

# Social Engineering

## Introduction

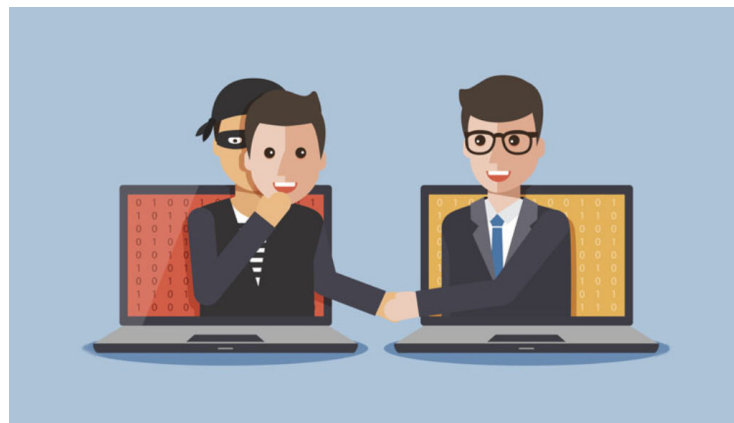
In the term of computer & cyber security, social engineering define a type of attack in which the attacker exploit human vulnerabilities by means such as influence, persuasion, deception, manipulation and inducing, so as to get classified information, hack computer system and network, obtain unauthorized access to restricted areas, or breach the security goals (such as confidentiality, integrity, availability, controllability and auditability) of cyberspace elements (such as infrastructure, data, resource, user and operation).

## Content

- - What is social engineering?
- - Types of social engineering
- - Life Cycle of Social engineering attack
- - Impact of Social Engineering
- - Social Engineering & information system security

## Social Engineering Definition

Social Engineering is the art of Human Hacking. The attempt to control human Social Behaviours & Natural Tendencies is called as social Engineering. Social engineering attacks that include interpersonal interaction involve direct communication (such as in person or by telephone) or interaction that is mediated through electronic means (e.g., electronic media, email, and Internet).



Social engineering is the act of gaining either unauthorized access to a system or sensitive information, such as passwords, through the use of trust and relationship building with those who have access to such information. A social engineer uses human psychology to exploit people for his or her own use.

## Classification of Social Engineering

There are two aspects of Social Engineering. Such as-

### ☐ Human based

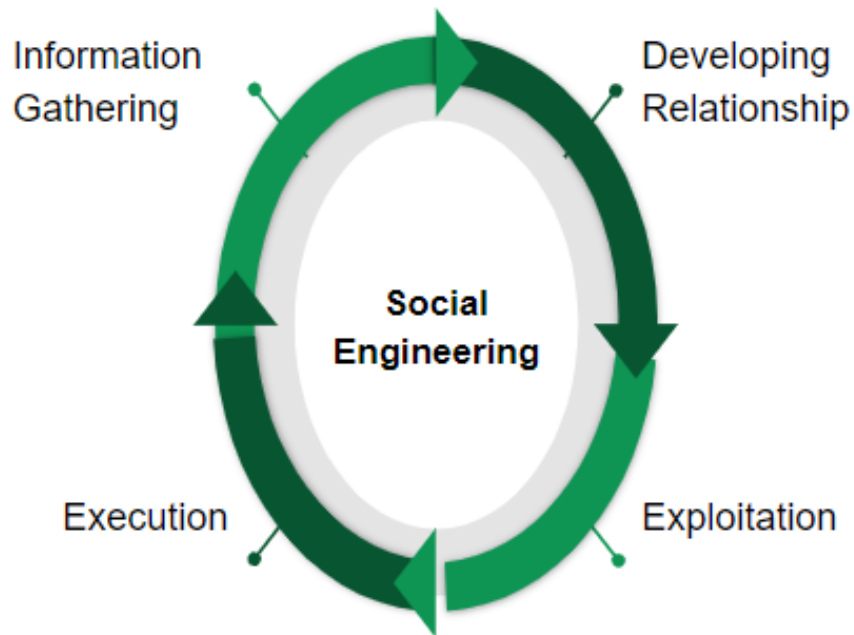
- **Impersonation:** In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor.
- **Being a third party:** In this attack, the hacker pretends to have permission from an authorized person to use the computer system. It works when the authorized person is unavailable for some time.

- **Posing as an important user:** In this type of attack, the hacker pretends to be a VIP or high-level manager who has the authority to use computer systems or files

## □ **Computer Based**


- **Phishing:** An exploit generally defined as a phisher impersonating a trusted third party to gain access to private data. Victim are Providing Confidential Information through email, text, pop-up for the Urgency, Curiosity, & Fear by attacker.
- **Baiting:** Baiting involves dangling something you want to entice you to take an action the criminal desires. Attacker provide fake offers or bait, where attached malware or spyware. It can be in the form of a music or movie download on a peer-to-peer site or it can be a USB flash drive with a company logo labeled. Then, once the device is used or downloaded, the person or company's computer is infected with malicious software allowing the criminal to advance into your system.
- **Spear Phishing:** Specific version of phishing where an attacker chooses specific individuals or enterprises. the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
- **Scareware:** victims being bombarded with false alarms and fictitious threats. malicious computer programs designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection.
- **Pretexting:** A pretext is a made-up scenario developed by threat actors for the purpose of stealing a victim's personal data. Intruders impersonate as a bank official, police officer, etc and cleverly manipulate user to provide the credential.

## Life Cycle of Social engineering



**Information Gathering:** The foremost step of a social engineering attack is information gathering. At this stage, the attacker gathers information about target to gain credibility and to establish a trust relationship. The attacker may receive information about preferences, understanding, political affiliation, educational backgrounds, family information, financial information and other social information.

**Developing Relationships:** After data collection, the attacker uses to start a targeted interface by using the collected data. Once the attacker builds trust of target, he then moves to the next step.



**Exploitation:** The backbone step of social engineering attacks life cycle is exploitation. At this stage, the attacker calls for a task to be carried out. This may be a malicious activity, such as logging in, or may be software installation or other malicious activities. Consequently an attacker has already build the trust of the target, many psychological factors may carry out such activities. This action has different types of features including spam email, trickery, password reset, logging in and cloud access.

**Execution:** The subsequently step of the social engineering attacks life cycle is execution. During the execution phase the attacker receives sensitive information, log-in credentials and access to the cloud or system.

## **The 3 Critical Success Factors:**

- **Trust:** You must be trusted by your victim.
- **Satisfaction:** Your opponent must be satisfied to you
- **Relation Ship:** The relationship between you & target person will be good.

## **Impact of Social Engineering:**

**It exploits the Human Psychology to Manipulate people into-**

- Making Security mistakes
- Giving away Confidential Information

**For this reason the victim faced in-**

- Financial implications.
- Productivity costs.
- Operational disruption.
- Reputational damage.

## **Social Engineering & Information System Security:**

You need to be follow some method for securing your Information System from Social Engineering attack.

### **Such as-**

- You have to be very attentive in determining fake offers.
- Avoid opening unknown email and attachments.
- Avoid sharing personal information.
- Use two-factor or multifactor Authentication.
- Keep your device updated.

## **Conclusion**

Social engineering attacks are particularly difficult to mitigate, due to diversity in techniques and targeting human weakness. The human vulnerabilities are the main cause of failure in detection of these attacks. The lack of knowledge of these attacks makes this technique more powerful and difficult to detect. . Knowledge awareness sessions have proven to be ineffective in mitigation of these attacks. A key mechanism for combating social engineering must be the education of potential victims, in order to raise their awareness of the techniques and how to spot them. To protect the Social Engineering, employee or individual education, training & awareness is the key. Policies, procedures and standards are an important part of an overall anti-social engineering campaign.

## Reference

### Citation:

- Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
- Jamil, Abid & Asif, Kashif & Ghulam, Zikra & Nazir, Muhammad & Alam, Syed & Ashraf, Rehan. (2018). MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. 5040-5048. 10.1109/BigData.2018.8622505.
- P. López-Aguilar and A. Solanas, "Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism," 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), 2021, pp. 1363-1368, doi: 10.1109/COMPSAC51774.2021.00192.

URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9529789&isnumber=9529356>