UNICAL ACADEMY

3.2 KEY TECHNIQUES OF SOCIAL ENGINEERING ATTACKS

UNICAL ACADEMY

Key Techniques of Social Engineering Attacks:

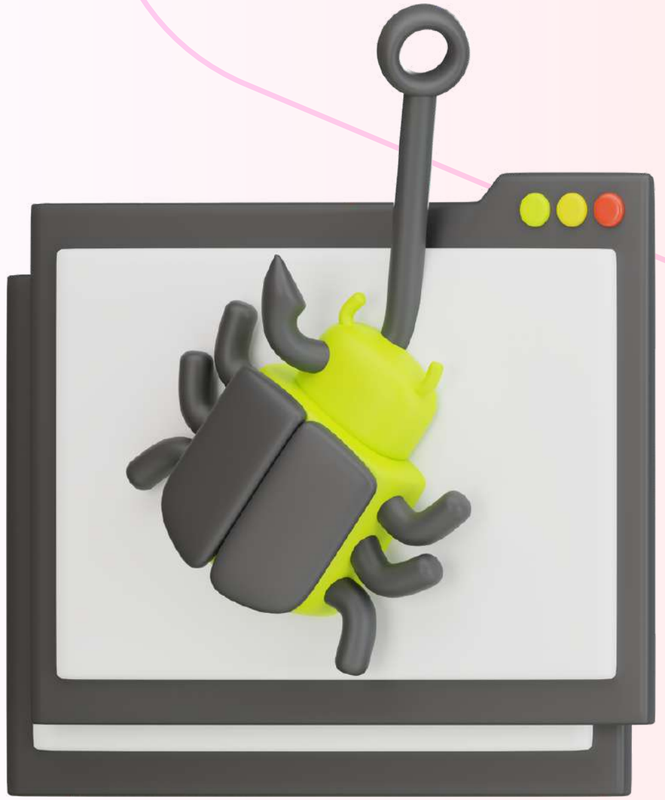
Social engineering assaults employ various techniques to gain access to the victim's sensitive data or network. These attacks come in various forms and can be carried out from any place where human interaction is involved. Let's take a look at them.

01.

Baiting (Hybrid attack):

As the name suggests, baiting attacks harness a false promise to disorient a victim's greed or hunger. They trap users to steal their personal information or infect their systems with malware.

The most common type of baiting involves the usage of physical media to disperse malware. For example, criminals leave the bait – typically malware-infected flash drives – in areas where there is a high probability of the potential victims seeing them. These areas include parking areas, elevators, washrooms, etc. The bait has a specific face value that can trick the victim into believing its authenticity. The external look of the bait can have a label that discloses an organization's payroll list.



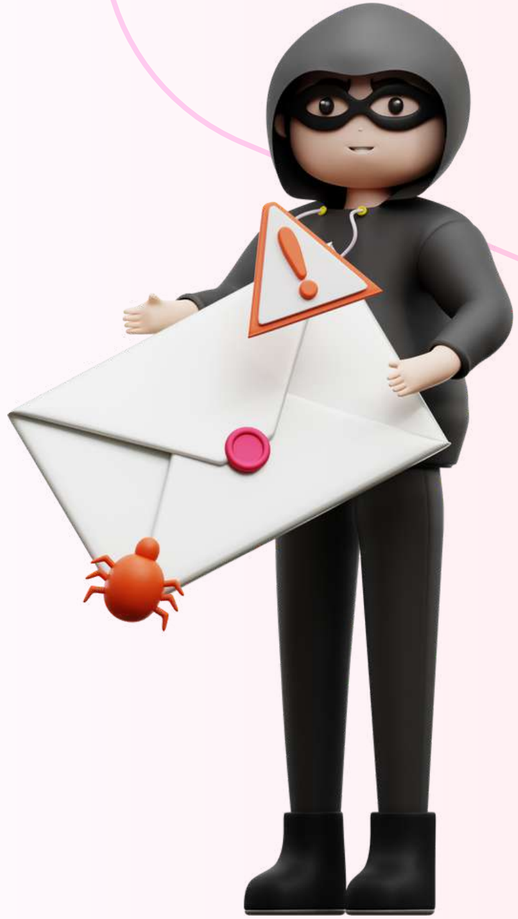
Potential victims are generally convinced by the face value of the bait and, in turn, may insert it into a work or home computer system. This results in direct infection of the victim's computer as the malware gets installed on the victim's device dynamically.

Baiting can be carried out in the physical as well as the online world, where online baiting consists of providing enticing ads that redirect users to malicious sites or motivate users to download a malware-infected computer application.

UNICAL ACADEMY

02.

Contact spamming and email hacking (Hybrid attack):
In this type of attack, attackers hack into an individual's email or social media account to gain access to their personal contacts. Once hacked, the contacts are told that the individual has lost all credit cards. These contacts are then misled into transferring money to the attacker's account. In another use case, a 'must-see video' is forwarded to the victim's contacts, which is linked to malware or a keylogging Trojan.



03.

DNS spoofing and cache poisoning attacks (Tech-based attack):

DNS spoofing manipulates a user's browser and web servers to redirect the user to malicious websites when a legitimate URL is entered. Once infected with this attack exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.

DNS cache poisoning attacks categorically infect a user's device with routing instructions to acquire multiple legitimate URLs to access fraudulent or malicious websites.

04.

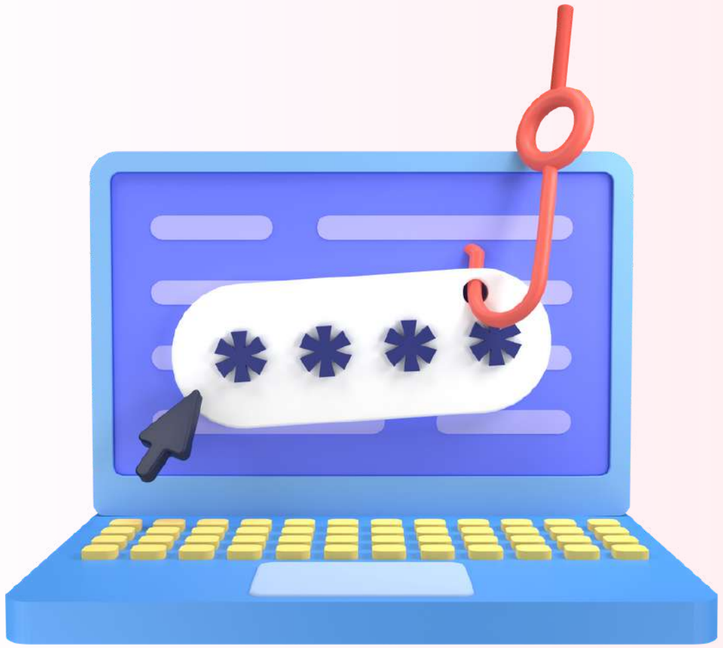
Phishing (Tech-based attack):

Phishing is one of the most popular social engineering attack types. Phishing scams employ email and text message campaigns to create a sense of urgency, curiosity, or fear in victims. They trick victims into disclosing sensitive information, clicking on malicious links, or opening attachments containing malware.

For example, attackers send an email informing the user of an online service that alerts them of a policy violation. The alert may ask the user to take immediate action, such as a password change.

This may include a link to an illegitimate website that is identical to its legitimate version. It may prompt the user to enter the correct credentials and a new password. Upon submission of the form, the information entered by the user is sent to the attacker.

In this type of attack, identical or near-identical messages are sent to all users through phishing campaigns. Hence, detecting and blocking such attacks are easier for mail servers having access to threat sharing platforms that are seemingly integrated within their framework.



05.

Physical Breach Attacks (Hybrid attack):

Physical breaches involve attackers that appear in-person, identifying themselves as legitimate users to typically gain access to technical devices that are hard to breach.

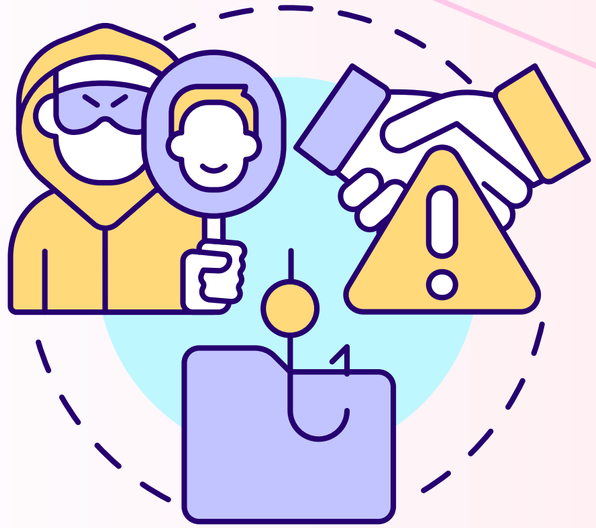
Such attacks are commonly observed in organizational environments, such as government offices, businesses, or other enterprises. Attackers may pretend to be a representative of a known, trusted vendor for the company. In some cases, the attackers may even be recently fired employees who are holding a grudge against their former employer.

The attackers have a dubious identity but believable enough to avoid questions that can catch them in a spot of bother. Therefore, the attackers need to research at their end to avoid high-risk situations. So, if an attacker attempts a physical breach attack, they are guaranteed to have a highly valuable reward if successful.

06.

Pretexting (Hybrid attack):

In a pretexting attack, the cybercriminal obtains sensitive information by using a series of lies. The scam is generally initiated by an attacker who misleads the victim into believing that they need sensitive information to perform a critical task.



The attacker initially establishes trust with the victim by impersonating co-workers, police personnel, bank and tax officials, or other individuals who have right-to-know authority. The pretexter then asks questions to confirm the victim's identity. In this way, the pretexter gathers important personal data of the victim.

All kinds of sensitive information and data records are gathered using the pretexting attack. The sensitive information may include social security numbers, personal addresses, and phone numbers, phone records, bank records, etc.

07.

Scareware (Hybrid attack):

In this type of attack, victims are bombarded with false alarms and fictitious threats. Users are tricked into thinking that their computer system is infected with malware, prompting them to install software that has no technical capability at all or, in some cases, the software is malware itself. Scareware is, therefore, referred to as deception software, rogue scanner software, and fraudware sometimes.

One example of scareware is a legitimate-looking popup displayed on the victim's browser while surfing the web. The text on the popup may read "Your computer may be infected with harmful spyware programs". The popup offers the victim two options — either to install the disclosed malicious tool (malware-infected) or to get redirected to a malicious site by clicking the pop-up window, thereby infecting the victim's computer.

Scareware is sometimes distributed via spam email that may highlight illegitimate warnings or offer users to buy worthless and harmful online services.

08.

Spear phishing (Tech-based attack):

Spear phishing is a targeted version of the phishing scam. In this type of attack, an attacker identifies and chooses specific individuals or organizations. Once the target victim is identified, the scam then tailors messages based on the victim's characteristics, designation, and contacts to make their attack less conspicuous.

Spear phishing attacks are harder to detect and have better success rates. They may involve an attacker who impersonates an organization's consultant and sends an email to one or more staff members.

The mail is worded and signed exactly as the consultant usually does, thereby deceiving its recipients into believing that it's an authentic message. The message is convincing enough to prompt recipients into changing their passwords. In some cases, the message provides a link that redirects the recipients to a malicious page where the attacker captures their credentials with ease.

09.

Vishing and Smishing (Hybrid attack):

Vishing and smishing are variants of phishing social engineering attacks, wherein one of the examples includes ‘voice fishing’, which means simply calling up and asking for data. In some cases, the attacker may act as a co-worker, for instance, impersonating an IT helpdesk personnel and asking for login information. Smishing attack uses text SMS to obtain sensitive information.

10.

Watering Hole Attack (Tech-based attack):

Watering hole attacks infect popular websites with malware to target multiple users at the same time. In such attacks, the attackers perform a careful analysis to identify weaknesses in specific websites. They look for prominent vulnerabilities that are currently existing, not generally known, and patched. Such weaknesses are termed as zero-day exploits.

In some cases, the attackers may note that a site has not updated its framework to patch out known vulnerable issues and, in turn, infect it with malware. Website owners generally choose to delay software updates to keep software versions stable. They switch once the newer version has a proven track record of system stability. Attackers exploit this behavior to target recently patched vulnerabilities.