**What is Social Engineering?**

Social engineering is the art of manipulation in order to gain sensitive information. The information these criminals are seeking could be your password, banking information, or access to your computer to install bad software that will give them control over your computer. They can also take advantage of your inclination to trust to gain access to places they shouldn’t.

**What does Social Engineering look like?**

One of the most common forms of social engineering is phishing. We will cover that in a different lesson.

Another form of social engineering is baiting scenarios. These schemes will put something that people want out onto the internet in hopes that people will click. These can be found on sites offering free downloads of new movies, music, or books. The criminals will hide bad software in the download that will infect your computer.

Another form of baiting if leaving a storage device, such as a USB, for someone to find. The person who finds it will usually plug it in to their computer inorder to find who it belongs to. The USB is loaded with bad software and infects the computer.

Criminals will also send out responses to questions you never asked. With this form of social engineering, you will usually get an email saying how they can help you with a problem you may have. They will send these emails to millions of people in hopes of getting a few responses. If you take them up on their offer they will ask you to log in with your username and password. When you do they will install software that will allow them to gain access at a later date.

Another common form of social engineering is called tailgating or piggybacking. This is where a criminal tags along with another person who is authorized to gain entry into a restricted area. This can be done by manipulating a person’s kindness, such as holding a door for someone. For example, if someone wanted access to the school. They could wait for a teacher or student to enter and walk up behind them and usually, that teacher or student would hold the door open and allow that person access.

**How do you protect yourself from being a victim of social engineering?**

**Slow Down:** Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review. Read each email and message carefully.

**Don’t let a link be in control of where you land:** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in an email will show the actual URL at the bottom, but a good fake can still steer you wrong. If an email is telling you to click a link, instead go to the site with a search engine.

**Be careful of downloads:** Don’t download files from untrustworthy sites or senders. Sites that offer you free movies or music will usually download bad software that can take control of your computer.

**Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it’s a scam.

**Reject requests for help or offers of help.** Real companies and organizations do not contact you to provide help unless you ask for it. If you did not ask for help from the sender, consider any offer to ’help’ a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations on your own to avoid falling for a scam.

**Set your spam filters to high**. Every email program has spam filters. To find yours, look at your settings options, and set these to high. Make sure to remember to check your spam folder periodically to see if a real email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase ’spam filters’.

**Secure your computing devices**. Install anti-virus software, firewalls, email filters, and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn’t automatically update, manually update it whenever you receive a notice to do so.

**Robots don't call you:** Real companies don’t use robots when they call you. If the person who called you sounds like a recording or a robot, then that call is most likely a scam.

**Be aware:** When online or in real life be aware of what you are doing or where you are browsing. You can usually see the signs of a social engineering website or emails. Look at the website or email address. Also if you are going into a place where not everyone is allowed such as the school don't hold the door for people unless you know they are allowed there.