**Social engineering** is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization’s sensitive information by using social engineering, which targets the weakness of people.

**Behaviors Vulnerable to Attacks:**

* Authority
* Intimidation
* Consensus or Social Proof
* Scarcity
* Urgency
* Familiarity or Liking
* Trust
* Greed

**Factors that make companies vulnerable to attack**

* Insufficient Security Training
* Several Organizational units
* Lack of Security Policies

**Phases of a Social Engineering Attack**

* Research the target company
* Select a target
* Develop relationship
* Exploit the relationship

**Human-based Social Engineering**

Human-based social engineering involves human interaction.

* **Impersonation** is a common human-based social engineering technique where an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use a phone or another communication medium to mislead their target and trick them into revealing information.
* **Vishing** (voice or VoIP phishing) is an impersonation technique in which the attacker uses Voice over IP (VoIP) technology to trick individuals into revealing their critical financial and personal information and uses the information for financial gain. The attacker uses caller ID spoofing to forge identification.
* **Eavesdropping** refers to an unauthorized person listening to a conversation or reading others’ messages. It includes the interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging.
* **Shoulder surfing** is the technique of looking over someone’s shoulder as they key information into a device.
* **Dumpster diving** is the process of retrieving sensitive personal or organizational information by searching through trash bins.
* **Reverse social engineering:** a perpetrator assumes the role of a knowledgeable professional so that the organization’s employees ask them for information. The attacker usually manipulates questions to draw out the required information.

A good example of a reverse social engineering virus is the “**My Party**” worm. This virus does not rely on sensational subject lines but rather makes use of inoffensive and realistic names for its attachments. By using realistic words, the attacker gains the user’s trust, confirms the user’s ignorance, and completes the task of information gathering.

* **Piggybacking** usually implies entry into a building or security area with the consent of the authorized person.
* **Tailgating** implies accessing a building or secured area without the consent of the authorizedperson. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them.
* **Diversion theft** is a technique where attackers target delivery professionals or transport companies. This technique is also known as “Round the Corner Game” or “Cornet Game.” The main objective of this technique is to trick a person responsible for making a genuine delivery into delivering the consignment to the wrong location, thus interrupting the transaction.
* **The honey trap** is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company.
* **Baiting** is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users.
* **Quid pro quo** is a Latin phrase that meaning “something for something.” In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials.
* **Elicitation** is the technique of extracting specific information from the victim by involving them in normal and disarming conversations.

**Computer-based Social Engineering**Computer-based social engineering relies on computers and Internet systems to carry out the targeted action.

* **Pop-up window:** The common method of enticing a user to click a button in a pop-up window is by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services.
* **hoax** is a message warning its recipients of a non-existent computer virus threat. It relies on social engineering to spread its reach. Usually, hoaxes do not cause any physical damage or loss of information; but they cause a loss of productivity and use an organization’s valuable network resources.
* **Chain letter** is a message offering free gifts, such as money and software, on the condition that the user forwards the email to a predetermined number of recipients.
* Instant Chat message: An attacker chats with selected online users via instant chat messengers and tries to gather their personal information such as date of birth or maiden name.
* **Spam** is irrelevant, unwanted, and unsolicited emails designed to collect financial information such as social security numbers, and network information. Attackers send spam messages to the target to collect sensitive information, such as bank details.
* **Scareware** is a type of malware that tricks computer users into visiting malware-infested websites or downloading or buying potentially malicious software. Scareware is often seen in pop-ups that tell the target user that their machine has been infected with malware.

**Phishing**

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user’s personal or account information.

The target receives an email that appears to be from the bank and requests the user to click on the URL or the link provided. If the user is tricked and provides their username, password, and other information, then the site forwards the information to the attacker, who will use it for nefarious purposes.

**Types of Phishing**

* **Spear phishing** messages seem to come from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. In reality, the message is sent by an attacker attempting to obtain critical information. Spear phishing generates a higher response rate compared to a normal phishing attack
* **whaling attack** is a type of phishing that targets high profile executives like CEO, CFO,politicians, and celebrities who have complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim into revealing critical corporate and personal information, generally, through email or website spoofing. Utmost care is taken ate every stage of attacking.
* **Pharming** is a social engineering technique in which the attacker executes malicious programs on a victim’s computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim’s traffic to an attacker-controlled website. This attack is also known as “Phishing without a Lure.” Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification. Pharming attacks can also be performed using malware like Trojan horses or worms.
* **SPIM (Spam over Instant Messaging)** exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called Spimmer. Spimmers generally make use of bots to harvest Instant Message IDs and forward spam messages to them.

**Mobile-based Social Engineering**Attackers use mobile applications to carry out mobile-based social engineering.

* **Publishing Malicious Apps:** The attacker first creates the malicious application and publishes it on major application stores using the popular names. Unaware of the malicious application, a user will download it onto their mobile device, believing it to be genuine. Once the application is installed, the device is infected by malware that sends the user’s credentials.
* **Repacking Legitimate Apps:** A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user’s mobile device collects the user’s information and sends it to the attacker.
* **Fake Security Applications:** the attacker first infects the victim’s computer by sending something malicious. They then upload a malicious application to an app store. When the victim logs on to their bank account, malware in the system displays a pop-up message telling the victim that they need to download an application on their phone to receive a message from security. The victim downloads the application from the attacker’s app store, believing they are downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information.
* **SMiShing (SMS Phishing)** the SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

**🡺 Insider Threats**

An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization’s information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. Insider attacks may cause great loss to the company.

**Types of Insider Threats**

* **Malicious insider** threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.
* **Negligent Insider:** Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks.
* **Professional insiders** are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company’s network and sell the organization’s confidential information to competitors or black-market bidders.
* **Compromised Insider:** An outsider compromises an insider who has access to the critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.

**Social Engineering through Impersonation on Social Networking Sites**

Social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as name, address, mobile number, date of birth, project details, job designation, company name, and location.

**There are two ways an attacker can perform impersonation on social networking sites:**

* By creating a fictitious profile of the victim on the social media site
* By stealing the victim’s password or indirectly gaining access to the victim’s social media account.

Attackers create a fake account and scan the details on the profile pages of various targets on social networking sites such as LinkedIn and Twitter to engage in spear phishing, impersonation, and identity theft.

**🡺 Identity Theft**

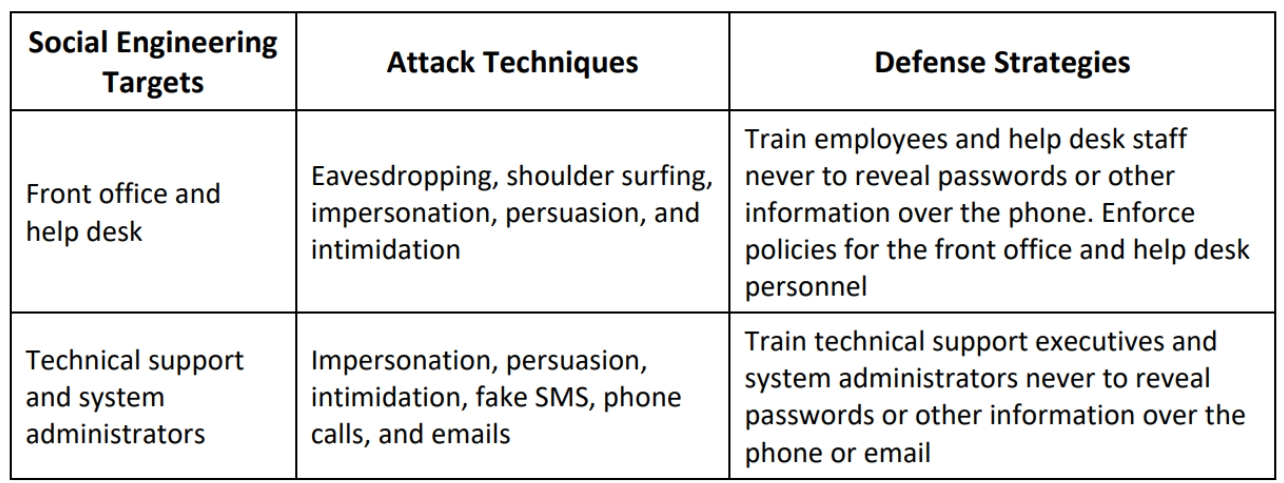
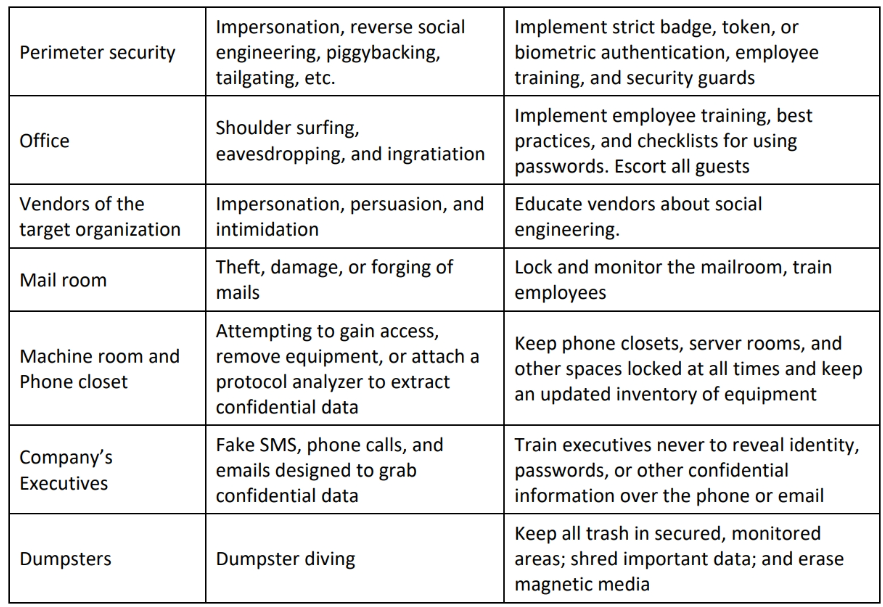
The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone’s identification. Identity theft occurs when someone steals others’ personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts.

Types of Identity Theft

* **Child Identity Theft:** This type of identity theft occurs when the identity of a minor is stolen.
* **Criminal Identity Theft:** A criminal uses someone’s identity to escape criminal charges.
* **Financial Identity Theft:** This type of identity theft occurs when a victim’s bank account or credit card information is stolen and illegally used by a thief.
* **Driver License’s Identity Theft:** A person can lose their driver’s license, or it can easily be stolen.
* **Insurance Identity Theft:** It takes place when a perpetrator unlawfully takes the victim’s medical information to access their insurance for medical treatment.
* **Medical Identity Theft:** This is the most dangerous type of identity theft where the perpetrator uses the victim’s name or information without the victim’s consent or knowledge to obtain medical products and claim health insurance or healthcare services.
* **Tax Identity Theft:** This type of identity theft occurs when the perpetrator steals the victim’s Social Security Number to file fraudulent tax returns and obtain fraudulent tax refunds.
* **Identity Cloning & Concealment:** This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply in order to hide their identity.
* **Synthetic Identity Theft:** This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity.
* **Social Security Theft:** This is another common type of identity theft where the perpetrator steals victim’s Social Security Number in order to derive various benefits such as selling it to an undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or applying for and obtaining a new passport.
* **Detecting Insider ThreatsInsider Risk Controls:** Insider data risk presents another layer of complexity for security professionals. It requires designing security infrastructure in such a way that user permissions, access controls, and user actions are monitored efficiently.
* **Deterrence Controls:** The deterrence controls that the security professionals must have in place to deter insider threats are DLP (Data Loss Prevention) tools, and Identity and Access Management (IAM) tools.
* **Detection Controls:** The detection controls that the security professionals must have in place to detect insider threats are IDS/IPS, log management systems, and Security Information and Event Management (SIEM) tools.

**How to Detect Phishing Emails?**

To detect phishing emails, first, hover your mouse pointer over the name in the “From” column. Doing so will show whether the original domain name is linked to the sender’s name; if it is not, then it could be a phishing email. For example, an email from Gmail.com should probably display it’s “From” domain as “gmail.com.”

Check to see if the email provides a URL and prompts the user to click on it. If so, ensure that the link is legitimate by hovering the mouse pointer over it (to display the link’s URL) and ensure it uses encryption (https://). To be on the safe side, always open a new window and visit the site by typing it in directly instead of clicking on the link provided in the email.