Week 5 – National Cybersecurity Awareness Month

Social Engineering is a term used when talking about Internet threats like phishing emails, and other types of scams. It is defined as the manipulation or the taking advantage of human qualities to serve an agenda. We are seeing these types of scams skyrocket in recent months, and a huge reason for this is that social engineering relies on human emotions such as empathy, curiosity, and fear, rather than a large amount of technical skill to gain access to sensitive data. The human element is what makes these types of scams the hardest to prepare for and detect, however with a little vigilance we can make it harder for social engineers to get what they want.

What does social engineering look like in action?

It could be a phishing email designed to look like it is from a credible business, like Amazon or your bank. Or, it could be disguised to look like it comes from someone you know such as a friend or family member. Some emails may even appear to have been sent to you by mistake, with a subject line such as "Our Vacation pics", where the social engineer is counting on human curiosity to open the file, but if you click that link or open that attachment, you could be installing malware or viruses.

Phone calls or text messages, such as the popular IRS tax scam and the tech support scams use aggressive tactics that utilize the element of fear in the hopes it will cause victims to react quickly without stopping to think if the call or message is legitimate.

Physical or in-person exchanges, like mentioned in the scenario where you are asked to hold the door for someone, or a late night knock on the door from someone claiming to be in trouble and needs to use your phone are ways scammers use emotions of empathy or sympathy to scam good hearted victims. Fraudulent charity scams in the wake of disaster are another example of this.

How can we protect ourselves?

Being vigilant is the best way to combat these threats. If an unexpected email from someone you know comes in with an attachment, reach out to the sender via a new email and confirm that they sent the attachment. When you are asked to hold the door by someone who can't reach their badge, instead offer to hold their tray so they can get to their badge. Be careful not to put too much information on social media sites and ensure your privacy settings are setup to limit access, as social engineers will often take the time to search social media and other online avenues to gather information that they can use to impersonate a friend or relative in order to get what they want. When it comes to social engineering, there is no harm in erring on the side of safety.