**What is phishing ?**

Phishing can be known as a cyberattack that uses disguised text messages, email, telephone, and many more as an attack weapon. The objective of phishing is to steal user’s data including login credential, bank pin, or any other things that benefit the attacker. For example, the attacker tried to trick the victims by emailing a message to notify their bank is having a transaction problem which leads to them do believe in the message and click the link to access their bank account like they normally do without noticing that is a fake website. Phishing had become one of the popular attacks for hackers because most victims will think that they are on a legitimate website by looking at the design.

**Types of Phishing:**

1. **Email phishing**

Email phishing is one of the most common types of phishing used by attackers. We are moving into a technology era where we use to send and receive documents, notifications, important messages through email because of its reflexibility. The attacker will grab the chance to send messages to victims through email by notifying them there is a problem or error occurred in your bank, social media account, or any other platform that they used. The attacker might use a similar organization’s email address to lower the alert of the victims. Unexperienced victims will likely click on the link and access the fake domain that mimics the same as the original domain created by the attacker. Most victims will not realize it is a mimicked domain and they will likely key in the login credential where they are giving it to the attacker.

1. **Angler phishing**

Angler phishing is a new type of phishing where it highly used in social media by most attackers. Angler phishing is used to trick the victims and make them fall into the attacker’s trap. Angler phishing attacks are usually performed using fake or duplicate corporate social media accounts. The attacker will use the same profile picture and similar username as the real corporate account to trick the victims. They might use the fake account to announce there are promotions and discounts, those who are interested need to provide their name, email, and phone number to them. The greedy victims might think it’s a good opportunity to get the offer and they will likely provide information to them. The attacker can also inform victims to click on the link to receive the offer where the link opened will download the viruses secretly behind.

1. **Whaling**

Whaling is a common type of phishing where it is used to target high-profile target or senior executives. It usually aimed to steal a huge amount of money or highly sensitive information or data from an organization. Senior executives have more control over the organization’s system where the attacker is trying to trick them to gain access to their computer system and control the system of the organization. For example, Snapchat high-ranking employee was fooled into revealing employee payroll information by an attacker impersonating the CEO.

1. **Smishing and vishing**

Smishing and vishing are similar to email phishing but they use the telephone for communication instead of email. Smishing involves attacker or criminal sending text messages to victims where it is very similar to email phishing. Vishing involves a telephone conversation where the attacker might dial victims using the telephone. For example, the victims are asked to update their account details, change their password. The attacker can act as the staff calling from the card company or the bank to request the victims to provide their information.

1. **“Evil Twin” Wi-Fi**

“Evil Twin“ Wi-Fi is a type of phishing where it is a Wi-Fi attack that works by taking advantage of the Service Set Identifier(SSID) of the wi-fi. The cybercriminal or attacker will provide wi-fi access points as its SSID named as any coffee shops, airports, public parks, or shopping malls to trick victims. Victims will think that it’s a public wi-fi and it is safe to use but the cybercriminal is taking advantage of this to steal the data or information of the victims through data packets. The victims might get viruses installed on their devices once they connected to the “Evil Twin Wi-Fi” provided by the cybercriminal.

1. **Spear phishing**

Spear phishing is known as sophisticated phishing where it had used in one of the most famous data breaches in recent history. Spear phishing is similar to email phishing but the attacker or cybercriminal already has some or all of the information of the victim such as their name, age, place of employment, job title, phone number, email address, and many more. The attacker will send emails to victims that contained victims’ information. It is called spear phishing because the attacker is baiting the victims by providing their information where they will believe a specific organization like a bank or insurance company will have their information only. With the information provided by the cybercriminal, the victims will lower their alert and follow the next instruction given by the cybercriminal such as giving out their bank account’s password or click on the malicious link.

1. **Business Email Compromise (BEC)**

This type of phishing is targeted at key individuals in the finance or accounting department. BEC is involved via a business email compromise scam where the attacker tried to trick victims by impersonating the CEO of the organization. The victims will likely follow what the fake CEO said because they are afraid to lose their job if they do not follow the instruction given by the CEO. For example, the fake CEO is telling the finance or accounting department to transfer money to an unfamiliar bank account where they just follow without confirming that the CEO is real.

1. **Clone Phishing**

Clone phishing is used by the cybercriminal where they have to create a similar or nearly identical replica of a legitimate message which previously delivered, email containing an attachment or link. The cybercriminal might only change the attachment or link and others are identical to the previous message to trick victims by clicking in the link and the viruses will automatically be downloaded into their devices secretly behind. In simple terms, clone phishing is a type of phishing which identical to the previous message with only attachment or link swapped with a malicious one.