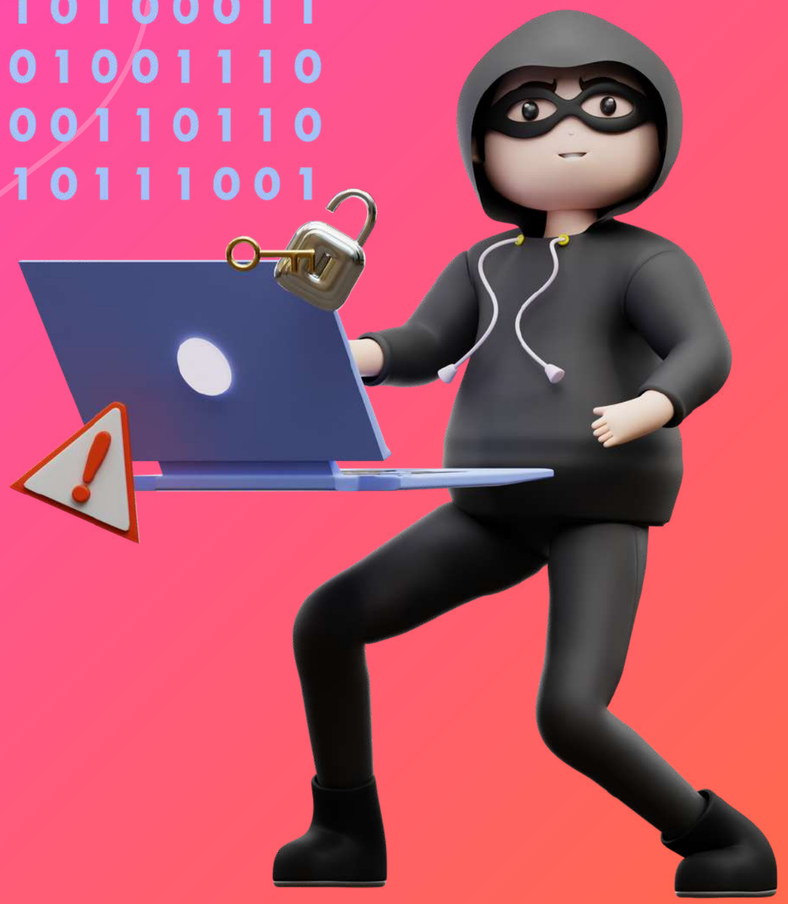
UNICAL ACADEMY

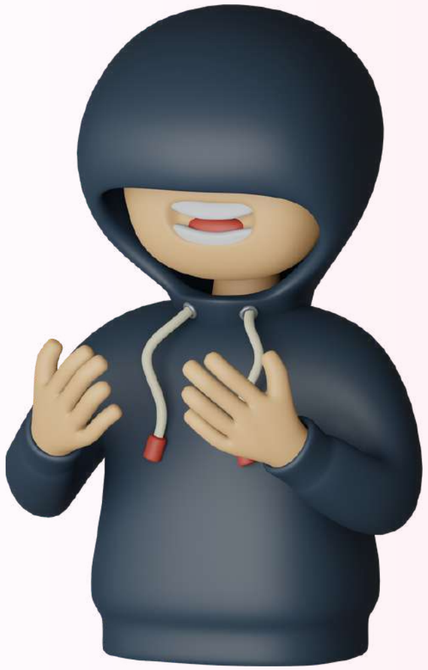


2.1 TYPES OF SOCIAL ENGINEERING

Common characteristics of social engineering attacks

Social engineering attacks pivot around the attacker's use of psychological tricks, such as persuasion or confidence. When the user is exposed to these tactics, they are more likely to take action than stay silent.

In most attacks, attackers mislead users by using an array of psychological manipulation techniques enlisted below:



UNICAL ACADEMY

01.

Emotional Manipulation:

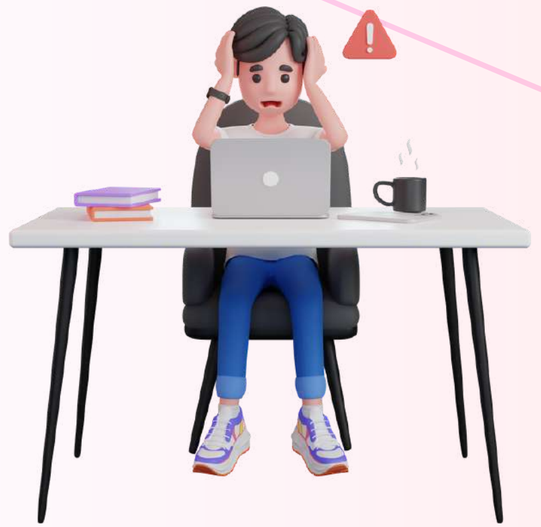
Emotional manipulation by exploiting heightened emotions gives attackers the upper hand in any kind of interaction with the victims. In such cases, when the victims are in an enhanced emotional state, they are more prone to taking irrational or risky actions. Emotions, such as anger, curiosity, excitement, fear, guilt, and sadness are often used in equal measure to convince the target victims.

UNICAL ACADEMY

02.

Immediate Action:

Attackers tend to use time-sensitive opportunities or requests to fool users. The users may be motivated to compromise sensitive information or critical resources under the disguise of a serious problem that needs immediate action.

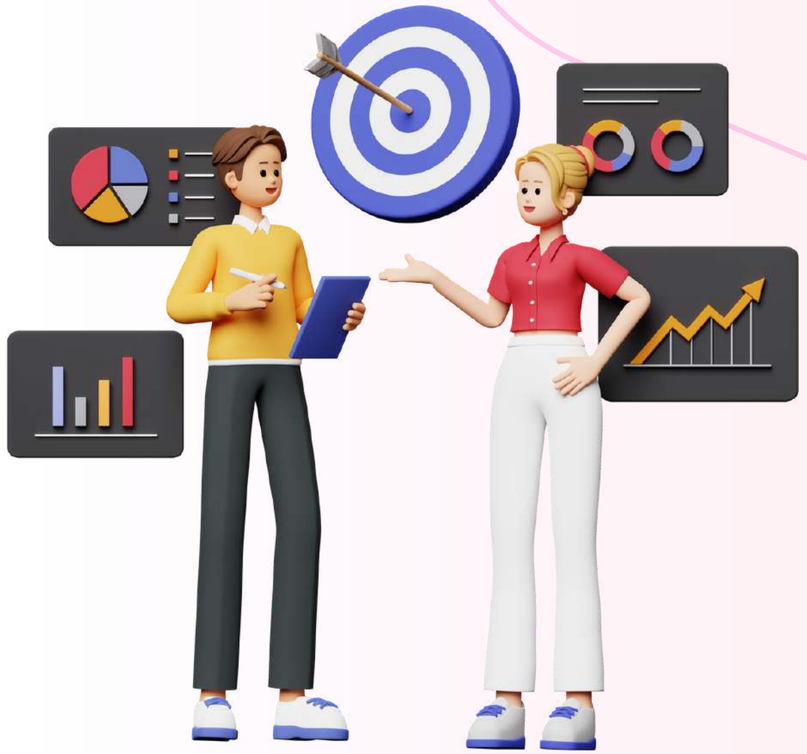


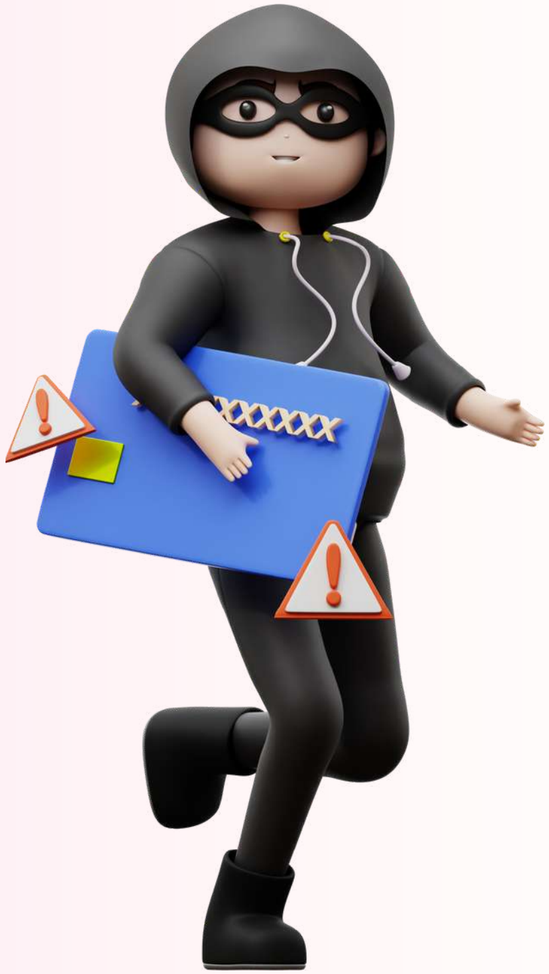
In some scenarios, users may be exposed to a form of a reward or prize that may disappear if they do not act immediately. Both these approaches tend to override the critical thinking or logical reasoning ability of the victim.

03.

Trust:

Social engineering attacks thrive on believability. Confidence and faith play a crucial role in these types of attacks as the attacker is aware of the fact that he is lying to the user. Attackers conduct substantial research on the target victim to cast a defined narrative that won't arouse suspicion.





04.

Simplistic methods:

Some exceptions to these common traits include simplistic methods that attackers use to gain network or system access. For example, a hacker at the common food court of a large organization building may “shoulder surf” users working on their tablets or laptops and try to access their sensitive information without sending an email or writing a line of virus code.