Let's look at each one of them in detail.

Elicitation

Using elicitation, the attacker extracts the information from the victim without asking direct questions. Rather, the attacker asks open-ended questions and then keeps narrowing them to the point that the victim reveals the information. In this process, the victim does not realize that he or she is revealing valuable information to the attacker.

Interrogates

The attacker interrogates the victim to extract valuable information. The attacker can ask open-ended questions. The idea is to learn the information from the victim. However, the attacker needs to be conscious of asking too many questions, which can create a doubt in the victim's mind.

The attacker, other than asking questions, can also observe the victim. For example, the attacker may pay attention to the following:

- Body language
- Body gestures - the movement of hands and feet
- Way of talking
- Facial expressions

Pretexting

Pretexting, or impersonation, Is a practice of obtaining personal information by pretending to be someone else. Using pretexting, the attacker hides the real identity of himself or herself. The attacker lies about the purpose for which information is required. The purpose of the conversation is fabricated, pretexted to gain personal information.

Pretexting can be performed through various methods, such as

- Telephone
- E-mail
- Instant messaging
- Website

Pretexting can be targeted to anyone. It is most often used by:

- Corporate spies
- Private investigators
- Law enforcement agents

Know the Motivation Techniques

An attacker, when using social engineering, has to use a method or technique to obtain the desired information. There are various techniques that can be used by the attacker. Some of the commonly used techniques are:

- **Authority**: The attacker shows authority by pretending to be from law enforcement or something similar. The attacker displays confidence in pretending to be someone with authority and pressurizes the victim to provide information. For example, the attacker may call the reception and tell the receptionist that he is calling from the police department and needs certain information.
- **Scarcity and urgency**: With this technique, a sense of urgency is created, which forces the victim to make a quick decision without thinking much. For example, the attacker may call a user to share the password to be reset immediately, or his account will be terminated.
- **Social proof**: Social proof is mostly used when the victim is in a situation that he or she does not know how to deal with. The victim makes a decision by observing others. The attacker can apply this technique on more than one way by displaying an act that convinces them that this is the correct behavior.
- **Fear**: The attacker use fears to make the victim do what they want them to do. The attacker creates a situation in which the victim is forced to act quickly to avoid a dangerous outcome.

Know Phishing and Its Types

Phishing is a social engineering attack that uses technical deception to convince a user to provide personal information, such as passwords, social security numbers, credit card numbers, bank account details, and so on. In the phishing attack, the attacker creates a replica Website or Webpage that tricks the user into providing personal information. The Website or Webpages are real lookalikes of the original Website or Webpages that the user gets tricked. The URLs are close to the original, which most of the time, users don't bother to check. One of the key intent of using phishing is for financial advantage.

There are three key methods that can be used in phishing:

- **Mass mailing:** A large number of audiences are targeted. It is quite likely that some of the audiences are going to fall for this method. This method is usually performed using SPAM.
- **Instant messaging:** In the last few years, instant messaging is one of the key media in phishing. Malicious URLs are sent with attractive messages to lure users in clicking them
- **Malicious Websites:** Phishing can also be initiated through malicious Websites.

Phishing is a four-stage process. These stages are as follows:

- **Initiation** - The attacker prepares for an attack.
- **Execution** - The attacker sends out the mass mail or instant message to hundreds or thousands of users.
- **User Action** - User performs two tasks - first, clicks on the URL and then enters the personal information on the Webpage that is loaded.
- **Completion** - The information that is entered by the user is received by the attacker and saved at his end. It is now up to the attacker to use this information.

By the end of the fourth stage, the phishing attack is successfully completed. In a phishing attack, the attacker can use various attack methods. Some of these attack methods are:

- Man-In-The-Middle
- Session hijacking
- Phishing through search engines
- Link Manipulation
- URL Obfuscation Attacks
- Client-side vulnerabilities
- Cross-site scripting
- Malware / Keyloggers / Screen loggers / Trojans
- E-mails (Deceptive Phishing)
- Hosts file poisoning
- DNS-based Phishing
- Content-Injection

Reasons for Successful Phishing Attacks

There are various reasons for a phishing attack to become successful. Some of the common reasons are as follows:

- **Lack of knowledge**: Users are not trained enough or are completely unaware of the dangers of the phishing attacks. Attackers use this method on several hundred and thousands of users at once, and several users fall prey to the attack.
- **Visual deception**: Attackers very smartly use a similar URL or domain names with the exact replica of the Website. Users are deceived with the replica of the Website and without realizing enter their user credentials, which are then captured by the attacker and used on the real Website.
- **Visual Indicators**: Users mostly do not pay attention to the URL or the domain name and, therefore, end up being a victim of the phishing attack.

Types of Phishing Attacks

Even though there are several types of phishing attacks, the following are the three prominent ones:

Spear Phishing

Spear phishing is focused on specific targets. Like phishing, it does not focus on the mass public. In this form of phishing, the attacker takes time to research the target, who typically are from organizations. The attacker sends out personalized E-mails that typically carries a sense of urgency.

The E-mails are designed to lure the target to click the provided URL. After the URL is clicked, malware is downloaded, or personal and sensitive information is exposed.

Spear phishing is usually used with the pretexting technique. The attacker gathers the information from various Websites, specifically focusing on social networking Websites.

Whaling

Whaling, a phishing attack, targets senior executives or high-profile candidates within an organization. It follows the same process as phishing but targets the high-profile candidates, specifically the CxO candidates.

Pharming

In this type of phishing attack, the user is redirected to a real lookalike Website. When a user types the correct URL in the Web browser, the user is redirected to a real lookalike Website. The user has not done anything wrong, but the attack has still occurred. This is done by DNS cache poisoning. The real IP address mapped to the legitimate URL is changed to an IP address that redirects the user to a malicious Website, which is a real lookalike. The user will not be able to suspect anything here because the URL is correct.

Know Hoax, Baiting, Shoulder Surfing, and Tailgating

The following methods are commonly used in social engineering:

Hoax

A computer hoax happens through the Internet. The hoax attacker uses hook tactics to draw the victim's interest, warns the victim of dire consequences, and requests the victim to send the same message to many recipients.

Shoulder Surfing

Shoulder surfing is a social engineering attack performed by looking over the shoulder of the victim to retrieve credit card number, password, or any other pertinent information. The attacker directly observes the information entered by the victim by standing very close or behind the victim or uses vision enhancing aids or binoculars to observe from far. Shoulder surfing attackers also use the technique of fixing up closed-circuit cameras hidden behind the wall or ceiling to obtain sensitive information.

Baiting

Baiting is an attack that uses CDs, DVDs, or USB drives. It does not use E-mails as the medium but relies on storage devices. Mostly, the USB drives are used in this scenario. The USB drives are loaded with the malware and placed in places where they are easy to find. For example, a user may find a USB drive in the parking lot of his office. When the user uses the USB drive on the company's laptop, the malware is triggered and infects the laptop. Through the laptop, the malware can eventually spread to the network.

Tailgating

Tailgating is a social engineering act of gaining access to an electronically locked system or a restricted area by following a user who has legitimate access, with the intention of accessing vulnerable information. Tailgating is also known as piggybacking.