CCNA Security

Lab - Social Engineering (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Objective

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

Resources

- Computer with Internet Access

Step 1: Research Social Engineering Examples

Social engineering, as it relates to information security, is used to describe the techniques used by a person (or persons) who manipulate people in order to access or compromise information about an organization or its computer systems. A social engineer is usually difficult to identify and may claim to be a new employee, a repair person, or researcher. The social engineer might even offer credentials to support that identity. By gaining trust and asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

Use any Internet browser to research incidents of social engineering. Summarize three examples found in your research.

_____

_____

_____

Answers will vary depending on current events.

Step 2: Recognize the Signs of Social Engineering

Social engineers are nothing more than thieves and spies. Instead of hacking their way into your network via the Internet, they attempt to gain access by relying on a person's desire to be accommodating. Although not specific to network security, the scenario below illustrates how an unsuspecting person can unwittingly give away confidential information.

"The cafe was relatively quiet as I, dressed in a suit, sat at an empty table. I placed my briefcase on the table and waited for a suitable victim. Soon, just such a victim arrived with a friend and sat at the table next to mine. She placed her bag on the seat beside her, pulling the seat close and keeping her hand on the bag at all times.

After a few minutes, her friend left to find a restroom. The mark [target] was alone, so I gave Alex and Jess the signal. Playing a couple, Alex and Jess asked the mark if she would take a picture of them both. She was happy to do so. She removed her hand from her bag to take the camera and snap a picture of the "happy couple" and, while distracted, I reached over, took her bag, and locked it inside my briefcase. My victim had yet to notice her purse was missing as Alex and Jess left the café. Alex then went to a nearby parking garage.

It didn't take long for her to realize her bag was gone. She began to panic, looking around frantically. This was exactly what we were hoping for so, I asked her if she needed help.

She asked me if I had seen anything. I told her I hadn't but convinced her to sit down and think about what was in the bag. A phone. Make-up. A little cash. And her credit cards. Bingo!

I asked who she banked with and then told her that I worked for that bank. What a stroke of luck! I reassured her that everything would be fine, but she would need to cancel her credit card right away. I called the "help-desk" number, which was actually Alex, and handed my phone to her.

Alex was in a van in the parking garage. On the dashboard, a CD player was playing office noises. He assured the mark that her card could easily be canceled but, to verify her identity, she needed to enter her PIN on the keypad of the phone she was using. My phone and my keypad.

When we had her PIN, I left. If we were real thieves, we would have had access to her account via ATM withdrawals and PIN purchases. Fortunately for her, it was just a TV show."

"Hacking VS Social Engineering -by Christopher Hadnagy http://www.hackersgarage.com/hacking-vs-social-engineering.html

Remember: "Those who build walls think differently than those who seek to go over, under, around, or through them." Paul Wilson - The Real Hustle

Research ways to recognize social engineering. Describe three examples found in your research.

_____

_____

_____

Answers will vary.

Step 3: Research Ways to Prevent Social Engineering

Does your company or school have procedures in place to help to prevent social engineering?

_____

If so, what are some of those procedures?

_____

_____

_____

_____

_____

_____

Use the Internet to research procedures that other organizations use to prevent social engineers from gaining access to confidential information. List your findings.

_____

_____

_____

_____

_____

_____

_____