UNICAL ACADEMY

1.1 WHAT IS SOCIAL ENGINEERING?

What is 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.

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.

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.

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.

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.