CYBERSECURITY

Information Sheet
Social Engineering

Tags: Cybersecurity, Attack Vectors, Threats, Phishing

365 ARCHITECHS

Malicious attacks accomplished through human interactions are known as social engineering. They use psychological manipulation to trick people into giving away confidential information or taking actions that may not be in their best interests.

This information sheet considers the different types of social engineering attacks that threat actors use to gain access to systems to steal information, harm reputations or disrupt operations.

This attack vector can be very difficult to defend against due to the unpredictable nature of human interactions.

Phishing

Phishing attacks are still the most common and successful method used to gain initial access to an organisation[1]. There are several types of phishing attacks, including:

Phishing	*Spear Phishing*	*Whaling*	*Vishing & SMiShing*

See Information Sheet: Phishing Attacks.

Pretexting

Pretexting involves a threat actor presenting themselves as someone else by inventing a scenario. It typically involves the threat actor playing a role in a plausible situation, for example, pretending to be a bank officer calling about authorised use of a credit card.

Waterholing

Waterholing relies on users trusting the websites that they often frequent. Threat actors prepare traps at favoured waterholes waiting for unwary prey to let down their guard and trick individuals into clicking on links, accessing infected pages or providing confidential information that they wouldn't normally do.

Baiting

Baiting is the modern-day equivalent of a trojan horse that relies on the curiosity or greed of the individual. Threat actors leave USB sticks or other removable media in locations where they will be found, with the knowledge that someone is likely to try to access the information.

Once inserted into a device, the removable media can inject malware, infecting hosts and networks.

Quid Pro Quo

Quid Pro Quo means a favour for a favour. In this type of cyber-attack, a threat actor provides something of perceived value in return for providing information, such as a password.

A common example is where a call is received from a purported IT helpdesk operator, advising that there is a problem with the user's computer. The user is requested to divulge their password in order for the "helpdesk operator" to solve the problem.

Tailgaiting

Tailgaiting occurs when a user grants access to a threat actor who appears to be legitimate. Examples include holding a door open for someone who pretends to have lost their key or allowing someone to use their device temporarily.

[1] Fireeye Mandiant Services M-Trends 2020 Report