Forms of Social Engineering

Social engineering is all about manipulation and tricking the victim to do something they shouldn't—and wouldn't normally—do, such as giving out personal information or giving access to sensitive corporate data. The term actually encompasses many different tactics. Let's examine a few of the most common attacks.

Phishing

Phishing emails come in a variety of styles. Some might say you've won the lottery or just inherited a lot of money from an aunt you don't remember. Some will be urgent; you have to do something right now or something bad will happen to your account. And others might be sneaky, pretending to be your boss requesting you click on a link or download an attachment. Avoid falling victim to these attacks by looking closely at any email asking you to provide information. Double checking email addresses and hovering over links is a good place to start.

Pretexting

Pretexting is simply someone on the telephone (or on social media) who is pretending to be someone they are not in order to steal information. The "pretexter" will create a scenario such as saying you have an unusual charge on your credit card, and they need some information to confirm your identity in order to resolve the issue. They might sound sympathetic, overly helpful or official in order to gain your trust. Don't fall for it!

Baiting

So, you found this lonely USB drive just hanging out. How do you find out whom it belongs to? Whatever you do, don't plug it into your home computer or work computer! That USB drive could be a baiting attempt. If you plug it in, it could install malware onto your device. Baiting attempts usually offer goods in exchange for something like a login and password or, in the case of the USB drive, a free USB drive if you can't locate the owner.

Quid Pro Quo

If you give me something, I will give you something. Don't be fooled by this form of social engineering. *Quid pro quo* is similar to baiting but generally involves the victim giving information and the criminal giving a supposed service in return. For example, someone posing as your internet provider calls you up and offers to improve your PC's performance for free. All he needs is your password. Be aware!

Tailgating

So, you're driving to work and this guy behind you just will not back off. Time for a brake check! *(No, don't do that!)* You get to work, you're about to open the door with your pass card, and BAM! This time, it's a human tailgater. Tailgating occurs when an unauthorized person gets into a restricted area by slipping in behind authorized individuals. "Tailgaters" may pose as a delivery person to gain entrance, or even as a friendly fellow employee who lost their badge or left it inside. Never allow tailgating!