IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ჯ Peer-reviewed & Refereed journal ჯ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131139

SOCIAL ENGINEERING: RISK AND COUNTER MEASURES

Yashaswini Nag M N[1], Suraj Kumar[2], Harsh Ranjan[3], Ayush Kapoor[4]

Assistant Professor, Dept. of CSE (Cyber Security), RNSIT, Bengaluru, India[1]

Student, Dept. Of CSE (Cyber Security), RNSIT, Bengaluru, India[2]

Student, Dept. Of CSE (Cyber Security), RNSIT, Bengaluru, India[3]

Student, Dept. Of CSE (Cyber Security), RNSIT, Bengaluru, India[4]

Abstract: Social engineering, a major cybersecurity threat, exploits human psychology to bypass technical defenses. This paper examines techniques like phishing, pretexting, baiting, tailgating, quid pro quo, and vishing, which manipulate victims to reveal confidential information or breach security protocols. The associated risks include financial loss, identity theft, reputational damage, operational disruption, and legal consequences. Countermeasures such as education and awareness programs, multifactor authentication, strict access controls, and advanced technologies like AI and machine learning are essential to mitigate these threats. Understanding human behavior and training people can greatly reduce the risk of social engineering attacks, strengthening overall cybersecurity defenses.

Keywords: Social engineering, social attacks, social technology, phishing, information security social engineer, cyber attacks, computer network, malware, Information security.

I. INTRODUCTION

Using social engineering, hackers are suitable to manipulate individualities to force them to inevitably apportion their non-public details or allow access to systems. Employing technology and hacking are not the same, as social engineering works on the abecedarian vulnerability of security which is the mortal aspect. Man is vulnerable to a variety of feelings similar as trust, fear, urgency and curiosity. Phishing, baiting and pretexting all of these correspond of use of ruse where fake emails or stories are used to wisecrack individualities with the intention to trick them into allowing people to install malware or indeed gain access to information in defended areas. An illustration of this ruse in action could be setting oneself as a technician fixing an issue when in reality they wanna a login credential, this allows them to insure that the association can suffer significantly and the person can have their identity and essential details compromised. bushwhackers operating at a high- position demonstrate that indeed successful associations with cyber security are weak against social engineering, which begs the question as to how to deal with attacks in the first place. Technological defenses like firewalls and anti-phishing tools are pivotal but not sufficient on their own. Regular training and mindfulness programs are essential to equip people with the knowledge to fete and respond to social engineering attempts[1]. For illustration, tutoring workers to corroborate the identity of guests or emails before participating sensitive information can baffle numerous attacks. Organizations should also apply strict security programs like multi-factor authentication to minimize the impact of successful attacks. Eventually, social engineering highlights the significance of addressing both technological and mortal aspects of security. By understanding the psychology behind these attacks and fostering a culture of dubitation and alert, individualities and associations can make a stronger defence against the ever- evolving trouble of social engineering. Creating a security-conscious terrain and maintaining constant alert are crucial to precluding and mollifying the pitfalls associated with social engineering attacks.

II. LITERATURE REVIEW

CONCEPTS OF SOCIAL ENGINEERING

Social engineering is a tricky system where bushwhackers deceive individualities into giving away non-public information or compromising security systems by exploiting mortal vulnerabilities. Unlike traditional hacking, which relies on specialized chops, social engineering leverages cerebral manipulation, similar as erecting trust and creating a sense of urgency. Common tactics include phishing (transferring deceptive emails), pretexting (fabricating fake scripts), baiting (offering enticing deals), and tailgating (gaining unauthorized access by following someone into a secure area).

Cybercriminals favor social engineering because it’s simpler to exploit mortal crimes than to breach specialized defences. They frequently target groups like the senior, who may have difficulties with ultramodern technology, and children, who might warrant internet mindfulness. The non-public information they seek includes bank account figures, passport details, and credit card information. Understanding social engineering is essential for developing robust defences. enforcing education and mindfulness programs, multi-factor authentication, strict access controls, and comprehensive security protocols can significantly reduce the threat of these attacks. The social engineering cycle, or attack cycle, generally involves stages like surveillance (gathering information), engagement (initiating contact with the target), exploitation (executing the deception), and prosecution (achieving the bushwhacker’s thing). By feting these stages, associations and individualities can more prepare and cover themselves, creating a more secure terrain against these sophisticated threats[8]. From the figure(1) that I've created, this is the illustration of social mastermind cycle and it's known as the attack cycle. This attack cycle figure helps the bushwhacker to follow those way to avoid any confusion and try to achieve their target similar as stealing the information or damage the system. It has four stages in social mastermind cycle that includes the following, which I'll explain each

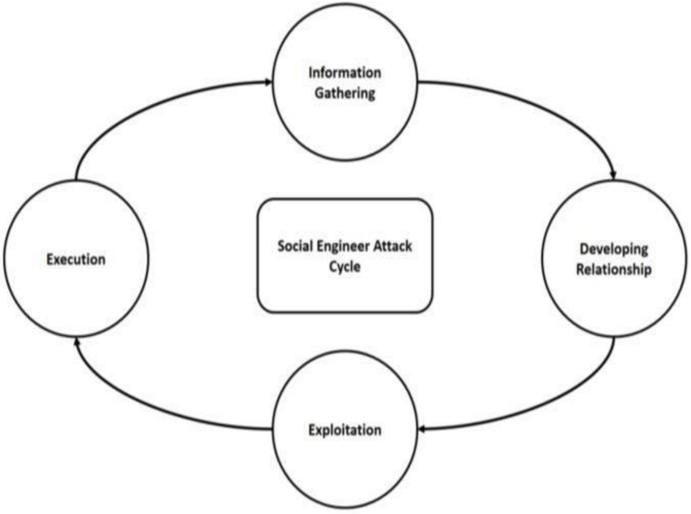

Fig. 1. Social Engineering Attack Cycle

A. Information Gathering

The first step in a social engineering attack is collecting information about the target, whether it’s a person or an organization. The attacker spends a lot of time researching their target, which can take weeks or months. They look for information on the organization’s website or on personal social media profiles like Facebook or Instagram. This stage is very important because it allows the attacker to gather enough information to plan their attack. The more information they collect, the better they can figure out how to access the target’s data. Accurate information is key; if the information is wrong, the attack might fail. This step helps the attacker feel confident and ready to approach their target.

B. Developing a Relationship

After gathering the needed information, the attacker starts building a relationship with the target. This step requires the attacker to be clever and patient to gain the target’s trust. The attacker often uses fake identities and the collected information to seem helpful and trustworthy. To build trust, the attacker engages the target in personal conversations, making the target feel comfortable and confident in the attacker. This communication can happen through emails, social media, or phone calls. The attacker spends time maintaining this relationship until trust is established.

C. Exploitation

In the exploitation stage, the attacker takes advantage of the trust they have built with the target. They use the information they gathered and the relationship they developed to get more personal details. The aim is to find the target into giving away confidential information, like login details or bank account numbers, without making the target suspicious. This technique is called pretexting. For example, the attacker might convince the target to share their bank security number over a phone call. Once the target gives away this sensitive information, their security is compromised, allowing the attacker to access their systems and data. This step is crucial for the attacker to gain unauthorized access and misuse the obtained information.

D. Execution

Once the attacker has gained access to the system, they create multitudinous problems for the target, whether an association or an existent. They might shoot phishing emails containing malware or dangerous links. At this stage, the attacker aims to steal precious information, similar as fiscal or other confidential details, using the trust they erected with the target. The theft of sensitive information can have severe consequences for the association, potentially leading to discipline under regulations like the Data Protection Act 2018 and indeed ruin. After achieving their pretensions, the attacker ends the commerce with the target and removes all traces of the attack to avoid discovery. They insure no substantiation is left before, making it delicate for investigators to identify them. If successful in hiding their identity, attacker can return in the future to repeat their tactics. provocations for social engineering attacks include fiscal gain, vengeance, entertainment, challenge, pride, and spying. By understanding these provocations and tactics, we can more defend against similar pitfalls.

III. ATTACK VECTORS

An attack vector is a path or means by which the attacker can gain access to exploit system vulnerabilities, including the human element.

A. Social Approach

The attack vectors in social approach can be arise through different acts:-

1) Tailgating: Tailgating is a social engineering fashion where an attacker follows an sanctioned person into a confined area. The attacker takes advantage of the victim's innocence or politeness, asking them to hold the door or simply slipping in before it closes. This system allows the attacker to bypass security measures that are in place to circumscribe access. With the rise of regulations forbidding smoking within company demesne, tailgating has come an indeed more effective tactic. Smokers stepping outside for breaks can inadvertently give openings for unauthorized person to tailgate in groups, making it easier for the unauthorized person to blend in and gain access to secure areas. Understanding and recognizing tailgating is vital for maintaining secure surroundings. administering strict access controls and promoting awareness among workers about the significance of not holding doors for strangers can help palliate this trouble.

2) Impersonating: Impersonating involves a threat actor assuming a false identity to gain credibility and carry out malicious actions. This technique can be used in various forms, such as piggybacking, pretexting, and quid pro quo. Piggy backing: Similar to tailgating, the attacker seeks physical entry into secured areas by gaining permission from someone with legitimate access. The attacker may impersonate business personnel who require temporary access. Pretexting: This attack includes creating a believable scenario to engage the prey. The attacker impersonates an authority figure or trustworthy entity to breach security protocols and gain access to credentials and personal information. A credible story and thorough research on the target are essential to avoid suspicion. Quid Pro Quo: In this context, the attacker offers a fake technical service that requires sensitive information to succeed. The attacker, posing as an IT support technician, aims to infect the targeted system by offering assistance to a victim experiencing technical difficulties. Impersonation is a versatile and effective method in social engineering, as it leverages trust and authority to trick down victims and gain unauthorized access.

3) Eavesdropping: Eavesdropping is a social engineering fashion where attackers hear in on private exchanges or communication channels to gather sensitive information. Within a company, workers may bandy classified matters out loud, assuming only authorized labor force are present. still, trouble actors can exploit these security breaches simply by being in the right place at the right time. attackers can also proactively block communication channels, similar as emails and telephone lines, to listen in on non-public exchanges. By harkening in on these dispatches, they can gather precious data that can be used to compromise security and gain access to sensitive data. Understanding the pitfalls of wiretapping highlights the need for secure communication practices and mindfulness of implicit vulnerabilities.

4) Shoulder surfing: Shoulder surfing involves directly observing someone to gather personal information by looking over their shoulder. This technique is frequently used to extract authentication data, such as passwords or PINs. By positioning themselves strategically, attackers can visually capture sensitive information as the target enters it on a device.

DOI: 10.17148/IJARCCE.2024.131139

This simple yet effective method emphasizes on the importance of being vigilant about who might be watching when entering confidential information.

5) Dumpster Diving: Dumpster diving is a fashion where attackers search through trash to find sensitive information. constantly, individualities and associations fail to properly dispose of documents, papers, and indeed attack, which can contain confidential data. By sifting through discarded particulars, attackers can recover precious information that can be used for vicious purposes. This underscores the significance of securely disposing of sensitive paraphernalia to help data breaches.

B. Socio-Technical Approach

Social engineer has many techniques that works over email, phone call or social media. The possible reasons why the victims give away their confidential information to the techniques of social engineer easily is due their greed, curiosity, or fear. There are so many techniques that uses in social engineer which I will include the most common used technique and explain the purpose of each technique:

1) Phishing: This fashion is one of most popular social mastermind that used in emails or textbook dispatches that's aimed to produce feeling a sense of fear, fear, rapacity, can curiosity in victims. When the bushwhacker sends the phishing dispatch or textbook communication to their target which contains vicious link that the takes the target to the malicious website similar as fake bank platform which will ask the target for bank details similar as word, account number and security number. This will affect the target as their non-public information will get lost or it sends contagions into the target's device similar as smartphone or computer to damage it and steal the information.

2) Baiting: Baiting exploits human behaviour, such as greed or curiosity, to trick victims into disclosing sensitive information. For example, an attacker might send a fake email offering a free iPad and ask the target to input their personal information, including bank details. Once the target provides this information, they may lose money due to the scam. Baiting can occur through various channels, including emails, sms, or websites. Essentially, the attacker offers something enticing that the target wants or is interested in, causing the target to take the bait. This method is effective because it leverages the target's natural desires to lure them into a trap, ultimately compromising their security.

3) Vishing: Vishing, or voice phishing, is a method that uses phone calls to deceive victims. Attackers pose as trustworthy figures, such as bank representatives, and create urgent scenarios to trick victims into revealing sensitive information like account numbers and security codes. This technique relies on direct communication to bypass digital security measures and exploit the victim's trust. Recognizing the signs of vishing is crucial for protecting personal information from these manipulative attacks.

4) Scareware*:* Scareware is a tactic that uses fear to trick targets into believing their device, like a pc or laptop, is infected with a virus. The attacker sends a fake warning message to scare the target, then pretends to offer help to fix the nonexistent problem. They instruct the target to download a file that supposedly solves the issue but actually contains harmful software (malware). Once the malware is installed, it allows the attacker to steal information or damage the system. This method works because the target, panicked by the fake threat, trusts the attacker's offer of assistance. The attacker uses this false sense of help to get access to the target's confidential information, exploiting their fear to achieve malicious goals[6].

IV. RISK ASSOCIATED WITH SOCIAL ENGINEERING

Social engineering poses several risks for both individuals and organizations:

A. Financial Loss: Victims can suffer financial losses due to fraudulent transactions or theft of sensitive financial information. This includes unauthorized access to bank accounts and credit card fraud[9].

B. Identity Theft: Personal information obtained through social engineering can be used for identity theft. This can lead to long-term consequences such as damaged credit scores and reputational harm.

C. Reputational Damage: Organizations targeted by social engineering attacks may face reputational damage. Public disclosure of a breach can erode customer trust and result in lost business opportunities.

DOI: 10.17148/IJARCCE.2024.131139

D. Operational Disruption: Social engineering attacks can disrupt business operations, leading to productivity loss and increased costs for recovery. This includes downtime due to compromised systems and resources needed to address the breach.

E. Legal and Regulatory Consequences: Failing to protect sensitive information can result in legal action and regulatory fines. Organizations must comply with data protection laws, and breaches can lead to substantial penalties.

F. Psychological Impact: Victims may witness stress, anxiety, and loss of trust. The emotional risk can affect both individualities and workers within associations.

V. COUNTER MEASURE FOR SOCIAL ENGINEERING ATTACKS

A. Do Not Click on Suspicious Links or Attachments.
   a. Avoid clicking on links or opening attachments in emails or messages from unknown senders
   b. Verify the sender's identity before engaging with any email or message content[7].

B. Do Not Share Sensitive Information
   a. Never share personal information like passwords, bank details, or phone numbers in response to unsolicited request.
   b. Always double-check URLs before clicking on them.

C. Education, Awareness, and Training
   a. Train and educate employees on recognizing and dealing with social engineering techniques.
   b. Raise awareness about common social engineering tactics and how to avoid them.
   c. Implement security protocols for handling data securely[11].

D. Use Multi-Factor Authentication (MFA)
   a. Encourage the use of MFA, including passwords and biometric verification (e.g., fingerprints), especially before making payments or performing sensitive actions.

E. Create and Follow Security Policies
   a. Develop and enforce organizational security policies to regulate data handling and ensure compliance with security protocols.

F. Secure Your Devices and Services
   a. Install firewalls and antivirus software on all devices and keep them up to data.
   b. Regularly scan systems to detect and eliminate potential infections.
   c. Ensure that all software on devices is updated to the latest versions.

G. Use Strong Passwords
   a. Create strong passwords that include a combination of letters (uppercase and lowercase), numbers, and symbols.
   b. Avoid using easily guessable passwords.

H. Install Spam Filters
   a. Use spam pollutants to block phishing emails and dispatches.

VI. CONCLUSION

This paper introduces a model to help understand social engineering attacks more. It looks at three main corridor how attacks work, mortal sins, and different attack styles Cybersecurity is more important now than ever due to increased internet use and rising social engineering attacks like phishing and data theft. These attacks exploit mortal sins. The quotation from' Cyber security culture neutralizing cyber pitfalls through organizational literacy and training' highlights the challenges and the need for collaborative trouble in cybersecurity. Preparedness is crucial educating druggies, using strong security measures, and having exigency plans. Social engineering is a significant trouble because it manipulates people to gain sensitive information. To reduce pitfalls, individualities and associations must be watchful and visionary in guarding data. Understanding social engineering and following good security practices can help falling victim to these attacks. nonstop education and mindfulness help make a strong security culture and adaptability against these evolving pitfalls.

DOI: 10.17148/IJARCCE.2024.131139

REFERENCES

[1] X. Song et al., "Defining Social Engineering in Cybersecurity," IEEE Journals Magazine.

[2] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, and R. Hegarty, K. Rabie, and F. J. Aparicio-Navarro, "Discovery of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[3] I. Ghafir et al., "BotDet: A System for Real-Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.

[4] Stylish, R., "What You Need to Know About Social Engineering Phishing," Infotech. [Online]. Available: https://www.infotech.co.uk/socialengineering-and-phishing-definitiveguide

[5] I. Ghafir et al., "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74, no. 10, pp. 1-17, 2018.

[6] J. Abawajy, M. A. Hassan, and T. Kim, "Trust Exploitation in Social Engineering Attacks: A Review," Journal of Network and Computer Applications, vol. 192, p. 102901, 2021.

[7] B. Gupta, M. Lal, and K. Sharma, "AI-Driven Anti-Phishing Mechanisms: A Review of Behavioral and Contextual Approaches," ACM Trans. Cybersecurity, vol. 15, pp. 22-35, 2022.

[8] C. Hadnagy, "Social Engineering: The Science of Human Hacking," Wiley, 2020.

[9] J. Pavur et al., "Operational Disruptions in Healthcare Due to Social Engineering Attacks: A Case Study," J. Cybersecurity Res., vol. 28, no. 4, pp. 12-25, 2023.

[10] S. Ahmed, M. U. Rehman, and A. Khan, "Dynamic Phishing Detection Using NLP: An AI-Powered Approach," IEEE Trans. Inf. Forensics Security, vol. 16, pp. 2345-2357, 2021.

[11] R. Alshammari, A. Alenezi, and F. Altalhi, "Gamification Techniques in Cybersecurity Training: Enhancing Awareness and Retention," J. Educ. Comput. Res., vol. 60, no. 3, pp. 625-645, 2022, vol. 74(10), pp. 1- 17, 2018.