TOP 5 TYPES OF SOCIAL ENGINEERING

1 PHISHING

Medium:

- links in emails
- links on social media
- links in instant messages or texts

Tactics:

- impersonate popular, trusted brands (ex. Amazon)
- use link shorteners, create URLs that emulate real ones or embed redirection links in URLs that look real
- instill a sense of urgency by using fear, threats or excitement to get the victim to act right away.

Goal

Most commonly, to trick victims into providing sensitive information by convincing them they're currently on or going to a trusted site. Or get the victim to visit a malicious URL in order to infect their computer with malware..

2 WATERING HOLE

Medium:

- public websites

Tactics:

- often used to attack a whole group of targets
- inject malicious code into a public website their target(s) frequent
- once the victim(s) visit(s) the compromised site, malware (usually in the form of a backdoor trojan) is installed on their computer

Goal

To get malware onto the target's machine. Can be used to obtain information, gain remote access to a device, or to simply destroy the victim's device or network. Water holing is a common tactic used in cyber espionage.

3 BAITING

Medium:

- USB drive
- free download
- fake software update
- generic version of software

Tactics:

- entice victim with an item or good they want
- offer free music, movie, software downloads, etc.
- hand out free USBs or leave infected USBs lying around for intended victim(s) to take

Goal

Use the promise of a good or item to deceive the victim into executing malicious code or software on their device.either by downloading or plugging in an infected device

4 QUID PRO QUO

Medium:

- phone

Tactics:

- a lot like baiting, but instead of offering a free good, quid pro quo attacks offer a service.
- often impersonate IT services
- ask for credentials so they can get into your system and "fix" something for you
- often ask victim to disable antivirus so they can install the "update"
- spam call all employees of a business they are trying to infiltrate until they get someone to fall for the scam

Goal

Convince the victim allow them access into their computer or company's system by handing over their credentials or downloading malware.

5 PRETEXTING

Medium:

- phone
- email
- text

Tactics:

- rely on building a false sense of trust with the victim
- build a credible story that leaves little room for doubt
- often pose as the victim's, bank, insurance company, etc..

Goal

To convince the victim to give up their personal or company information.