UNICAL ACADEMY

SOCIAL ENGINEERING

UNVEILING THE HUMAN FIREWALL

UNICAL ACADEMY

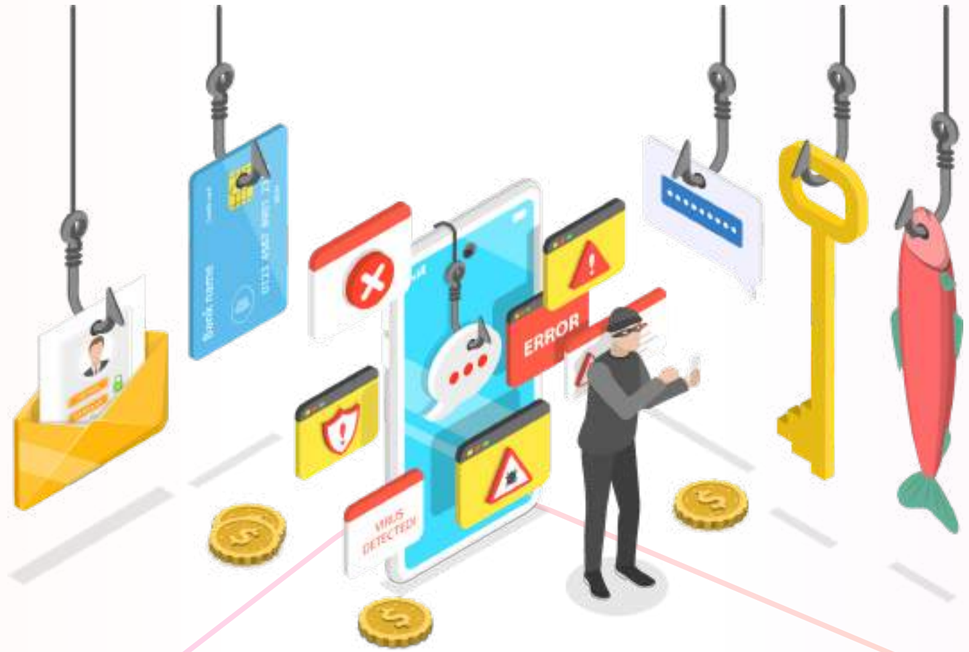
About Social Engineering

Social Engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

Social engineering is a range of malicious activities undertaken by cybercriminals through human interactions. This article explains what social engineering is, along with its types, attack techniques, and prevention trends in 2020.

UNICAL ACADEMY

Social engineering is defined as a range of malicious activities undertaken by cybercriminals intended to psychologically manipulate someone into giving out sensitive information and data. The users are tricked into giving away sensitive data or making security faults by using psychological manipulation techniques. In simpler terms, social engineering relies on human error rather than vulnerabilities in network systems, software, and operating systems. Mistakes committed by legitimate users are less predictable, making them harder to identify. This article gives a comprehensive understanding of social engineering, its types, attack techniques, and prevention best practices.



UNICAL ACADEMY

Table of Contents

UNICAL ACADEMY

What Is Social Engineering?

Social engineering is a range of malicious activities undertaken by cybercriminals intended to psychologically manipulate someone into giving out sensitive information and data.

Under social engineering, a perpetrator initially investigates and examines the victim. Here, the victim's basic background information is gathered, wherein the information may include potentially vulnerable entry points and security protocols required to carry out the attack.

The attacker then tries to perform subsequent actions that hamper the victim's security practices by gaining their trust. Once the victim trusts the attacker, they may reveal sensitive information or grant access to critical and secure resources.

UNICAL ACADEMY

According to a 2020 report by Pulplesec, about 98% of all cyber attacks in the US used social engineering as the key tactic to break through security measures.

Social engineering specifically relies on human error rather than vulnerabilities in network systems, software, and operating systems. Mistakes committed by legitimate users are less predictable, so identifying them is harder than detecting malware-based intrusion.

UNICAL ACADEMY

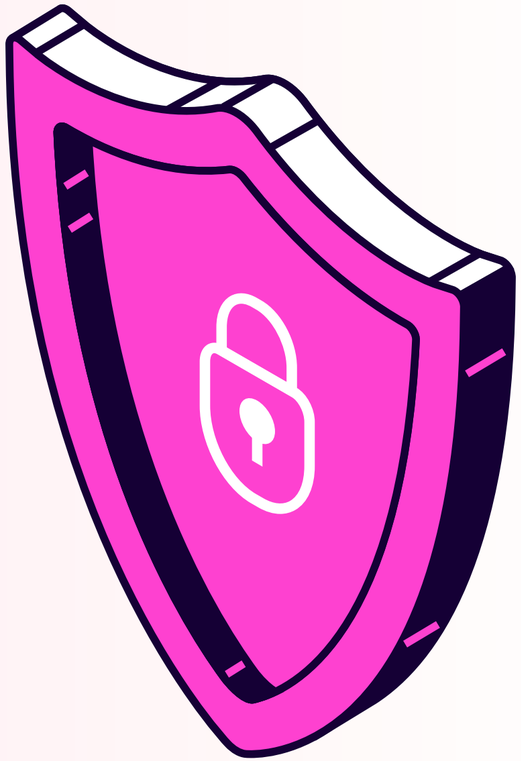
In general, social engineering attacks primarily have two main objectives:

- Cause harm or inconvenience by disrupting business or corrupting data. The act of intentionally trying to stop someone from achieving something or to stop something from developing.

- Gain access to valuables, such as sensitive and critical information or money.

UNICAL ACADEMY

How does social engineering work?



Social engineering attacks generally occur when there is well-established communication between attackers and victims. The attacker prompts and motivates the user into compromising sensitive information, rather than explicitly employing a brute force attack for breaching the user's data.

The social engineering attack life cycle provides criminals a reliable process that can easily deceive the victim.

UNICAL ACADEMY

Social Engineering Lifecycle

The steps involved in the social engineering life cycle include:

01.

Target research: Preparation for an attack requires pre-planning from the perpetrator. Research time is invested in identifying the target's name, personal details, and background information. Based on this information, the attack methods/ channels are selected:

UNICAL ACADEMY

Social Engineering Lifecycle

02.

Target hook: In this step, the attacker engages the target victim with a fabricated story that would be convincing, based on the information collected in the first step. The goal of the attacker here is to win the confidence of the victim.

03.

The attack: Once the target has obtained the necessary trust, the goal now shifts to extracting the information which is the real goal. Based on the intention, the attacker then uses the information or sells it.

04.

Once the attack's objective is complete, the window of engagement is then closed by the attacker, typically with the goal of avoiding any detection or suspicion. The attacker then attempts to cover their tracks and disappear to the best of their ability.

A common example of social engineering attempts made on senior citizens who may not have the required knowledge to identify digital foul play. An attack may be carried out using a combination of phone and email phishing techniques and convince the victim of passing out sensitive bank/ social security login details.