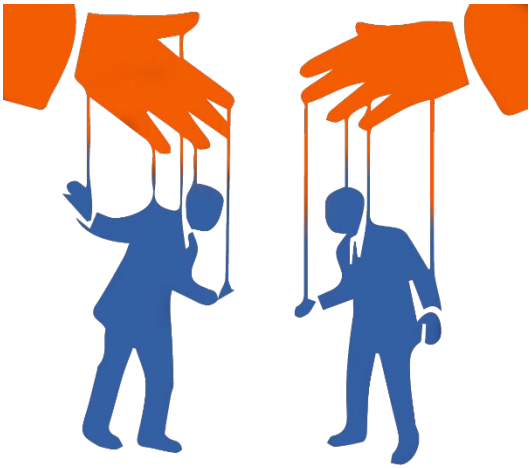
CYBER OCTOBER

Week 2: Social Engineering

Edwards AFB is the center of test and evaluation for the military. Why wouldn't the enemy try to seek as much information as they can? At home, what might you have that someone would like to get access to? Credit card data? Personally identifiable Information (PII)? According to Fifthdomain.com; Social Engineering attacks have increased 500% from Q1 to Q2 2018. Why would it increase so much? There could be many reasons, but most likely because the benefits for the perpetrator are so great.

What is Social Engineering?

Social Engineers takes advantage of human behavior to conduct reconnaissance on a company or entity to discover information to help them infiltrate their network, or gain company secrets.



Impact of Social Engineering

In Sept of 2018, Ji Chaoquna, Chinese Engineering student was arrested of spying on US engineers, scientists, and defense contractors. It is not known yet, what information or how he got it. But one can only assume.

Advanced Persistent Threats (APT) from China stole the equivalent of 5 libraries of congress or 50 terabytes of data says the NSA. Including secrets from the B-1, C-17, F-35, and F-22. Part of their hacking scheme is to do research on the organization structures of their targets. This enables them to know what and who to target.

They gained access to the computers by attaching malicious logic to emails and disseminating them to people in critical positions via Phishing emails. Usually these emails are positioned to look like legitimate business communication, or enticing to the recipient.

So this leaves the big question on how did they know who to send phishing emails to in companies that held the research that they sought.

Protecting yourself against social engineering

Active Reconnaissance

- Avoid strangers asking questions about what you do. Such as social functions, public events. They know that people who work with classified material will be at these events.
- If help desk or a representative of an organization you belong to calls, be wary of pushy tactics. They won't ask personal information.
- If someone calls your office number ensure you verify who they are. If its tech support and you don't have a ticket, ask them to come by your office for verification.
- Social Engineers have been known to record a company's hold music and put their target on hold while playing the music to coax them into thinking it came from the same phone system.
- If it seems too good to be true, it probably is.

Figure 1 J-31 vs F-35

Passive Reconnaissance

- Prevent Social Media reconnaissance
  - Don't put where you work on your social media page.
  - Don't be specific about your job or position within the company or brag about the projects you may or may not be on.
  - Only allow friends to see your profile
  - Harsh criticism of your employer could help social engineer, with conversation of same pre-text. This would help get them "on your side". By saying they have same problems at their company, or act like employee of your company and vocalize their distaste of management.
- Avoid being a target in public, with squadron shirts, airplane decals on your car windows etc. These can lead to active reconnaissance on you.