LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.2.2 - Principles of Social Engineering

Lesson Overview:

Students will:

- Compare and contrast different types of social engineering techniques.

Guiding Question: What are 7 types of social engineering techniques?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.2 - Explain common threat vectors and attack surfaces

- Principles of Social Engineering
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Principles of Social Engineering

Social engineering is the concept of using relationships, persuasion, and body language to steal some otherwise secretive or personal information or persuade someone to perform some action. Social engineering could be done by a single person, or several individuals could collude together to manipulate a victim's behavior. The actual act of social engineering could be done using technical forms of communication such as texting, email, and social media, or via-in person forms of communication such as face-to-face.

Social engineering takes advantage of an unsuspecting victim's bias. Biases are a person's basic beliefs that influence their every decision. For example, most individuals would stop to help an elderly man or woman if they saw they were struggling in public to perform some common act, such as reaching for a can of food on the top shelf in a grocery store or lifting and carrying a heavy package to their car. This action is influenced by a bias or belief that physically challenging tasks that are more difficult for elderly individuals could be performed by those who have more youth or strength. Thus, the bias leads to the action of helping the elderly individual.

In the same way, bias guides our behavior and interactions when faced with malicious content. For example, many have a bias toward helping others in need. Thus, receiving an email asking for your help to pay for a recent widow's bills or to help a struggling student pay for college may influence some to send some of their own money to help. The result of falling victim to the social engineering attack all starts with exploiting a bias. These attacks also commonly exhibit a series of abstract principles that optimize a social engineering attack's effectiveness. These principles are meant to exploit a particular bias and persuade the potential victim to respond to the attack. They include authority, intimidation, consensus/social proof, scarcity, urgency, familiarity/liking, and trust.

Authority is meant to exploit a bias toward obedience and compliance. A person tends to obey authority, so the malicious actor acts as an authority figure to gain information. ***Intimidation*** is meant to exploit a bias of fear. Like authority, people can exploit fear and threaten someone into acting as they normally would not. ***Consensus***, or social proof, is meant to exploit the bias of following the crowd. If everyone else is doing it, then it must be okay. ***Scarcity*** is meant to exploit a bias based on the desire to be exclusive. Scarcity looks like "for a limited time only" or "You are the lucky winner!" to make a person feel special or encourage them to make a mistake. ***Urgency*** is meant to exploit a bias toward speedy action without careful thought. Urgency can look like "you must pay this by" or "you must change your password within the hour." This is an attempt to get a user to make a mistake by acting quickly and not thinking beforehand. ***Familiarity*** or liking is meant to exploit a bias in common thought. An example of familiarity can be using a celebrity; Matthew McConaughey did this, so you should too. Finally, ***trust*** is meant to exploit a bias in relationships. Trust can look like "I will give you this in return." It is an attempt to gain the trust of the user in return for confidential information. All these principles exploit a bias that can cause humans to not reason through situations. These are the reasons why social engineering attacks succeed. They short-circuit the victim's reasoning and thought process, causing them to be persuaded to behave in the way the attacker desires them to.

Defense

Defending against social engineering attacks involves recognizing when these principles are being used in action. Recognizing when someone is trying to persuade you to perform some action that you would not normally do or that would cause you harm by using one of the principles mentioned previously and refusing to comply prevents the social engineering attack from successfully occurring. Detecting these principles can be difficult, as attackers are very well trained and skilled at exploiting biases. When the social engineering attack occurs via email, texting, or some other form of technical communication, recognizing key words and phrases such as “Act now,” “Supplies are limited,” “You were chosen as a winner,” etc. are all potential clues to a social engineering attack.

There are several examples of phishing attacks that have caused victims to provide their personal information or money. These examples are great learning tools for us to remain on guard and to always protect information that could be used to harm us.