Sri Lanka Institute of Information Technology

Module: IE2022

Year 2, Semester 1

Social Engineering

R.M RAAHIM MAHMOOTH IT23363366
B.Sc. (Hons) in Information Technology
Specialized in Cyber Security

Abstract

Social engineering is one of the most critical threats in the modern landscape of cybersecurity, leveraging manipulation of human behavior to ensure access to information or systems that are unauthorized. Review the report on how social engineering has evolved from historical examples, such as the Trojan Horse, to modern techniques, including phishing and AI-driven attacks. It enumerates the psychological principles attacked by attackers, inclusive of trust and fear, while it details impacts on individuals and organizations as financial losses, reputational damages, and psychological impacts. The mitigation strategies to be discussed will look upon policy enforcement, auditing, training, and the use of advanced cybersecurity tools as important lines of defense. It concludes the report with the likely future directions of social engineering, including more advanced AI-based techniques and IoT vulnerabilities.

Content

Chapter 1: Introduction

In the modern world of technology, lots of things are evolving day by day therefore humans also need to be updated. This is why two thousand has been known as the information era. Technologies are developing on the other hand, threats and risks are also increasing. A genius, **Gene Spafford,** once said, *"The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards"* This means you never get a 100% safe system unless it's entirely isolated and deactivated.
Social engineering means using tricks to exploit human behaviors and get them to reveal sensitive information that can be used in the wrong way by a malicious individual or group. Compared to the other types of cyber threats which tend to infiltrate system loopholes, social engineering threats collaborate with people's trust. Looking at the world that is connected as it is at present, social engineering is still one of the most efficient and lethal ways to get into the systems. Gaining unauthorized access to the information and systems involves the capacity to trick or mislead individuals in organizations of all sides is a risk. Social engineering is effective because it takes advantage of people, of human tendencies, to be trusting, helpful, and conflict avoidance. The attackers make these manipulations, with knowledge of people's behaviors, and the use of the psychological factors.

Cybercriminals get access to the system by identifying the system vulnerabilities in another way, they manipulate human behaviors through social engineering. It exploits human psychology to manipulate people into making mistakes and giving away confidential information. Specifically, if we are talking about cybersecurity, then social engineering is noted as bad. It means deceptive strategies employed by the aggressors to compel the targets to disclose some information which is personal or… password, credit card information, etc. These techniques rely on getting the human emotion (usually fear and urgency) to trust and fall for the trick and so they get a round technical security.

Information Gathering

In the real-world **social engineering** is widely used for various attacks including **phishing, pretexting, baiting, fake phone call, USB stick trap and impersonation**. Mostly these attacks are based on the victim's emotions such as fear, anger, carelessness, urgency, and confusion. In an attack scenario, a social engineering campaign will involve a plan to influence you or an employee to click a pop-up email like "***You won free in-game items! Click this link to claim them!!!***", Download a file or enable macros, Wire funds to the attacker's account, provide account credentials or through a fake phone call saying he/she have emergency, most commonly these kinds of attackers, before the execution of the attack they get to know every publicly available information about the victim (passive information gathering). Also, the attacker sometimes closely interacts with the victim to collect information and sensitive data. This is known as active information gathering. It is not always immoral or improper to use social engineering. However, it is still important to acknowledge that several companies – including cybersecurity ones – employ it to serve noble goals, such as during penetration testing, for instance. Social engineering is often used by ethical hackers as it creates realistic physical environments to assess the organization's security. It helps evaluate risks of failures in people- cantered security measures, for instance, vulnerability to phishing or control penalties. These can then go a long way towards enhancing the firm's shield mechanisms as well as availing the employees of the way they must comport themselves in the face of threats. Besides, it affords an organization the opportunity to be alert always of new strategies that may be employed by adversaries, thus minimizing future destructive experiences.

Chapter 2: Evolution of Social Engineering

Have you ever wondered where and what was the first record of social engineering has been played?
Computer technology has advanced enough to support the idea of security social engineering over the last few decades, but people have been using human psychology to manipulate other ways back for hundreds of years. The first recorded instances of social engineering – the ancient art of screwing people out of their money with a big smile day back, amazingly enough, to 1184 B.C. during the Trojan War
.

The First Recorded Social Engineering - The Trojan Horse Attack

Do you know the tale of Trojan Horse trick- a plot detailed in the great novel, The Odyssey? The year was 1184 B.C. The Trojans, Greeks engaged in shared war with Troy. After a decade-long siege, the Greeks recognized the need for a clever strategy to overcome the Trojans. They built a large wooden horse and hid the soldiers inside it. They left the horse at the gates of Troy as an offering of peace, and they had given up the fight. The Greek soldiers emerged from the horse and attacked the city of troy.
The story of the Trojan Horse serves as an outstanding lesson in manipulating emotions, providing the foundational understanding of how social engineering has been a part of human throughout history.

During the **Pre-Internet Era,** social engineering relied on face-to-face interactions. Impersonating authority figures like law enforcement or using pretexting, creating fabricated scenarios to manipulate human emotions was common. Early social engineers searched for information through Dumpster diving method, where they collect sensitive information's from discarded documents was a simple and effective method to gain personal information or organizational data. After the invention of computer, email and internet during **early 1990s-2000s**, there was a wide spread of using of email, which gave rising to phishing attacks, where attackers sent fake and anonymous emails that appeared in a form of legitimate source like bank or online service to trick and get the targeted person password, or credit card numbers and other personal

information's, Cybercriminals started to create more sophisticated pretexts, such as fake password requests, fake support requests to exploit people's trust in online communication.

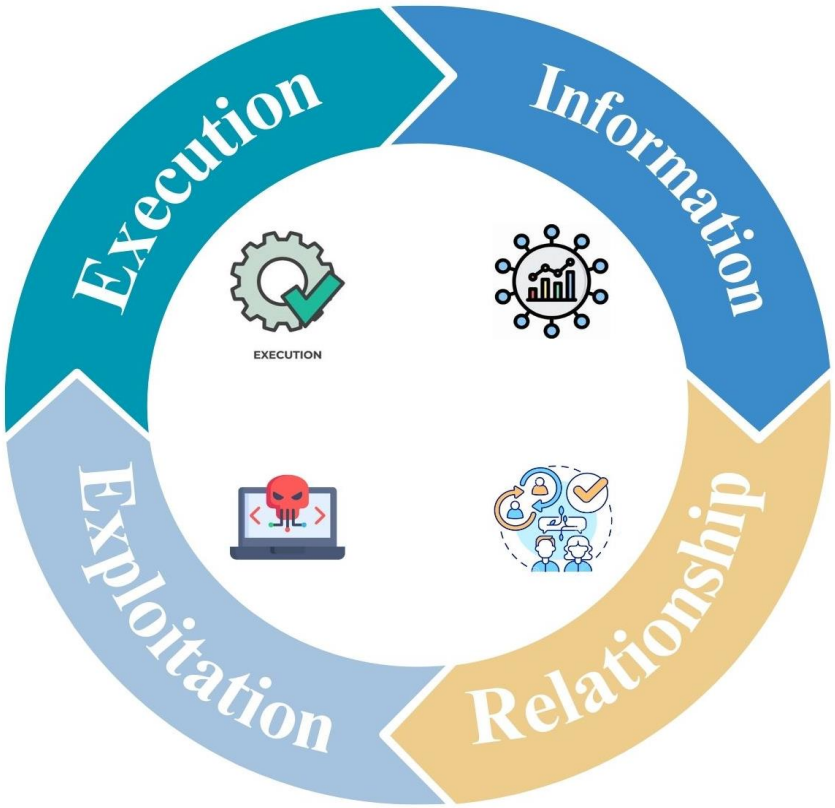
During the **social media era 2000-2010s**, the rise of social media platforms made social engineering attack far more easier , it enabled the attackers to gather details and personal information about the targeted victim, by analyzing the publicly shared data, People were also tricked into providing personal data and information through harmless online quizzes like fill the above from You will get free internet data or win a phone. The attacker tricked the people by downloading malware through "free" software, music, or videos. Social engineering **from 2010-Present**, attacker became incredibly talented and started conducting research targeting specific induvial or companies to create personalized email or messages that appeared as legitimate. Attackers often used to cooperate on high ended profile data breaches. Also aimed at the senior executives or high-ranked officials personal accounts and details. The attacker would tailor the content to the target's role in the relevant organization to gain access to valuable data of the organization and transfer funds.

Social engineering attacks in **the age of AI (Artificial Intelligence)**. In the recent years, the use of AI technology has enabled even more advanced method of attacking. It helped in creating deepfake realistic but fake images, audio, documents or videos and trick employees into performing harmful actions to the organization. Using AI automated tools attackers analyzed victims' behavior and generates human like conversations to increase the chance of success in manipulating. Attackers have become more personalized over time, focusing on one individual rather than random targets, while early phishing campaigns targeted a large number of audiences. Social engineering attackers have continuously adapted to changes in technology and communication, becoming far more sophisticated and harder to detect the attack. To decrease cybercriminal attacks, awareness and defensive measures must evolve in the ever-changing landscape of threats.

Chapter 3: Life Cycle of Social Engineering attacks

There is predictable four-steps that applies to social engineering attacks, typically referred as the attack cycle. This includes the following: information gathering, establishing relationships and rapport, exploitation, and execution.

However. Certain factors can cause this life cycle to repeat, either in a part or in a full, when targeting a specific individual, group, or an organization. For an instance of directly approaching the final target, an attacker may use a series of smaller attacks.



Life Cycle of social engineering

3.1 Life Cycle

Information Gathering	Criminals will research their targets via social media, blogs, and internet search
Relationship and rapport	Time to create a manipulative background via email or phone. Gaining trust is Key
Exploitation	An attacker impersonates someone important, making a demand usual under stress that leads to a branch.
Execution	The attacker exits and closes off communications quickly and quietly with money or valuable information

3.1.1: Information gathering

The likelihood of success for most attacks depends on this first phase: Information gathering, which involves collecting data about the target. This step is critical because it allows the attackers to understand the targets vulnerabilities and what is the best mechanism to exploit gathered information's.

Information gathering can be passive or active. In passive approach, the attackers collect publicly available information from various places (Open-source intelligence techniques (OSINT). This includes scanning social media profiles, blogs, public records, and websites to identify individuals, their roles, relationships and their personal interests and habits. An attacker could impersonate members of an IT team, like the hacker in Uber's compromise successfully did not gain access to the company's system.

In an active approach, the attackers interact with the target audience directly with the use of technical tools like sending fake websites to solicit further details and phishing emails. The attackers become familiar and comfortable with the target. The goal of this phase is to gain enough information to move to the next stage – establishing relationships and rapport.

3.1.2: Establishing relationships and rapport.

Once the attacker has gathered enough information, they will proceed to the next stage, which involves establishing rapport with the target. During this stage, the hacker develops a persona that would fit into the expectations or preference of the victim and portrays them as trustworthy or familiar. This may be in disguised to appear as a coworker, a trusted vendor, or even a friend of a friend.

In this stage, the key is establishing rapport. The attackers will discuss casual conversation topics with the target, give them praise, or show mutual interests. This will be done to decrease the guard and raise the comfort levels about trusting each other. In some instances, this would be supplemented by attackers with a sense of urgency or authority in coercing the victim into complying. It is expected that the more the victim feels comfortable, the more likely he or she is to release information or follow an attacker's instructions without any further question. The time needed can range from days to weeks to months, depending on the complexity of the attack and depending on how much trust would be required.

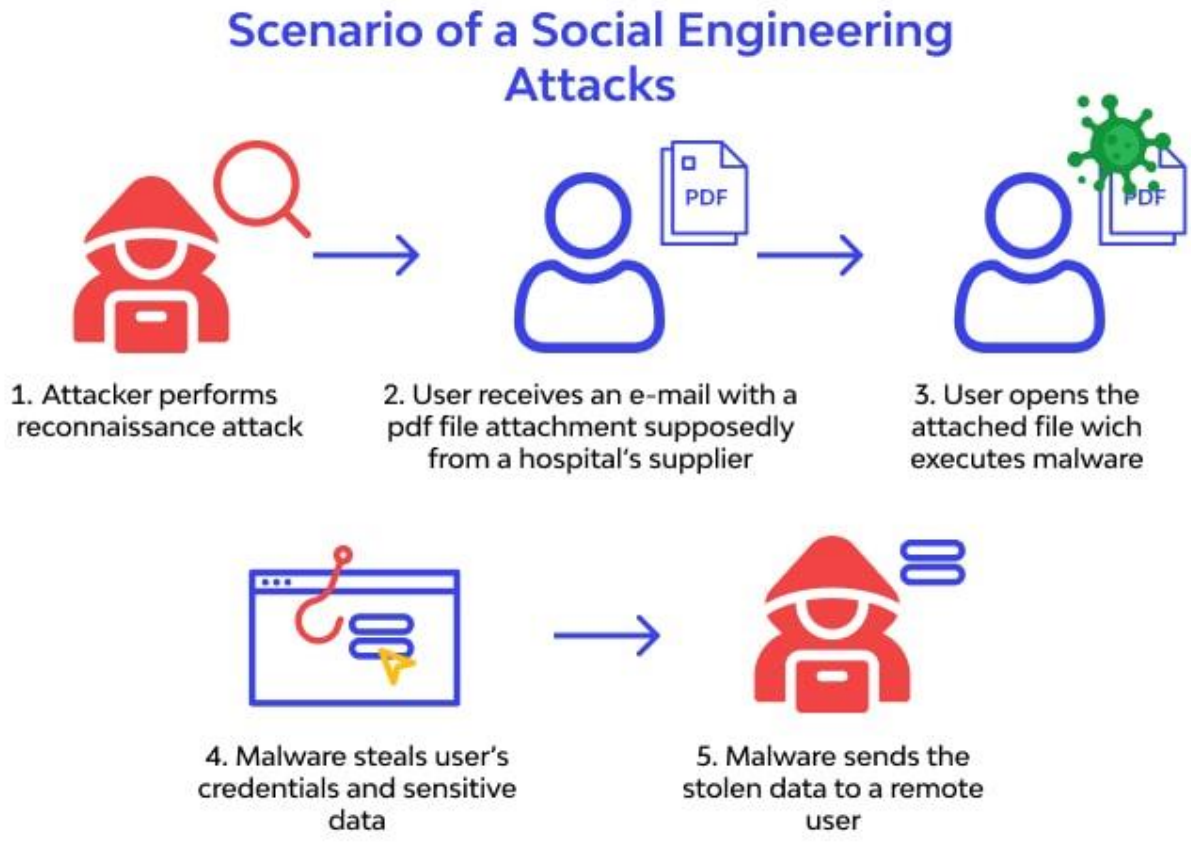
3.1.3: Exploitation

At the exploitation stage, an attacker utilizes the gained trust to influence the target audiences into revealing sensitive information or performing a particular action that is of benefit to the attacker. This is where the attacker's social engineering skills come to the fore, where one may request the victim to provide login credentials, open malicious email attachments, or gain access to secured areas or systems.

Depending on the target, there are many forms of attacks. In a spear-phishing attack, for instance, an attack can result in convincing a victim to click on a link that is malicious but shows a sense of legitimacy. In a more elaborate scenario, he could employ any of the two combined techniques, baiting, for example, which involves providing a lure piece of information or material, or quid pro quo where the target thinks that they are getting something in return for his or her cooperation. The attack at this point is near completion of his aim hence leading to the final act, which is execution.

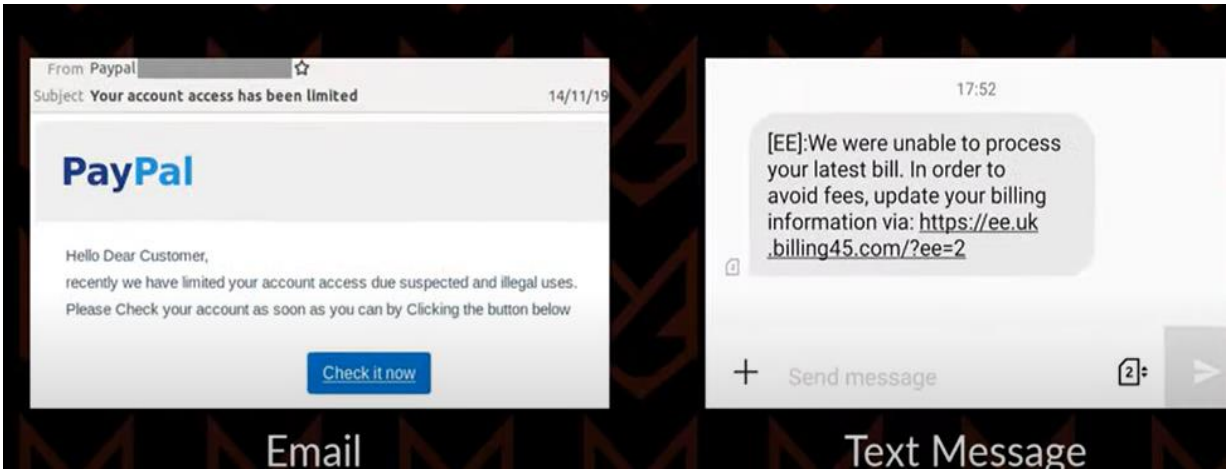
3.1.4: Execution

Execution is the stage where the attacker uses the information or access gained to attain their end goal, which may vary depending on the type of attack: from data theft and financial gain to malware spread and gaining control over a network. Sometimes it is immediate, such as stealing login credentials and then accessing accounts. In other contexts, the attacker can plant backdoors with the provided access to conduct further exploitation without the victim knowing. In this stage, the traces would be disguised by the attackers by making the detection possibility as minimal. They remove the records of the interaction, tamper with the logs, and thereby keep their activities in line with obscurity. At this point, the attacker can simply leave the system once the objective has been achieved or may continue re-exploiting the victim for more gain.



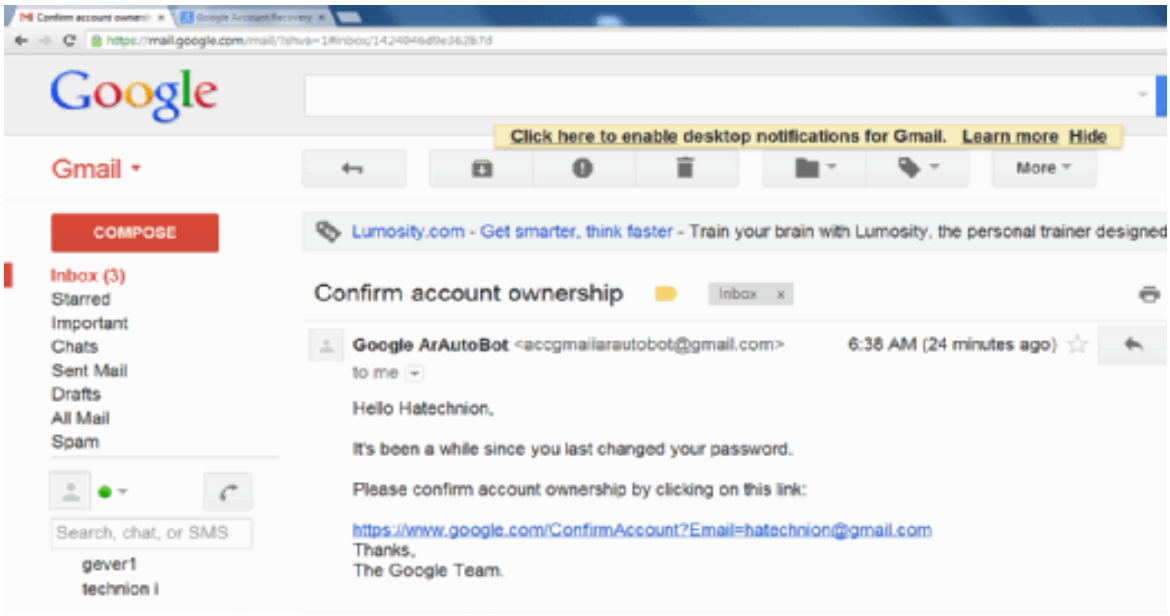
Chapter 4: Types of Social Engineering attacks

4.1 Phishing



Phishing is conducted through email and text message.

Phishing is a highly malicious and most common attack in which victims are tricked into providing **sensitive information**, in sense of **urgency, curiosity** and **fear**. They also create good imitations of other messages supporting to be from, for example, banks and other officially recognized institutions. Phishing presents a more pronounced risk to businesses more so because it deals with the last layer of security, the human one. An effective attack disrupts the whole network to compromise data, cause a loss of money, or harm reputation. Phishing poses a significant threat to businesses as it targets the weakest links in an organization, the human element. Mostly phishing attacks are conducted via emails, phone, SMS, social media, or other forms of personal communication for the user to click a malicious link or download infected information. Some phishing uses malware, bots, and trojans, to gain more user access.



Email that contains a link to click on and an urgent request for the user to respond quickly.

Common types of phishing attacks

i **Spear phishing** – A type of attack to target a specific individual in an organization. For instance, an employee is targeted to gain access to an organization's network.

ii **Whaling phishing** – The attack which is intended to target a high-profile individual often has deep access to sensitive areas of the network.

iii **Vishing** – A term used to define voice phishing, is an attacker who uses the phone to try to steal information. The attacker pretends to be a trusted friend or a relative or to represent them.

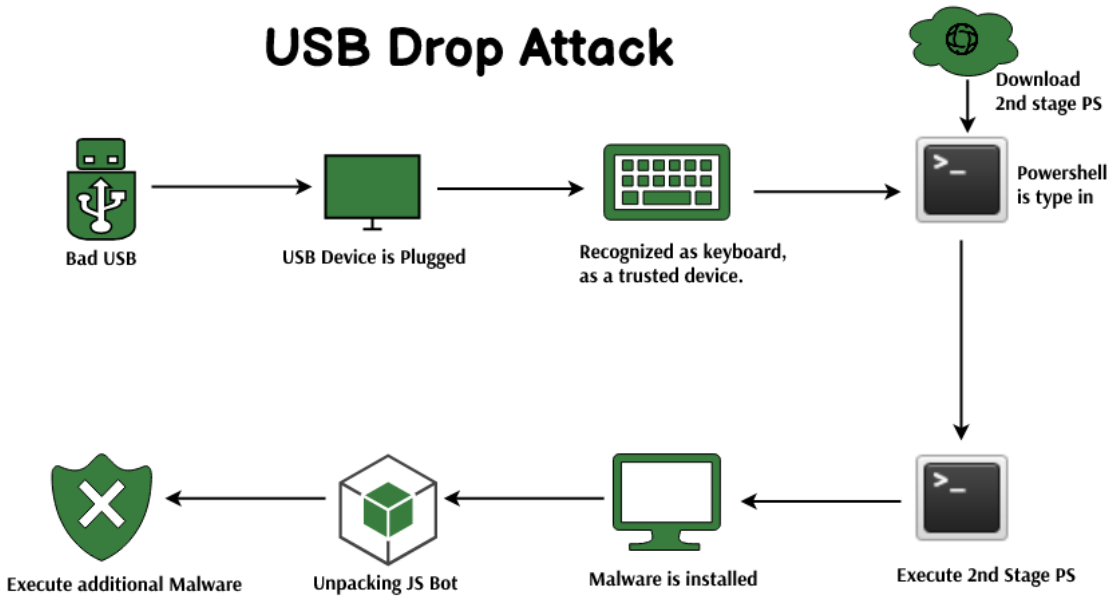
iv **Smishing** – The term is derived from SMS phishing, which is texts containing malicious links. The attackers might be from a cellular service providing you with a gift for paying your billon time, but when?

v click the link; your device may be infected by malware and other Viruses.

4.2 Baiting using USB devices.

As the name suggests, Baiting is a type of a social engineering attack where scammers make false promises to the user to lure them and reveal their personal information or install malware on the system. It is a technique that stimulates and exploits curiosity.

Baiting frauds can be in many different forms of tempting ads or online promotions, such as free game or movie downloads, music streaming or phone upgrades. The attackers hope that the password used by the user would be similarly used on other sites, which can allow the attackers to access the victim's information or sell the information to the attackers on the dark web.
Baiting can be also found in a physical form, most commonly via a malware-infected flash drive. The attacker would leave the infected flash drive in an area where the victims are mostly likely to see it.



USB Device attack

4.3 Pretexting

Pretexting is a form of social engineering in which an attacker tries to persuade a victim to give up valuable information, where attacker uses some sort of fabricated scenario in order to obtain sensitive information, systems, or services, which increases the likelihood of the success rate of a future social engineering attack.

Social engineering relies on a hacker impersonating a person that the victim trusts or knows, such as a colleague, delivery person, or government organization, in order to obtain access to information or sensitive systems. In many cases, pretexting may involve contact with human beings either in person or by means of a phony email address they use to initiate the first step of a potential attack aimed at breaking into a network or stealing data with the use of email. The story is effectively told in a pretexting attack through the use of legitimate-appearing message formats and images-such as government logos-tone, and wording. Keep in mind that an attack such as this can be done online, in person, or over the phone.

How pretexting is done

4.4 Impersonation

The concept of impersonation automatically makes one think about the art of deceit by pretending to be another person. In social engineering, it has developed into a sort of cyberattack. Cyber criminals are using it against organizations to gain access to networks and systems to commit fraud, identity theft, and sell data to the highest bidder on the dark web.

The genre of criminals exists, known as "pretexters, in which the act of impersonation is performed-just the way art would be impersonated within many means-reaching out to play the role of a trusted individual in order to extract sensitive information from the victim. Pretexting can be thought of as an art and practice of posing somebody else to mislead a recipient into divulging sensitive data such as passwords, credit card numbers, and other confidential information.

Another popular technique is pretexting, which involves one getting access to some restricted systems and/or services. An impersonator could play a wide array of roles in the course of his career- from other employees, technicians, IT support, auditors, or managers. To mount an effective attack, an impersonator has to research his target well. Impersonation attacks may be of many forms and can affect individuals as well as business entities.

Chapter 5: Psychology behind Social Engineering

Social engineering is a manipulative technique that leverages human psychology to gain much-needed information, access, or influence among the masses. Understanding the psychology behind social engineering significantly helps in devising ways and strategies whereby people and organizations can protect themselves against such methods. Here are some key psychological principles involved:

5.1 Trust and Authority

Social engineers may present themselves as authority figures by the use of a title, uniforms, or official documentation to establish credibility. Generally speaking, people tend to trust a person in authority and could well carry out a request that is made by them.

5.2 Scarcity and Urgency

A perception of urgency or scarcity can be used to prompt quick decisions without any thinking about the underlying reason for such choices. This can be quite common in phishing emails, where there is an urgent need to do something or face some undesirable outcome.

5.3 Reciprocity

This is the principle of returning favors. Social engineers may give something little or useful to make the victim feel obliged to comply with a subsequent request.

5.4 Social Proof

In deciding how to act, people often look to others in ambiguous situations. Social engineers might cite examples of others who have complied with similar requests to persuade their targets.

5.6 Fear and Anxiety

In general, threats-imagined or real-prompt one into action without giving much thought to critical thinking. Social engineers may now exploit such fear tactics, insinuating that dire consequences will be experienced if a request is not satisfied.

Chapter 6: Impact of Social Engineering

.6.1 Financial losses.

One of the direct and an the most severe impact of social engineering is financial losses, because of social engineering, both individual and organizational attacks may result in huge financial losses. The cost of these attacks can be substantial, with losses often reaching millions of dollars, mostly for large organizations. In addition to direct monetary losses, company or the organization may incur significant cost associated with investigating the attack and recovering the losses and additionally they can implement high security measures to prevent from future incidents In this regard, the FBI has stated that as of 2019, the loss resulting from BEC scams amounted to over $1.7 billion in the US alone, placing them at serious risk to company finances.

6.2 Reputational Damage

Reputational damage is another significant impact of social engineering attacks. When a company suffers a data breach or fails victims to a scam the public perception can be affected, this leads to the loss of customer confidence and damage to both the direct and indirect organization. The negative publicity can affect the growth of the organization, the incident can make it difficult for business recovery. It will also lead to a loss of clients, decreased sales, and a drop in stock prices. Rebuilding a damaged reputation often needs a considerable number of efforts, including additional security investments, additional stakeholder meetings which affect their busy schedules and public relation campaigns.

6.3 Psychological Effects

Apart from that, social engineering attacks psychologically affect the individuals. There is a possibility of victims experiencing stress, anxiety, and the loss of confidence, especially if an individual has caused a breach unknowingly. The feelings of employees who have fallen prey to social engineering techniques may be that of embarrassment or guilt; such feelings may reduce morale in the workplace, leading to low productivity. The threat of cyberattacks, on a larger scale, can be seen to give rise to a culture of fear and suspicion where trust in communications, both digital and interpersonal, would be lessened.

Chapter 7: Mitigation Strategies

In the earlier Chapters of this report, there had been discussions on the social terminology, how does social engineering operate which is by manipulating psychological principles to exploit the victims, the motivations of conducting social engineering attacks such as financial gains, politics, personal interest, and revenge.

Schneier (s) has stated: "***Procedures are a tough balancing act. If they are too lax, there will be security problems. If they are too tight, people will get around them and there will be security problems***" (Schneier on Security - People and Security Rules). Only after understanding the risks versus a threat can be administrated effectively and implement security measures.

7.1 Policy

Establishing certain rules and guidelines published to employees in an organization and following them to minimize the risk of social engineering attacks.
or legitimate activity. The published policies and guidelines should address acceptable behavior, data handling, and communication protocols. **Access Control Policy,** an organization or any site can restrict access to sensitive information on a need-to-know basis. Employees should only have access to the data required for their roles. **Incident Response Policy,** the user or the employee should take specific procedures for reporting and responding to suspected social. engineering attempts.

7.2 Auditing

Information Auditing is complimentary to a policy-based approach. The objective of auditing is to test the level of awareness or exposure to social engineering attacks. Auditing ensures the policies are followed and identifies areas of vulnerability. It helps access the effectiveness of security measures and compliance with the organization's rules and policies. Test the employee's readiness for social engineering attacks by simulating phishing emails and other attacks.

7.3 Education, Training and Awareness

Some of the major mitigation strategies towards ensuring security and reducing risks in various environments include education, training, and awareness. Education empowers the respective individuals with knowledge on potential threats, procedures, and best practices an organization wishes to promote for personnel to recognize risks and respond appropriately. Training programs can provide staff with the requisite competencies that will enable them to cope with security incidents, identify vulnerabilities, and apply appropriate preventive measures. Awareness campaigns instill a security-conscious culture that makes employees more vigilant and compliant with laid-down policies.

7.4 Install antivirus software and update.

Make sure automatic updates are engaged or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied and scan your system for possible infections.

7.5 Regularly check your credit reports and bank statements.

There are also some preventive measures that one could take, such as reviewing credit reports and bank statements. Being up to date will let you detect the thefts of money, other types of errors, or identity theft right there and then. This may be one good way of keeping your records updated and catching unusual activities right in their tracks.

7.6 Do not open emails and attachments that are suspicious.

If you do not know the sender in question, you do not need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider’s site.

7.7 Use multifactor authentication.

One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.

7.8 Be wary of tempting offers.

If an offer sounds too enticing, think twice before accepting it as a fact. Googling the topic can help you quickly determine whether you are dealing with a legitimate offer or a trap.

Chapter 8: Tools and Technologies for defense

8.1 Email security solutions

Proofpoint

Enterprise Cybersecurity Solutions, Services & Training | Proofpoint US

Microsoft Defender for office 365

Microsoft Defender for Office 365 | Microsoft Security

8.2 Multi-Factor Authentication

Google Authentication

Get verification codes with Google Authenticator - Android - Google Account Help

Duo security

Identity Security, MFA & SSO | Duo Security

8.3 Security Awareness Training

KnowBe4

.Security Awareness Training | KnowBe4

SANS security awareness

.Security Awareness Training | SANS Security Awareness

8.4 Endpoint protection Platform

CrowdStrike: We Stop Breaches with AI-native Cybersecurity

8.4.2 McAfee Endpoint security

Antivirus, VPN, Identity & Privacy Protection | McAfee

Chapter 9: Future Developments in the Area

9.1 AI-Driven Attacks

With the progress in artificial intelligence and machine learning, new attack vectors have opened up for attackers in constructing highly sophisticated social engineering attacks. In the AI-driven phishing attack, ML algorithms can be used to automatically personalize phishing emails to make them highly relevant and convincing to the individual targeted. For instance, this can be done by AI delivering messages in the same tone and writing style as the target's contacts through aggregations from social media, professional networking sites, or other publicly available information. Most importantly, AI-generated deepfake voice or video could also be used in voice phishing- or video phishing in which an attacker calls or sends a video while impersonating trusted contacts or any authority figure, making such an attack more persuasive and difficult to recognize.

9.2 IoT Exploitation

The rapid expansion of the IoT has developed a huge network of connected devices that any attacker would love to take advantage of. IoT devices often only have minimal security and can, in turn, be manipulated easily by attackers. In such a context, the attackers leverage such devices to access sensitive information or use them as launching pads for larger attacks. For instance, an attacker may compromise a smart camera to monitor activities of a target, engage in smart speakers to issue malicious commands, or even leverage vulnerabilities in smart medical devices to affect patient treatment. In critical infrastructures such as power supply networks or traffic management, IoT gadgets that have been compromised will lead to paralysis in activities or support more extensive cyberattacks with greater damage.

9.3 Improved Social Media Exploitation

Social media is a were attackers research targets for intelligence. As more people and businesses continue to use social media, the attacker can use advanced data mining techniques to sift through large volumes of personal and organizational information. Machine learning algorithms can facilitate the construction of remarkably realistic fake profiles, elaborate online personas, or even fake

connections. These techniques allow attackers to conduct social engineering attacks, such as spear phishing or whaling, with the greatest success rate because the methodology of the attacker appears credible and knowledgeable due to the information gathered.

9.4 Behavioral Biometrics

Behavioral biometrics, which would involve analysis of habits such as type speed, mouse movements, or navigation behavior is also on the rise in order to verify or identify people. While it is considered far more secure than simple biometrics, such as fingerprints or facial recognition, it cannot be fully denied that behavioral biometrics are resistant to manipulation. The hackers of the future might try to reproduce the pattern of a target in order to spoof an authentication system. For instance, expert algorithms may learn the typing rhythm of a person or his navigation habits and then mimic those to get through security controls. This may be a channel through which the attacker gains unauthorized access to sensitive systems or data.

In all these cases, the attackers employ the latest in advanced technology to bypass security measures placed originally. Thus, the updating of defensive measures and vigilance in cybersecurity practices is a matter of grave concern.

Conclusion

The report has shown that social engineering has been a huge threat in the modern landscape of cybersecurity, one which keeps on changing. These social engineering attacks rely on a form of psychological manipulation to develop conditions under which people may leak sensitive information or take detrimental actions. Over time, these have evolved from simple pretexting to advanced AI-driven phishing and deepfake-based manipulation. Key techniques used include phishing, baiting, impersonation, and pretexting, variously based on the manipulation of human feelings like trust, fear, and urgency. This report thus reinforces the need for awareness, training, and policy-based methods in mitigation. Future developments will see the social engineering threat become increasingly targeted and technologically sophisticated, thus calling for continuing refresh of the defensive measures.

In the future, social engineering attacks will continue to become increasingly sophisticated, leveraging AI in driving attacks where machine learning algorithms create highly personalized phishing attempts or deepfake videos. The rapid expansion of IoT devices will result in new vulnerabilities as attackers leverage devices with poor security. Attackers will try to spoof authentication systems by simulating behavioral biometrics-for instance, typing speed or mouse movements. Since attackers are constantly changing, the defensive measures need to do so faster to stay ahead.

Reference

- **B. Schneier, "Schneier on Security - People and Security Rules." [Online]. Available: https://www.schneier.com. [Accessed: Oct. 9, 2024].**
- **FBI Internet Crime Report, "Business Email Compromise the 1.7 billion-Dollar Threat," 2019.**
- **Proofpoint, "Enterprise Cybersecurity Solutions Services & Training." [Online]. Available: https://www.proofpoint**No table of contents entries found.**.com. [Accessed: Oct. 9, 2024].**
- **Microsoft, "Microsoft Defender for Office 365," [Online]. Available: https://www.microsoft.com. [Accessed: Oct. 10, 2024].**
- **Google, "Get verification codes with Google Authenticator," [Online]. Available: https://support.google.com. [Accessed: Oct. 11, 2024].**
- **SANS Security Awareness, "Security Awareness Training," [Online]. Available: https://www.sans.org. [Accessed: Oct. 11, 2024].**
- **CrowdStrike, "We Stop Breaches with AI-native Cybersecurity," [Online]. Available: https://www.crowdstrike.com. [Accessed: Oct. 11, 2024].**
- **McAfee, "Antivirus VPN Identity & Privacy Protection," [Online]. Available: https://www.mcafee.com. [Accessed: Oct. 11, 2024].**
- **D. B. Olabode and A. E. Elijah, "Social Engineering Attacks," *ResearchGate*, Feb. 2022. [Online]. Available: https://www.researchgate.net/publication/358647625_Social_Engineering_Attacks. [Accessed: Oct. 11, 2024].**
- **Up Guard, "Impersonation Attack," [Online]. Available: https://www.upguard.com/blog/impersonation-attack. [Accessed: Oct. 13, 2024].**
- **M. Hassan and P. Kumar, "Analysing Social Engineering Attacks and Its Impact," *ResearchGate*, Jul. 2024. [Online]. Available: https://www.researchgate.net/publication/376443039_Analysing_Social_Engineering_Attacks_and_its_Impact#fullTextFileContent. [Accessed: Oct. 13, 2024].**
- **L. Tiwari and N. Gupta, "Social Engineering and Its Importance," *ResearchGate*, Sep. 2021. [Online]. Available: https://www.researchgate.net/publication/354849736_SOCIAL_ENGINEERING_AND_ITS_IMPORTANCE#fullTextFileContent. [Accessed: Oct. 13, 2024].**

- **R. Anderson, "Social engineering: Principles and techniques," *IEEE Transactions on Security and Privacy*, vol. 15, no. 6, pp. 34-45, 2023.**
- **J. Smith and M. Jones, "The rise of phishing attacks: A comprehensive study," *International Journal of Cybersecurity*, vol. 18, no. 3, pp. 123-135, 2022.**
- **T. White, "Deepfake and AI-driven social engineering: Implications for the future," *IEEE Computer Society*, vol. 52, no. 9, pp. 66-74, 2023.**
- **K. Brown, "Social engineering in the age of IoT: New threats and defenses," *Journal of Information Security*, vol. 29, no. 2, pp. 98-112, 2024.**
- **A. Patel, "The psychology of phishing: Why people fall for scams," *Cyberpsychology*, vol. 11, no. 1, pp. 45-56, 2022**