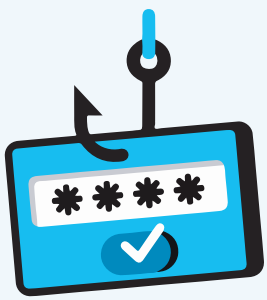
» **Phishing**

Phishing is the most popular type of social engineering activity. It is a fraudulent attempt at acquiring a victim's sensitive information such as passwords, credit card details, etc. by pretending to be a legitimate and trusted company or institution in an electronic message. In most cases, this attack can be launched via email; however, it is also possible to get exposed through chat applications, phone calls, social media or spoofed websites.

Spear phishing is basically the same as phishing, except that it targets a specific victim or organization that is more likely to be tricked into revealing confidential information. The attacker tries to use specific victim's personal information to gain trust and appear as a legitimate user. This information can be gathered from online activities related to the victim, or his social accounts. If the attack succeeds, the attacker will gain the access and victim's sensitive data will be compromised.



» **Spear Phishing**

» **Baiting**

As its name sake, baiting involves luring a victim with something they desire. A good example is an infected flash drive with inscriptions like "Confidential", "My music" or the like. The victim is enticed to take the flash drive and unknowingly install the malware in his own device, thus giving access to the attacker.

Pretexting is, in essence, the practice of creating a plausible enough scenario that makes a victim feel comfortable to reveal confidential information, usually over the phone. Sometimes, impersonation is also involved. The more credible the impersonation or the scenario is, the more willing to provide sensitive information the victim is.

» **Pretexting**