University of Jeddah
College of Computer Science and Engineering
Department of Cybersecurity

Direct and Physical Social Engineering

By

Mashaer Aldeghalbi 2211175

Yara Alamri 2210362

Talah Fairaq 2006819

TABLE OF CONTENTS

01 Introduction

02 Differences between direct and physical social engineering

03 How does social engineering work?

04 Types & Techniques of social engineering attacks

05 Examples

06 Prevention Techniques

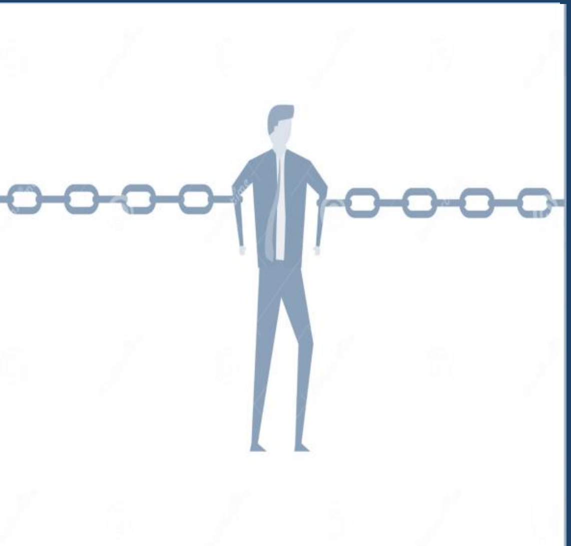
07 Social engineering and KSA

08 Conclusion

Introduction

Protecting sensitive data is important for people, governments, and organizations.
Although information protection is becoming increasingly effective,
people remain vulnerable to tampering and the HUMAN OBJECT IS WEAKEST LINK

What is Social Engineering ?



- **The way of influencing and deceiving someone into disclosing private information.** [2]

- **The main objective is to gain the trust of targets.** [1]

- **Social engineering includes a set of techniques used to trick people to disclosing sensitive information throughout face-to-face interactions, over the phone, emails, websites , etc.** [2]

Definitions

What is The Difference Between Direct and Physical Social Engineering ?

Direct social engineering Using interpersonal interactions, one manipulates individuals or groups.

- ➢ Face-to-face interactions.
- ➢ Phone calls.
- ➢ Internet communication.

Physical social engineering: Using physical objects or direct physical access, one manipulates others.

- ➢ Unauthorized entry.
- ➢ Tampering with devices/systems.
- ➢ Stealing physical.

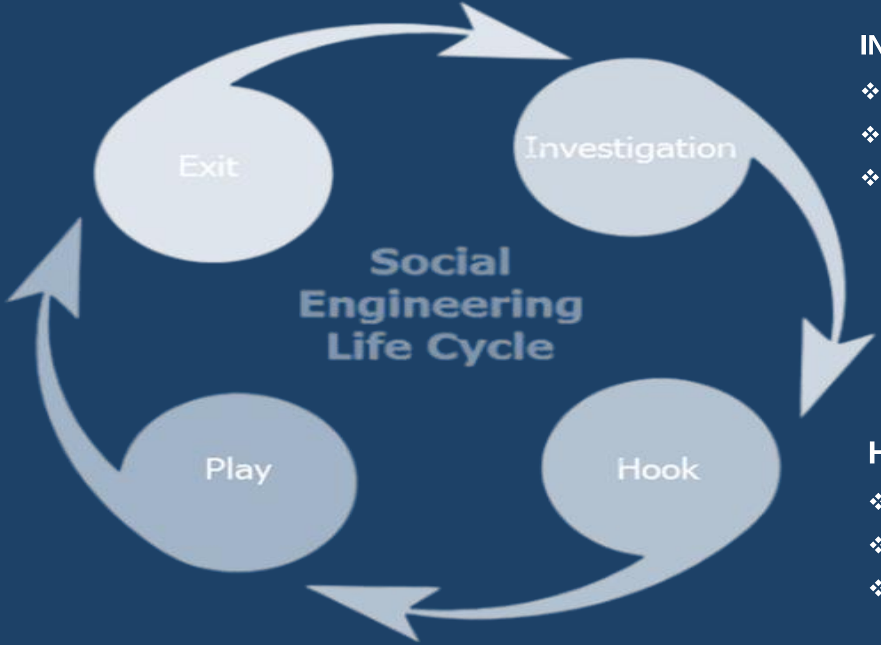
How Does Social Engineering Work ?

EXIT [3]

- Removing malware
- Cover tracks
- End the attack

INVESTIGATION [3]

- Identify the victims
- Gather background information
- Selecting attack method



PLAY [3]

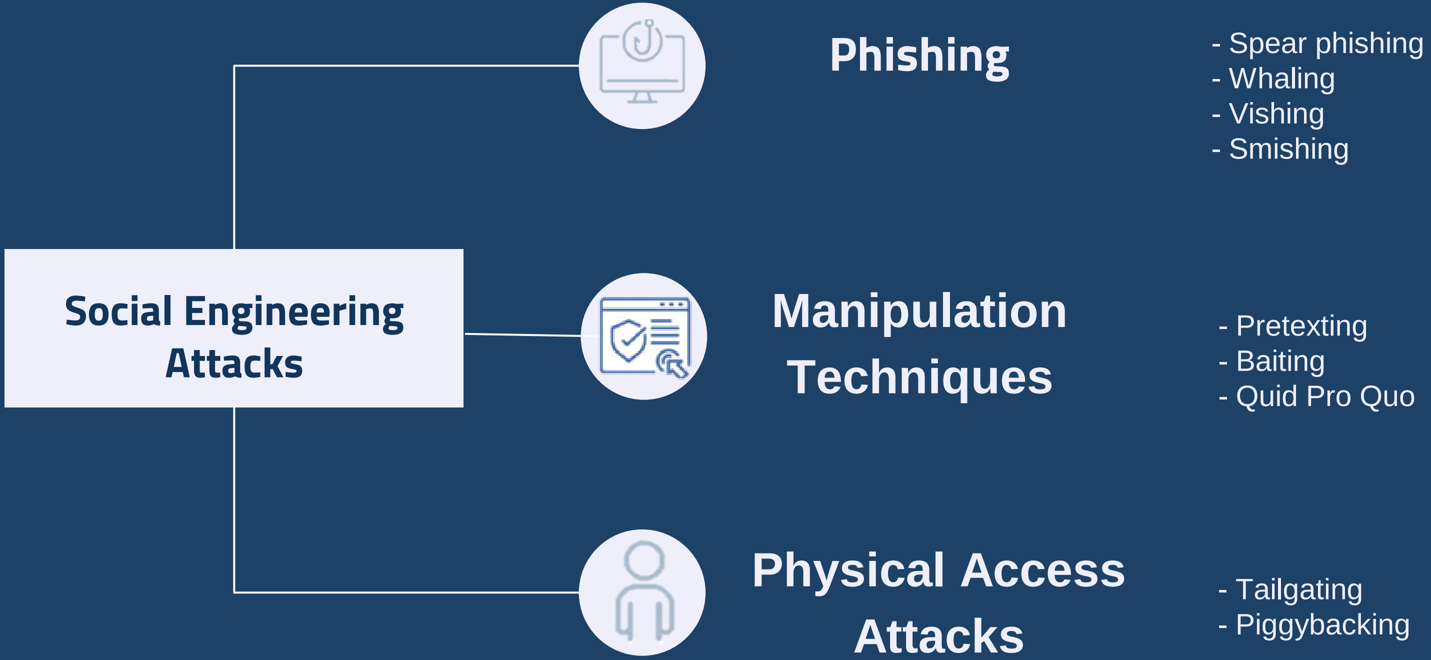
- Expand foothold
- Executing the attack
- Disrupt business

HOOK [3]

- Engage the target
- Spinning a story
- Taking control of the interaction

Types of Social Engineering

Types & Techniques of Social Engineering Attacks



Social Engineering Attacks

Phishing

- Spear phishing
- Whaling
- Vishing
- Smishing

Manipulation Techniques

- Pretexting
- Baiting
- Quid Pro Quo

Physical Access Attacks

- Tailgating
- Piggybacking

Phishing

1) Spear phishing: Is the practice of sending emails to specific individuals that have been previously researched in order to appear more convincing.[5]

2) Whaling: Highly targeted phishing attempts against high-level executives within a company.[5]

3) Vishing: Refers to phone calls that seek to deceive victims into exposing critical information or enabling remote access.[5]

4) Smishing: Is the practice of sending text messages via social engineering techniques similar to phishing emails.[5]

Manipulation Techniques

1) Pretexting: Creating a situation in which the victim feels forced to obey under fake circumstances, frequently by posing someone from a reputable organization.[5]

2) Baiting: Offering an easy reward (free download, gift card) to convince victims to provide passwords or install malware.[5]

3) Quid Pro Quo: Offering to "fix" an IT problem as a reward they request the victim's login information.[5]

Physical Access Attacks

1) Tailgating: Is the act of closely following an authorized individual in order to gain illegal entrance to a restricted position.[5]

2) Piggybacking: Getting an authorized person to allow access by leaving a door open or pretending to be an employee who forgot their passwords.[5]

Examples of Physical Social Engineering

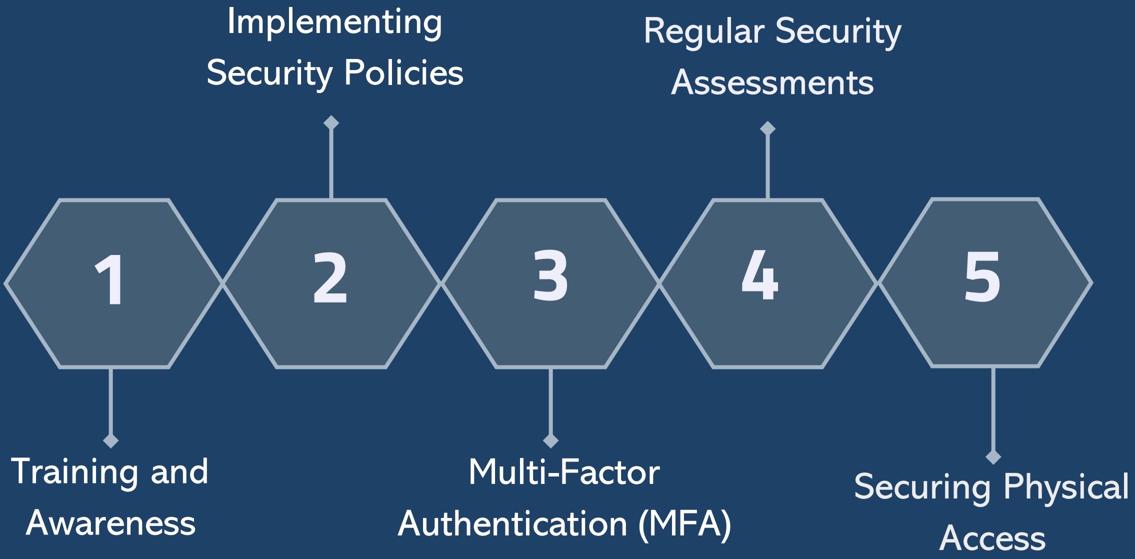
Fake IT guy and Dumpster diving

Be Aware of Fake IT and Dumpster Divers
Here's how attackers might gain access through social engineering:

- Pretending to be IT: Assume a fake IT specialist arrives at your company, asking to examine an equipment. Some devices inform IT to possible problems, making the argument sound realistic.[6]
- Faking authorization: In order to appear real, they may supply incorrect serial or device numbers. While some companies validate these details, attackers may exploit a security weakness.[6]
- Dumpster diving for information: Attackers may navigate through your company's trash for thrown documents that include serial numbers or other important information. The information that was stolen can then be misused to avoid safety protocols.[6]

Prevention Techniques

How to Prevent Social Engineering Attacks ?



1 Training and Awareness

2 Implementing Security Policies

3 Multi-Factor Authentication (MFA)

4 Regular Security Assessments

5 Securing Physical Access

Training and Awareness

Educating about the tactics used in social engineering attacks is crucial. Training should include how to recognize suspicious emails, phone calls, or in-person interactions and what steps to take when encountering them.

- Verify Email Sender's Identity.
- Identify your critical assets which attract criminals.
- Check the URLs. The URLs which start with https:// can be considered as trusted and encrypted website. The websites with http:// are not offering a secure connection.[7]

Implementing Security Policies

We've established clear security policies and procedures. These aren't just rules; they're guidelines to help understand the responsibilities when it comes to protecting data and handling sensitive information. From password management to data encryption, policies cover it all.[7]

Multi-Factor Authentication (MFA)

Using just a password isn’t enough to protect your accounts anymore. Multi-Factor Authentication adds extra layers of security, like a code sent to your phone(OTP), making it much harder for attackers to break in.[7]

Regular Security Assessments

Conduct regular security assessments to keep the systems in check. Vulnerability scans and penetration testing help us identify any weaknesses that could be exploited through social engineering attacks. It's all about staying one step ahead.[7]

- Continuously Monitor Critical System
- Utilize Next-Gen cloud-based WAF
- Penetration Testing
- Check and Update your Security Patches
- Enable Spam Filter

Securing Physical Access

Controlling physical access to sensitive areas and equipment through measures such as keycard access, security guards, and surveillance cameras can help prevent physical social engineering attacks.[7]

Social Engineering and KSA

Social Engineering and KSA

In an age of digital transformation and rapid technological advancement, the Banking, Financial Services, and Insurance (#BFSI) sector in Saudi Arabia, like the rest of the world, faces an escalating threat from cyberattacks, particularly social engineering attacks.[8]

But as cyber threats continue to evolve, Saudi Arabia is one of the world's leaders in cybersecurity development and preparedness, according to the latest rankings. The Kingdom of Saudi Arabia has secured second place in the Global Cybersecurity Index in the World Competitiveness Yearbook for 2023.[8]

Conclusion

Social engineering stands as a significant threat to individuals, governments, and organizations. Throughout our discussion, we've explored its distinguishing between direct and physical manipulation, understanding its methods, tactics and underscored the importance of prevention techniques.

In essence, by nurturing awareness, resilience, and collaboration, we can navigate cybersecurity challenges with confidence. Let's remain committed to safeguarding sensitive information and preserving our digital environments.

THANKS YOU ❤

DO YOU HAVE ANY QUESTIONS ?

Reference

[1] CISCO, “What is social engineering in cybersecurity?,” *Cisco*, 2023. https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

[2] M. N. O. Sadiku, A. E. Shadare, and S. M. Musa, “Social Engineering: An Introducction,” *ResearchGate*, Jul. 29, 2016. [Online]. Available:https://www.researchgate.net/publication/308315268_Social_Engineering_An_Introducction#:~:text=Social%20engineering%20consists%20of%20techniques%20used%20to%20manipulate,access%20to%20information%20or%20breaking%20normal%20security%20procedures

[3] “What Is Social Engineering? Definition, Types, Techniques of Attacks, Impact, and Trends |.” https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-social-engineering/

[4] V. Styran and V. Styran, “Social Engineering: What It Is and How to Prevent It? | BSG Blog,” *BSG Blog | Berezha Security Group*, Nov. 19, 2021. [Online]. Available: https://bsg.tech/blog/social-engineering-what-actually-is-it-and-how-to-prevent-an-attack/

Reference

[5] M. Security, "6 Types of Social Engineering Attacks," *www.mitnicksecurity.com*, Apr. 05, 2021. https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks

[6] "Physical social engineering attacks: how ready are you?," Jan. 30, 2020. https://welcomegate.com/physical-social-engineering-attacks-how-ready-are-you/

[7] Cybersecurity & Infrastructure Security Agency, "Avoiding Social Engineering and Phishing Attacks | CISA," *Cybersecurity and Infrastructure Security Agency CISA*, Feb. 01, 2021. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

[8] "Social Engineering in Saudi Arabia's BFSI Sector: Ongoing & CyberFuture," *www.linkedin.com*. https://www.linkedin.com/pulse/social-engineering-saudi-arabias-bfsi-sector-ongoing-cyberfuture/ (accessed Mar. 03, 2024).

Note: At slide 6, I used two resources [2] and ChatGPT to explain carefully to me, and I wrote down what I understood.