust, then, request sensitive information. For example, an IT Help Desk analyst calls a user requesting his/her credential to install updates or perform a fix in a computer system.

E. Baiting

Baiting attack happens when the attacker leaves a malware-infected USB flash drive in a location where it's sure to be found. This USB contains a legitimate looking and curiosity-piquing label. When the victim plugs the USB to the device, the attacker will take control and obtain his/her wants.

F. Tailgating

Tailgating depends on physical attack where an intruder follows an employee to gain unauthorized access to a restricted area within the organization. Once the intruder gets inside this restricted area, he/she can maliciously access sensitive information. This attack could lead to data leakage or data damage.

G. Shoulder Surfing

Shoulder Surfing attack occurs when the perpetrator looks over victim's shoulder to see sensitive information displayed on a device screen such as user credential. Another common way is using the smartphone camera to record user keystrokes.

G. Dumpster Diving

Dumpster Diving is a technique used to search in an organizations or user trash in hopes of finding useful information. The trash might contain papers, notes, CDs, DVDs or even company directories.

III. HOW TO PREVENT SOCIAL ENGINEERING ATTACKS

Social Engineering attacks can be prevented by implementing various security controls. Putting the following controls in place will help prevent this attack:

1. Strong Passwords:

Use strong password for your account and different strong password for different accounts as well. Never share the password. Ensure to meet the password policy in your organization.

2. Multi Factor Authentication:

Do not rely on one factor to authenticate to your account. It's true that password is security but it's still can be guessed or obtained. Enabling multi factor authentication will add extra strong step to secure your account.

3. Never Open Suspicious Email:

Never click on any link or download any attachment when you receive suspicious email which comes to your mail inbox or junk. Be extra caution and watch the following to identify suspicious email:

- Pay close attention to deceptive domains
- Exciting subject line
- Offers too good to be true
- Grammatical errors
- Sens of urgency
- Suspicious link
- Claim of authority

4. Enable SPAM Filter

Enabling SPAM filter offer protection over your mail inbox from social engineering attacks.

5. Never plug-in external flash drive

Never plug-in unknown flash drive to your devices. Infected flash drives allow the attacker to take control of your systems upon plug it in.

6. Never Respond to suspicious SMS or Phone Call

Never respond to suspicious SMS and phone call that ask you to provide sensitive information related to your account even if he/she introduces himself/herself and provide some true information about you. This information might be obtained illegally.

7. Establish Awareness Program

Establish awareness program for Social Engineering in your organization. This is important for the organization employees since they are the target of this type of attack. The awareness program enables the employees to understand what is the social engineering, its attack techniques and how to prevent them.

IV. CONCLUSION

This paper aimed to review the social engineering, its attack techniques, and what can be implemented by either organizations or individual in order to prevent social engineering attacks. The cybercrimes intend to steal sensitive information, disrupt services and destroy business; thus, organizations are required to place extra efforts to safeguard their data and business. Implementing security controls are not enough to be safe, it is mandatory to raise the awareness level of employees to sustain protection against cyber-attacks. The fact is, social engineering can be exploited by non-technical attackers, organizations should establish proper awareness program to ensure their employees become the first line of defence against this type of attack.

REFERENCES

[1] WILEY. Social Engineering, The Science of Human Hacking, 2nd Edition 2018.

[2] Kaspersky. What is Social Engineering (https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering).

[3] Webroot. What is Social Engineering (https://www.webroot.com/ie/en/resources/tips-articles/what-is-social-engineering)

[4] Behrouz A. Forouzan. “Data Communication & Networking”, 5th Edition, McGrow-Hill

[5] Microsoft. “Microsoft Cybersecurity Défense Operations Center”. (https://www.microsoft.com). an international guideline-based

[6] Application Security (https://www.imperva.com)

[7] McAfee. Internet Security(https://www.mcafee.com)

[8] Joe Gray, Practical Social Engineering: A Primer for the Ethical Hacker,(June 14, 2022)

[9] IBM: Social Engineering (https://www.ibm.com/topics/social-engineering)

[10] Raef Meeuwisse, How to hack a Human: Cybersecurity for the Mind (January7, 2019)

[11] Wiley, The Art of Human Hacking (https://www.wiley.com)

[12] David Hutter, "Physical Security and Why It Is Important", 2016, SANS Institute.

[13] "2020 Cyberthreat Defense Report". CyberEdge Group, https://cyber-edge.com/resources/2020-cyberthreat-defense-report-portfolio/