International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Social Engineering

Shraddha Shete , Nikita Solanki , Dhanshri Sakhale

Department of Computer Application, PES Modern College of Engineering, Pune, India

Guide – Prof. Miss. Rajlaxmi Kanade

ABSTRACT

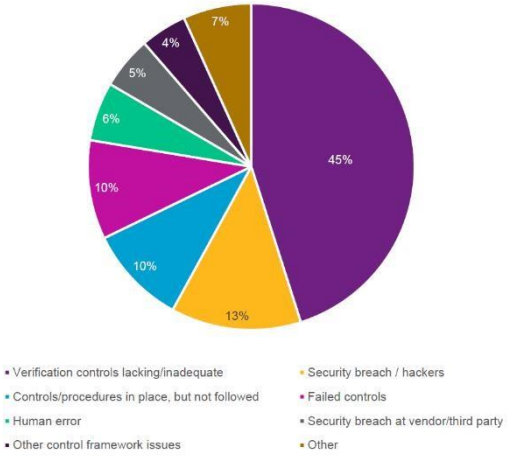
Social engineering is a type of cyberattack that relies on human psychology to trick victims into giving up sensitive information or taking actions that harm themselves or their organization. It is one of the most common and effective methods of cyberattack, and it can be used to steal passwords, credit card numbers, and other sensitive data. This paper provides an overview of social engineering, including its history, different types, and common attack vectors. It also discusses the psychology of social engineering and how to defend against it. The paper concludes by calling for more research on social engineering, as it is a growing threat to information security. Social engineering attacks can be divided into two main categories: pretexting *and* baiting*Social engineers are also very good at creating a sense of urgency or authority, which can make victims more likely to comply with their requests. There are a number of ways to defend against social engineering attacks. One important step is to train employees on how to identify and avoid social engineering scams. Organizations should also use security awareness tools to help employees spot suspicious emails and links. Social engineering is a serious threat to information security. However, by understanding how social engineering works and taking steps to defend against it, organizations can reduce their risk of falling victim to a social engineering attack.*

- ***Keywords :*** *Information security, social engineering, cyber security, cyber attack, hacking, Trust, Persuasion, Manipulation, Psychology, Awareness, Training, Prevention, Defense.*

1. Introduction

Social engineering is the art of manipulating people into giving up confidential information or performing actions that they would not otherwise do. It is one of the most common and effective methods of cyberattack, and it can be used to steal passwords, credit card numbers, and other sensitive data. Social engineering attacks can be divided into two main categories: pretexting and baiting. Pretexting attacks involve creating a false scenario in order to deceive the victim. For example, a social engineer might pose as a customer service representative in order to trick the victim into revealing their personal information. Baiting attacks involve sending the victim a malicious file or link that, when opened, will infect the victim's computer with malware. Social engineering attacks are often successful because they exploit the human tendency to trust others. Social engineers are also very good at creating a sense of urgency or authority, which can make victims more likely to comply with their requests. There are a number of ways to defend against social engineering attacks.

One important step is to train employees on how to identify and avoid social engineering scams. Organizations should also use security awareness tools to help employees spot suspicious emails and links. Social engineering is a serious threat to information security. However, by understanding how social engineering works and taking steps to defend against it, organizations can reduce their risk of falling victim to a social engineering attack.



2. Literature Survey:

2.1 What is social engineering?

Social engineering is a technique used by individuals or groups to manipulate or deceive others in order to gain unauthorized access to information, resources, or systems. It is a psychological manipulation tactic that exploits human behaviour and tendencies rather than relying solely on technical methods.

Social engineering typically involves exploiting trust, authority, or a sense of urgency to trick people into revealing sensitive information, performing certain actions, or compromising security measures. It can be conducted in various forms, such as in-person interactions, phone calls, emails, or online messaging.

2.2 Types of Social engineering attacks

Pretexting

In pretexting, the attacker typically poses as someone with authority, expertise, or a legitimate reason to request information or access. They may create a convincing backstory or fabricate a situation that evokes sympathy or urgency, making it difficult for the target to question their motives. The ultimate goal is to manipulate the target into providing the desired information or carrying out specific actions that benefit the attacker.

backstory or fabricate a situation that evokes sympathy or urgency, making it difficult for the target to question their motives. The ultimate goal is to manipulate the target into providing the desired information or carrying out specific actions that benefit the attacker.

One common pretexting scenario involves impersonating a member of a company's IT department. The attacker might contact an employee, claiming there is an urgent issue with their computer or network that requires immediate access. They may provide technical jargon to sound credible and gain the employee's trust. Once the attacker gains access, they can plant malware, steal sensitive data, or even expand their attack to other systems within the organization. Pretexting can also occur in other contexts, such as impersonating a customer, a service provider, or a government official. For instance, an attacker might call an individual, pretending to be a bank representative, and claim there is suspicious activity on their account. They may ask for personal information or instruct the person to transfer funds to a "secure" account, which is actually controlled by the attacker.

Phishing

Phishing is a type of cyber attack that involves fraudulent attempts to deceive individuals into divulging sensitive information, such as login credentials, credit card details, or personal data. It is a form of social engineering where attackers masquerade as trustworthy entities to trick victims into providing valuable information or performing actions that can be exploited for financial gain or unauthorized access. Phishing attacks commonly occur through various communication channels, including email, instant messaging, text messages (SMS), or even phone calls. Attackers employ psychological manipulation techniques to create a sense of urgency, curiosity, or fear, thereby increasing the likelihood of victims falling for their scams.

In a typical phishing scenario, attackers send deceptive emails that appear to originate from reputable sources, such as banks, social media platforms, or well-known organizations. The emails often contain convincing logos, branding, and language to make them appear legitimate. They may employ various tactics to entice victims into taking action, such as claiming there is a security breach, an account issue, or an urgent request for information.

These emails typically include malicious links that redirect victims to fraudulent websites resembling the legitimate ones. These fake websites are designed to collect sensitive data, often by mimicking login pages or forms where victims unknowingly input their credentials, which are then captured by the attackers. Alternatively, the email may contain attachments that, when opened, can install malware or ransomware onto the victim's device, allowing attackers to gain control or encrypt their files.

Vishing

Vishing, short for "voice phishing," is a form of social engineering attack that exploits phone communication to deceive individuals and gain unauthorized access to sensitive information. It involves fraudsters using voice calls to impersonate trusted entities, such as banks, government agencies, or service providers, with the goal of tricking victims into disclosing confidential data or performing certain actions.

During a vishing attack, attackers often employ psychological manipulation techniques to create a sense of urgency, authority, or fear, increasing the chances of victims falling for their schemes. They may use caller ID spoofing to display a legitimate phone number or even mimic automated voice systems to further enhance their credibility.

Shoulder Surfing:

Shoulder surfing is a type of information gathering technique used by attackers to gain unauthorized access to sensitive information by observing someone's computer screen, mobile device, or keypad entries. It involves physically positioning oneself close enough to a target to visually capture their actions or screen contents without their knowledge or consent. The term "shoulder surfing" stems from the idea of someone looking over your shoulder, as the attacker positions themselves discreetly to observe keystrokes, login credentials, personal identification numbers (PINs), or any other confidential information being entered.

Shoulder surfing attacks can occur in various contexts, including public spaces, workplaces, or even within the home environment. Attackers may take advantage of crowded areas, busy offices, or poorly designed workstations to blend in and gather valuable information.

Piggybacking:

Piggybacking, also known as tailgating, is a social engineering technique that involves unauthorized individuals gaining physical access to a restricted area by following closely behind an authorized person. This tactic exploits the natural inclination of people to hold doors open for others or to not confront unfamiliar individuals in shared spaces.

The concept of piggybacking is similar to someone sneaking into a building by closely following behind a person with authorized access, taking advantage of their legitimate entry to gain entry themselves. It can occur in various environments, including office buildings, residential complexes, or any location with controlled access points.

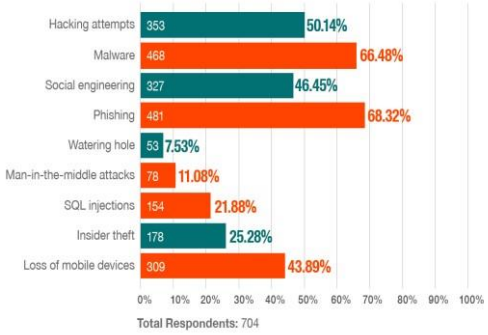
Piggybacking attacks can have serious security implications, as unauthorized individuals can gain access to areas that may contain sensitive information, valuable assets, or critical infrastructure. These attacks can lead to theft, data breaches, or compromise the safety of individuals within the premises.

Baiting:

Baiting is a social engineering technique where attackers intentionally leave physical or digital "bait" to lure individuals into taking actions that compromise their security or provide unauthorized access to their systems. It exploits human curiosity, greed, or helpfulness to manipulate victims into falling for the trap. In baiting attacks, the attacker strategically places enticing objects or content, such as infected USB drives, CDs, or even fake websites, where they know potential victims will find them. The goal is to exploit the natural inclination of individuals to pick up, use, or interact with items they come across.

One common example of baiting is the "lost USB drive" scenario. The attacker intentionally drops infected USB drives in public areas, such as office buildings, parking lots, or communal spaces. The drives are typically labelled with labels like "Confidential," "Salary Information," or other intriguing names, attracting the curiosity of individuals who find them. When the victim plugs the USB drive into their computer, malware is automatically installed, giving the attacker unauthorized access to their system.

Digital baiting techniques can include creating enticing online advertisements or email campaigns that offer free downloads, access to exclusive content, or the promise of financial rewards. When individuals click on these baits or download the offered files, they unknowingly infect their devices with malware or grant the attacker access to their personal information.



3. Impact of social engineering

Social engineering is a type of cyberattack that relies on human psychology to trick victims into giving up confidential information or performing actions that they would not otherwise do. It is a very effective attack vector, as it can exploit the human tendency to trust others and to be helpful. The impact of social engineering can be significant. It can lead to the theft of personal information, financial losses, and even the compromise of critical infrastructure. In some cases, social engineering attacks have even resulted in the deaths of individuals.

Here are some of the most common impacts of social engineering:

Data breaches: Social engineering attacks can lead to the theft of personal information, such as credit card numbers, Social Security numbers, and passwords. This information can then be used to commit identity theft, fraud, and other crimes.

Financial losses: Social engineering attacks can also lead to financial losses. For example, victims may be tricked into wiring money to a fake account or clicking on a malicious link that downloads malware onto their computer.

Loss of reputation: If an organization is the victim of a social engineering attack, it can damage the organization's reputation. This can lead to lost customers, decreased sales, and other financial losses.

4. Defending against social engineering

Social engineering is a type of cyberattack that relies on human psychology to trick victims into giving up confidential information or performing actions that they would not otherwise do. It is a very effective attack vector, as it can exploit the human tendency to trust others and to be helpful.

Here are some tips for defending against social engineering attacks:

Be careful about what information you share online: Don't share your personal information on social media or other online platforms. This information can be used by social engineers to create a false persona and gain your trust.

Educate yourself about social engineering: The more you know about social engineering, the better equipped you will be to spot and avoid social engineering attacks.

Use security awareness training: Security awareness training can help you learn how to identify and avoid social engineering attacks. This training should cover the different types of social engineering attacks, as well as how to spot the telltale signs of a scam.

Use security awareness tools: Security awareness tools can help you spot suspicious emails and links. These tools can also provide you with information on how to protect yourself from social engineering attacks.

Be aware of your surroundings: Be aware of your surroundings and be careful about who you give your personal information to. If you receive an unsolicited email or text message, don't click on any links or open any attachments.

Ask questions: If someone asks you for sensitive information, ask them questions to verify their identity. For example, you could ask them what department they're from, what their name is, and what their phone number is.

Report suspicious activity: If you think you've been the victim of social engineering, report it to the company or organization they claim to be from. You should also report it to the Federal Trade Commission (FTC). By following these tips, you can help protect yourself from social engineering attacks.

Here are some additional tips for defending against social engineering attacks:

Use strong passwords: Strong passwords are difficult to guess and crack. Use a combination of upper and lowercase letters, numbers, and symbols in your passwords.

Keep your software up to date: Software updates often include security patches that can help protect your computer from malware.

Back up your data: If your computer is infected with malware, you may lose your data. Back up your data regularly so that you can restore it if necessary.

5. Advantages

Assessing Vulnerabilities: By conducting social engineering experiments, organizations can identify weaknesses and vulnerabilities in their security systems and processes. This allows them to take proactive measures to strengthen their defences and protect against real-world threats.

Enhancing Security Awareness: Social engineering attacks can serve as wake-up calls for individuals and organizations, raising awareness about the importance of cybersecurity and the potential risks associated with trusting unknown or suspicious sources.

Training and Education: Organizations can use controlled social engineering exercises as training tools to educate employees about common social engineering tactics and teach them how to recognize and respond to such attacks. This can help improve overall cybersecurity awareness and preparedness.

Testing Incident Response: Social engineering simulations can be used to test an organization's incident response procedures and assess how well employees follow established protocols in the face of potential security breaches. This allows for refinement and improvement of response strategies.

Gathering Intelligence: In certain cases, government agencies or security organizations may use social engineering techniques to gather intelligence about potential threats or criminal activities. This can help in preventing and mitigating potential risks to national security.

6. Disadvantages

Exploitation and Manipulation: Social engineering involves the manipulation and deception of individuals, exploiting their trust, emotions, or vulnerabilities. This is inherently unethical and can cause harm, both psychologically and financially, to the targeted individuals.

Privacy Invasion: Social engineering often requires the collection of personal information about individuals without their knowledge or consent. This invasion of privacy is a significant concern and can lead to the misuse or abuse of sensitive data.

Legal and Ethical Issues: Engaging in social engineering activities without proper authorization is illegal in most jurisdictions. It violates laws related to privacy, fraud, and computer misuse. Additionally, social engineering goes against ethical principles, such as honesty, integrity, and respect for individuals' autonomy and privacy.

Financial and Personal Losses: Social engineering attacks can result in significant financial losses for individuals and organizations. Scammers may deceive individuals into revealing sensitive financial information, such as credit card numbers or bank account details, leading to fraudulent transactions or identity theft.

Weakening Security Awareness: While social engineering attacks can raise awareness about cybersecurity risks, they can also create a sense of scepticism and paranoia. This can undermine trust in legitimate communication channels and make individuals more susceptible to future attacks.

7. Applications

Security Testing and Assessments: Organizations may use controlled social engineering techniques to test the effectiveness of their security measures and identify vulnerabilities in their systems. By simulating social engineering attacks, organizations can assess the readiness of their employees and systems to resist and detect such attempts. their employees and systems to resist and detect such attempts.

Security Awareness Training: Social engineering can be employed as a training tool to educate individuals and employees about common tactics used by attackers. By experiencing simulated social engineering attempts, individuals can learn to recognize and respond appropriately to potential threats, enhancing overall security awareness.

Incident Response Testing: Social engineering simulations can be used to evaluate an organization's incident response capabilities. By observing how employees respond to social engineering attempts, organizations can identify areas for improvement and refine their incident response plans and procedures.

Red Team Exercises: Red teaming involves simulating real-world attacks to assess an organization's overall security posture. Social engineering techniques can be employed by the red team to test the effectiveness of physical security controls, employee awareness, and the organization's ability to detect and respond to social engineering attacks.

Risk Assessment and Policy Development: Social engineering can be utilized as a tool to assess an organization's susceptibility to attacks and identify potential risks. By understanding the techniques used in social engineering, organizations can develop policies and procedures that mitigate these risks effectively.

8. Future Enhancement

Stronger Authentication Methods: To combat social engineering attacks targeting passwords and authentication credentials, organizations are adopting more robust authentication methods. This includes multi-factor authentication (MFA), biometrics, and behavioural analytics, making it harder for attackers to impersonate legitimate users.

Continuous Security Testing and Red Teaming: Organizations are increasingly implementing continuous security testing and red teaming exercises to identify and address vulnerabilities. Regular assessments and simulations help evaluate an organization's resistance to social engineering attacks and improve incident response capabilities.

Improved Incident Response and Reporting Mechanisms: Organizations are strengthening their incident response capabilities to handle social engineering attacks effectively. This includes implementing clear reporting channels, establishing incident response teams, and conducting post-incident analysis to identify areas for improvement.

Security Awareness in Personal Life: Individuals are increasingly becoming aware of the risks posed by social engineering and are adopting security practices in their personal lives. This includes being cautious of sharing personal information online, verifying requests before responding, and regularly updating passwords.

9. Conclusion

Social engineering attacks can take many forms, from phishing emails to pretexting calls and baiting schemes. Phishing attacks use fake emails or websites to trick individuals into providing sensitive information, such as usernames, passwords, and credit card numbers. Pretexting involves creating a false pretext, such as pretending to be a customer or an authority figure, to gain trust and obtain sensitive information. Baiting involves tempting individuals with an offer or a reward, such as a free movie ticket or a USB drive, to get them to divulge information or perform an action, such as downloading malware or disclosing their credentials. Quid pro quo offers a benefit in exchange for information or access, such as offering a discount in exchange for a password or a badge. The success of social engineering attacks relies on exploiting human vulnerabilities and biases, such as trust, authority, urgency, and social proof. Social engineers use techniques such as

authority, urgency, and scarcity to create a sense of urgency and persuade individuals to act quickly without thinking critically. They also use social proof and liking to build rapport and create a sense of trust with their targets. For instance, they may use the name of a well-known brand or a person of authority to gain credibility, or they may use flattery and compliments to create a positive impression and build report.

10. References

[1]Cybersecurity: An Essential Guide to Computer and Cyber Security for
Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defence Strategies, and Cyberwarfare by Lester Evans

[2]https://www.vmware.com/topics/glossary/content/application-security
https://www.forcepoint.com/cyberedu/data-security

[3]https://en.wikipedia.org/wiki/Identity_management

[4]https://www.techopedia.com/definition/29841/database-security

[5]https://www.forcepoint.com/cyberedu/cloud-security

[6]https://whatis.techtarget.com/definition/mobile-security

[7] Social Engineering: The Science of Human Hacking by Christopher Hadnagy

[8] "Social Engineering Defined - Security Through Education". Security Through Education. Retrieved 3 October 2018.