UNICAL ACADEMY


# 1.3 SOCIAL ENGINEERING LIFECYCLE

# 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:

## 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.

**Exit:** 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.