**5 Social Engineering Attacks to Watch Out For**

We all know about cyber criminals who leverage their technical knowledge for malicious purposes and infiltrate into protected systems to extract sensitive information. These types of attackers remain in the news all the time. But there is another breed of malicious cyber attackers who do the same without using advanced tools or highly technical expertise. They use different tactics to access sensitive data. This activity is call social engineering because the criminals exploit the biggest vulnerability in an organization i.e. human psychology.

Social Engineering is a broad term that encompasses a number of malicious activities. Let’s look at five of the most common techniques used by social engineers for targeting their victims.

1. Phishing

Phishing is the most common social engineering attack that happens in the cyber world. Hackers commonly conduct phishing scams by sending emails that lure the reader into giving out their personal information or clicking a link. For instance, an email that impersonates your bank manager and asks you to urgently send your credit card detail. Or an email telling you that you have won a lottery ticket and need to click on a particular link to claim your money.

In general, a phishing scam intends to accomplish three things:

* Get personal information like name, address, financial details and social security numbers of targets
* Use misleading or shortened links, called phishing links, to redirect users to phishing landing pages
* Create a sense of urgency for the user to make them respond quickly to the demand of phishing email.

1. Pretexting

This is another form of social engineering where an attacker focuses on making a fabricated scenario or a pretext. A scammer usually ask the target to give certain information to confirm their identity. In reality, it actually leads an attacker to conduct identity theft or stage a secondary attack. Whereas a phishing attack misuses urgency and fear to its advantage, pretexting relies on creating a false sense of trust with the target.

1. Baiting

It is similar to phishing attacks in many ways. However, what distinguishes it from other types of social engineering is that it promises the victim a good or service that they will get. A baiter may offer free movie or music download for instance, to trick a user into handing over login detail.

1. Quid Pro Quo

It is similar to baiting, but instead of an item or good, the attacker promises a benefit or service in exchange of information.

1. Tailgating

This social engineering attack is also called piggybacking. In this attack, an unauthorized person physically enters a restricted area by following an authenticated employee by impersonating as a delivery man or someone relevant. Once the employee enters, the impersonator gets access to the building and can subsequently access confidential information.

It’s important for organizations to train their employees on how to identify social engineering attempts and act vigilant in times of potential security threats.