UNICAL ACADEMY

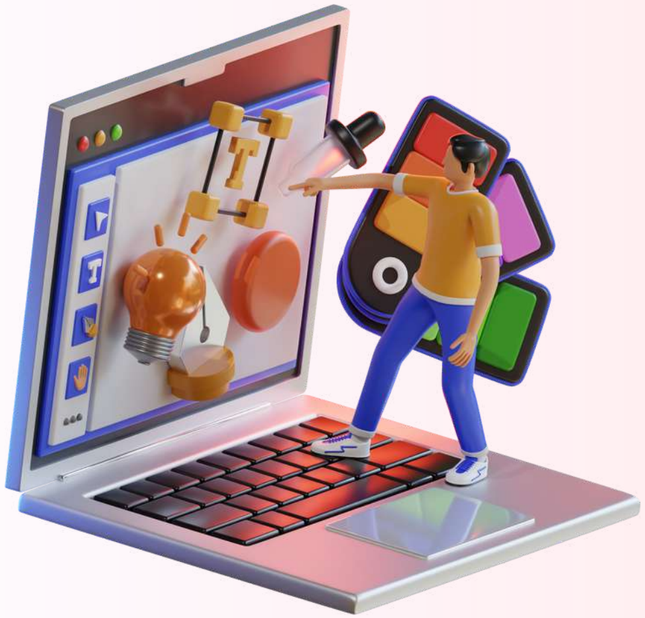
3.1 SOCIAL ENGINEERING ATTACKS CAN BE CLASSIFIED INTO THREE MAIN CATEGORIES

UNICAL ACADEMY

Social engineering attacks can be classified into three main categories:

01.

Technology-based attacks: A technology-based approach tricks a user into believing that he is interacting with a ‘real’ computer system and convinces him to provide confidential information. For example, the user will get a popup window informing him that the computer application has had a problem and needs immediate fixing.



It will tell the user to reauthenticate a computer application to proceed. As the user proceeds to reauthenticate, the user provides his ID and password on the popup window itself. Once they enter the necessary credentials for authentication, the harm is done.

The hacker or the criminal who created the popup window now has access to the user's ID and password and can, therefore, access their network and computer system.

02.

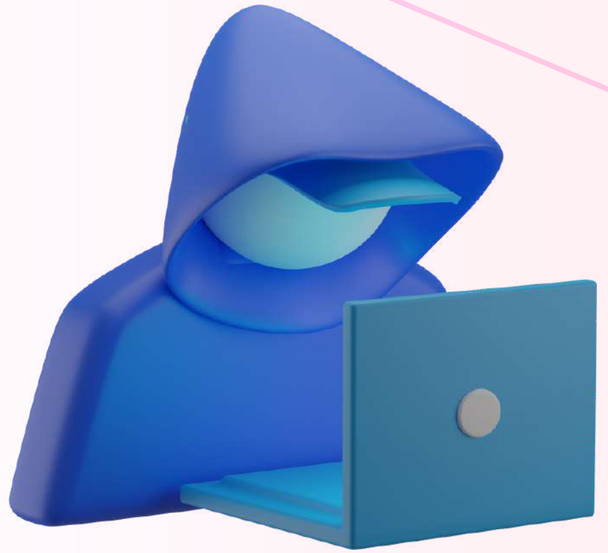
Human interaction-based attacks:

In a human interaction-based approach, the victim's unawareness is exploited to attack the system or network. This is typically accomplished whereby the attacker pretends to be a person or authority the victim already knows while hiding their true identity.

03.

Hybrid attacks:

IHybrid attacks are the most common form of cyberattacks, where the attacker uses both technology and human interactions as platforms for conducting the social engineering attack.



For Example:

In a call to the helpdesk, a corporate social engineering attacker pretends to be a person of very high clearance/ authority within an organization and says that he/she has forgotten the password and needs to reset it immediately. In response, a nervous help desk personnel resets the password and give the newly set password to the person waiting at the other end of the call, rather than sending it via email. Having access to an email, the attacker now proceeds to send fake emails to other employees to coerce them into giving out further sensitive information.

In the above example, the attacker gained control of a technology portal (email), using a human interaction-based social engineering technique, then using the tech-based platform to conduct more social engineering attacks – all part of the same attack.