SOCIAL MEDIA AND SOCIAL ENGINEERING

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Security is all about knowing who and what to trust. It is important to know when and when not to take a person at their word and when the person you are communicating with is who they say they are. The same is true of online interactions and website usage: when do you trust that the website you are using is legitimate or is safe to provide your information?

Ask any security professional and they will tell you that the weakest link in the security chain is the human who accepts a person or scenario at face value. It doesn't matter how many locks and deadbolts are on your doors and windows, or if have guard dogs, alarm systems, floodlights, fences with barbed wire, and armed security personnel; if you trust the person at the gate who says he is the pizza delivery guy and you let him in without first checking to see if he is legitimate you are completely exposed to whatever risk he represents.

What Does a Social Engineering Attack Look Like?

Email from a friend

If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well.

Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

Taking advantage of your trust and curiosity, these messages will:

- **Contain a link** that you just have to check out–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived

- **Contain a download** of pictures, music, movie, document, etc., that has malicious software embedded. If you download–which you are likely to do since you think it is from your friend–you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know. And on, and on.

Email from another trusted source

Phishing attacks are a subset of social engineering strategy that imitate a trusted source and concoct a seemingly logical scenario for handing over login credentials or other sensitive personal data. According to Webroot data, financial institutions represent the vast majority of impersonated companies and, according to Verizon's annual Data Breach Investigations Report, social engineering attacks including phishing and pretexting (see below) are responsible for 93% of successful data breaches.

Using a compelling story or pretext, these messages may:

- **Urgently ask for your help.** Your friend is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
- **Use phishing attempts with a legitimate-seeming background**. Typically, a phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.
- **Ask you to donate to their charitable fundraiser, or some other cause.** Likely with instructions on how to send the money to the criminal. Preying on kindness and generosity, these phishers ask for aid or support for whatever disaster, political campaign, or charity is momentarily top-of-mind.
- **Present a problem that requires you to "verify" your information by clicking on the displayed link and providing information in their form.** The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site). Because everything looks legitimate, you trust the email and the phony site and provide whatever information the crook is asking for. These types of phishing scams often include a warning of what will happen if you fail to act soon because criminals know that if they can get you to act before you think, you're more likely to fall for their phishing attempt.
- **Notify you that you're a 'winner.'** Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide information about your bank routing so they know how to send it to you or give your address and phone number so they can send the prize, and you may also be asked to prove who you are often including your social security number. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.
- **Pose as a boss or coworker.** It may ask for an update on an important, proprietary project your company is currently working on, for payment information pertaining to a company credit card, or some other inquiry masquerading as day-to-day business.

Don’t become a victim

While phishing attacks are rampant, short-lived, and need only a few users to take the bait for a successful campaign, there are methods for protecting yourself. Most don't require much more than simply paying attention to the details in front of you. Keep the following in mind to avoid being phished yourself.