WHEN HUMANS ARE 'HACKED': SOCIAL ENGINEERING ATTACKS AND MITIGATION

Joy Ezeife

ezeifejoy@gmail.com, Federal Polytechnic, Oko, +2348061126745

Abstract

Organizations are often very highly interested in stopping malware from entering their digital environments. However, the threat of social engineering is often neglected. Social engineering is the malicious practice where attackers manipulate and 'smartly' trick individuals into providing sensitive data or access credentials. Many people overlook the avenues through which these miscreants work in the psychology of people hence they fall victims to them. The threat of social engineering and the risks and damages it causes continues to increase. Many companies have lost a lot through the manipulations of social engineering on their staff and clients. The society at large is not left out no matter a person's level of literacy. These attackers digitally impersonate as corporate executives and are involved in all forms of 'hacking' of the human mind through their subtle convincing tools such as phishing, smishing and the likes. Hope is not lost however, since there are several ways organization s can mitigate the risk posed by social engineering.

Keywords: Social engineering, Password, cyber-attack, Protection, Two-factor authentication

Introduction

The fact that organizations place a tremendous focus on stopping malware from entering their environments is okay. However, the threat of social engineering is often overlooked. Social engineering is the practice where attackers manipulate and trick individuals into providing sensitive data or their access credentials. It is a challenging thing to defend social engineering. This is due to the fact that a lot of people put so much trust in others and have so much tasks to carry out, hence they tend to overlook the concerns of social engineering risks. Hence, the act of manipulating and influencing people to expose sensitive information is known as social engineering or social attacks Mouton *et al.*, (2014).

IBM (2023) notes that social engineering is increasing as a serious threat, while the imposed risks continue to grow. Globally, the average cost of a data breach reached $4.45 million in 2023 quite highest for the report and a 15% increase over the last 3 years. The detection and escalation costs moved up to 42% over this period also, representing the highest amount of breach costs, and depicting a move towards breach investigations that are more complex.

Also, businesses are divided into how they plan to manage the increasing cost and frequent occurrences of data breaches. The study found that while 95% of reviewed organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%), (IBM, 2023).

Tetri and Vuorinen (2013) observed that data gathering, fabrication and persuasion are used to exploit their victims. These attackers attempt to impersonate corporate executives, thus increasing the amount of spam that are brought to our inbox. However, the organization can put several tactics in place to help mitigate the risk posed by social engineering.

Kamal *et al.*, (2023) note that social engineering is the art of using manipulation, motivation, and convincing tricks which are applied to the users, and they share their confidential information with the attacker. The attacker generally sends bait in the form of an email message, and the victim accepts it as authentic information and takes necessary actions based on the guidelines of the email or message. Social engineering has a high success rate as compared to other cyber-crime as it exploits the weakest link of the information security system: “the human” (Kaushalya *et al.*, 2018; Chitrey *et al.*, 2012 & Krombholz *et al.*, 2015).

Sadiku *et al.*, (2016) opines that social engineering consists of techniques used to manipulate people into performing actions or divulging confidential information. It is the acquisition of sensitive information by an outsider. To achieve that, a social engineer tricks someone into providing access to information or breaking normal security procedures. The process of doing that is known as social engineering attack. Social engineering can be used in face-to-face interactions, over the telephones, letters, emails, websites or through persons. It threatens not only companies, organizations, and governments, but also individuals.

Types of Social Engineering

There are many kinds of social engineering attacks. According to (Rouse, 2016; Bisson, 2016; & Applegate, 2009), some of them are:

Phishing

Phishing seems to be the most common type of social engineering attack. It is associated with fake emails and websites. Phishing usually occurs when a malicious party sends a fraudulent email. The email is meant to trick the recipient into sharing personal information such as credit cards, passwords, or social security numbers. It can also be in the form of convincing a victim to click a hyperlink or download an attachment. Sometimes people will expose and share sensitive or private information to those they wish such as their superiors, clients or others. Phishing has been around for a long time, but it has become more numerous and sophisticated. Phishing emails use fear and urgency to their advantage, causing people to fall victims.

Scareware

This is a malicious computer program that is meant to convince the victim that their system is infected, pressuring the victim to buy and download fake antivirus software. The protection software regularly displays warnings for infections and demands payment for removing them.

Tailgating

This attack is also known as "piggybacking." This type of attack involves someone who lacks the proper authentication following an employee into a restricted area. This attacker tailgates the employee who has legitimate access to the area.

Pretexting

Pretexting occurs when one party lies to another in order to gain access to privileged information. The social engineer or fraudster creates a setting designed to influence the victim to release sensitive information. Pretexting attacks rely on building a false sense of trust with the victim. For example, the attacker may pretend they need some personal information in order to confirm the identity of the target. Most times, they claim that they are agents or staff of a financial institution whereas they are not.

Smishing

This is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals.

Baiting

Baiting involves the hacker promising an item or good to entice victims. It is similar to phishing attacks. For example, baiters may offer users free music if they surrender their personal information to a certain site.

Dumpster Diving

Dumpster diving is salvaging from large commercial, residential, industrial and construction containers for unused items discarded by their owners but deemed useful to the picker.

Shoulder Surfing

This is a type of social engineering technique used to obtain information such as personal identification numbers, passwords and other confidential data by looking over the victim's shoulder.

Classifications of Social Engineering Attacks

Mouton, *et al*., 2014 stated that social engineering attacks can be classified according to the manner in which the communication takes place during the exploit, and the interaction between attacker and target. Also, understanding the various types of attacks will help one to produce attack scenarios that represent possible real life attacks, showing a wide coverage of the diverse ways through which attackers operate.

There are various ways of classifying social engineering attacks. These are based on the unique perspective through which one looks at them, such as the following:

a. Main category: direct and indirect, based on the analysis of the other categories of these attacks. Direct attacks use direct contacts existing between the attacker and the victim to carry out the attack. These attacks are performed through physical contact, eye contact or voice interaction. Sometimes, the attacker’s presence on the working place is needed to carry out the attack. Mouton, *et al*., (2014) observed that they can be in form of physical access, shoulder surfing, dumpster diving, phone social engineering, pretexting, impersonation on help desk calls, and stealing important documents.

b. Human or software according to which entity is involved in the process of the attack.

c. Social, technical, and physical-based attacks, according to how the attack is carried out. Salahdine and Kaabouch (2019) notes that in direct attacks, social engineers interact in-person with the target at either the information gathering phase to gather the desired information or at the exploitation phase where the target is manipulated. Also, direct attacks are considered the most successful and dangerous attacks.

Ivaturi and Janczewski (2011) observed that direct attacks can also be either one-sided or two-sided, which are seen as unidirectional or bidirectional communication. In bidirectional communication, both parties communicate hence they use means such as email and direct face-to-face communication. Unidirectional communication is such that the target and attacker does not have an interactive communication. Also, one-way texting and emails can also be used.

According to Sekhar (2021), indirect attacks are such that instead of interacting directly with the target victims, attackers make use of devices such as computer or to collect the required information and carry out the attack. With the aid of these automated devices, these social engineers can attack by sending thousands of emails to many target victims within a short time. They can also use the computer and its associated devices to make several automated calls to target victims.

Mitigating Social Engineering Attacks

Sadiku et al (2016) notes that the strongest security technology can be overcome by a smart social engineer hence there is need to be steps ahead of these cybercriminals.

Newell (2023) notes that in mitigating social engineering attacks, protecting user devices against malware is one of the first endpoint hardening tasks an IT administrator or Information Security team will likely implement. As they attempt to secure various devices, their operating systems notwithstanding, preventing users from installing malicious software such as ransomware and spyware is paramount. There are also some basic steps to take in preventing the effects of social engineering attacks (Irwin, 2021; Newel, 2023). They are:

1. Strong passwords and two-factor authentication

Strong, unique passwords are the first line of defense when strengthening your organization's security posture. Sufficiently long and complex passwords mitigate the risk of shoulder surfing by making them tricky for someone to glance at a user's keyboard or touch screen and remember what they typed. However, a complex and/or long password is not enough to prevent social engineering.

A malicious actor can execute a successful phishing attack, for example, when the user has provided the password outright, regardless of its complexity. Two-factor authentication (2FA) or multi-factor authentication (MFA) should be implemented; otherwise bad actors have access to everything if they obtain a user's master password.

In two-factor or multi-factor authentication, not only does a user need their password, they also need either a randomly generated six-digit code or another form of authorization, biometric technology such as Face ID or Touch ID, or something physical to access the requested application. 2FA and MFA help reduce the risk that attackers can access systems especially when biometrics are used since they may not be able to confirm the authentication prompt.

2. Using firewalls, antivirus, anti-malware and spam filters to reduce the cases of malicious traffic.

3. User training

Never underestimate the power of user training. Social engineering attacks often follow a consistent pattern. Spelling errors, strange icon placement, email spoofing (where email messages are sent with a fake sender address) and a sense of urgency are all strong indicators that an email or phone call is a social engineering attack. Staff training will help them to:

a. Understand the consequences of social engineering attacks;
b. Become suspicious of unsolicited communications and unknown people;
c. Check whether emails genuinely come from their stated recipient: double-check sender's names and look out for spelling errors in the addresses.
d. Avoid opening suspicious email attachments;
e. Beware of tailgating or being led to obtain sensitive information from their superiors or others.
f. Avoid being rushed. Attackers create a sense of urgency to pressure their victims;

g. Think before providing sensitive information. No legitimate person will ever ask for passwords or such.

h. Check websites' security before submitting information, even if they seem legitimate and avoid websites that use ordinary Hypertext Transfer Protocol (HTTP) rather than Hypertext Transfer Protocol Secure (HTTPS);

i. Pay attention to Uniform Resource Locators (URLs), and 'typo squatting'. Such sites look genuine but their web addresses are subtly different from the legitimate site they're imitating;

j. Beware of clickjacking and become suspicious of everything being clicked on, letting the mouse hover over links to check where they are pointing to.

4. Test the effectiveness of the training

After training the staff, it is very important to test how effective the training measures are. Phishing attacks and the likes can be simulated to know an extent of the employees' susceptibility to phishing emails and others.

5. Principle of least privilege

The "principle of least privilege" is an Information Security concept where users should only be granted access to the specific applications and functionalities required to do their job. For organizations that use applications with user access levels, consider implementing and reviewing them regularly. In a situation where a user's credentials are compromised, the attacker's access can be limited to the user's specific access level. This ensures that the attack has a restricted scope of access and, ideally, is limited from accessing critical or sensitive data. After gaining initial access, attackers will attempt to move laterally through the network until they reach their final target. The "principle of least privilege" helps limit and mitigate the spread of social engineering attacks but is not a complete solution. Training users on being vigilant and cautious when receiving an odd request from a team member is a great additional step.

6. Zero trust network access

Connects users to company resources only after they have strictly verified their identity, continuously checks that the user and the device meet identity and security requirements, and totally prevents access to resources the user is not allowed to access (as the user can't even reach the part of the network those resources exist on). If the identity of a user or the security status of a device comes into question, network access can be restricted to all or some of the network. This prevents and/or reduces the spread of a bad actor in the corporate network, regardless of whether the device is compromised.

7. Build a positive security culture

It is necessary to dispel an unhelpful myth related to social engineering. Social engineering attacks exploit misplaced trust, not one's stupidity. That someone was able to exploit an individual or staff is as a result of the strong manipulative ability of the cybercriminal and it doesn't mean that the staff is not smart. Hence, this should be openly known as the culture in any organization. Everyone is a potential victim. The staff should know their organization's expectations of them towards security and report potential social engineering attacks instead of thinking that opening up will get them into trouble with their superiors. When the security culture is wholesome, responding to incidents will be timely.

8. Understand the psychological triggers

This aspect of vulnerability is common among humans. We tend to get suddenly excited whenever there is news of something big coming. Social engineers are cunning specialists in this kind of manipulation and 'hacking' of the human psychology. There is no need believing that a lottery has been won when none was applied for. Also, even though some people are philanthropists, it doesn't mean that one should submit his banking credentials wherever such 'philanthropists' are making online promises since most are fake.

Conclusion

Social engineering attacks are increasing as advancements in technology continue to increase. It is not easy to recognize all forms of such attacks since the attackers employ all kinds of manipulative techniques which trigger people's psychology into yielding to their tricks, hence being involved in what they would not ordinarily do. The malicious actors may create trust in their victims, gather all forms of intelligence, create cases of fake urgency, make great promises, convince them of being indebted and create emotions of fear to confuse and exploit their victims. It is therefore necessary for organizations and individuals to understand the various methods they use and become highly proactive towards social engineering. As Nigeria continues to battle inflation, it is very necessary to employ all relevant tools and involve stakeholders so as to reduce the menace of social engineering.

Recommendations

The following are the recommendations:

1. Organization should have a password policy and password training for the staff.

2. They should enforce the use of two-factor authentication by their staff and clients.

3. Individuals, customers, staff or clients should verify from their superiors before clicking any suspicious link, attending to any message or call for the provision of details.

4. Awareness should be increased on the prevalence of scareware and phishing activities.

5. People should learn not to be quick to attend to any online demand no matter what it is rather they should be quick to report.

6. Organizations should consider incentive or reward programs for users reporting spam and phishing attempts.

7. IT related firms should work to create a culture of support, education and prevention around social engineering.

8. Organizations should have continuous awareness programs on security.

9. There should be effective planning and implementation of security control measures.

References

Applegate, S. D. (2009) "Social engineering: hacking the wetware!" *Information Security Journal: a Global Perspective*, 18: 40-46.

Bisson, D. (2015) "5 Social Engineering Attacks to Watch Out For," Accessed on 12th May from http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watchout-for/

Chitrey, A., Singh, D., Bag, M. and Singh, V. (2012), A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *International Journal of Information & Network Security*, 1, 45-53

IBM (2023) Cost of a Data Breach Report 2023 Retrieved on 13th May 2024 from https://www.ibm.com/reports/data-breach

Ivaturi, K. and Janczewski, L. (2011) 'A Taxonomy for Social Engineering attacks', in Grant, G. (ed.) *International Conference on Information Resources Management*, 1–12.

Kamal, U. S., Farizah, Y. & Aziz, D. (2023) Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods *Sustainability 2023*, 15(*13*), 10471; https://doi.org/10.3390/su151310471

Kaushalya, S. Randeniya, R. and Liyanage, A. 2018), An Overview of Social Engineering in the Context of Information Security. *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, Bangkok, 22-23, 1-6.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced Social Engineering Attacks. *Journal of Information Security and applications*, 22, 113-122.

Mouton, F., Pepper, M. J. & T. Meyer, T. (2014) "A Social Engineering Prevention Training Tool: Methodology and Design for Validating the SEADM," *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018) 2014*, 1-9.

Newell , B. (2023) Mitigating Social Engineering Attacks. Retrieved on 13th May 2024 from https://www.jamf.com/blog/mitigating-social-engineering-attacks/

Rouse, M. (2016) "Social engineering," Accessed on 12th May 2024 from http://searchsecurity.techtarget.com/definition/social-engineering

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

Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. *Future Internet*, 11(*4*): 89. https://doi.org/10.3390/fi11040089

Saylor Academy (2024) An Overview of Social Engineering https://learn.saylor.org/mod/book/view.php?id=29612&chapterid=5157

Sekhar Bhusal, C. (2021) Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, 12 (*1*), 104-114. doi: 10.4236/jis.2021.121005.

Tetri. P. and Vuorinen, J. (2013) "Dissecting social engineering," *Behavior and Information Technology*, 32(*10*):1014-1023.