Module 13 Lesson Plan

Grade Level: High School

Subject: Physical Security and Social Engineering

Module Duration: 1 Hour

Overview and Purpose:

Module 13 is all about physical security and social engineering. In cyber security, physical security seems to be pushed under the rug. However, physical security is a very important aspect of cyber security. In this module, we take a whole section to discuss the importance of it, and provide different examples of physical security. The other section within Module 13 is social engineering which explains the different types of potential social attacks. Module 13 is composed of one slideshow, two activities, and an outline. The slideshow helps the students understand the two topics. Activity 1 is all about social engineering. The goal of it is to help students recognize the warning signs of an attack. Lastly, Activity 2 is about physical security. It is meant to introduce students to live images.

IT-A Iowa CS Guidelines:

- *Iowa Computer Science Standards—3A-CS-02. Compare levels of abstraction and interactions between application software, system software, and hardware layers.*
- *Iowa Computer Science Standards—3B-CS-02. Illustrate ways computing systems implement logic, input, and output through hardware components.*
- *Iowa Core—21st Century Learning Skills 21.9-12.TL.4 Demonstrate critical thinking skills using appropriate tools and resources to plan and conduct research, manage projects, solve problems and make informed decisions.*
- *Iowa Core—21st Century Learning Skills 21.9-12.ES.4. Demonstrate initiative and self-direction through high achievement and lifelong learning while exploring the ways individual talents and skills can be used for productive outcomes in personal and professional life.*

K-12 Cybersecurity Learning Standards:

- ***9-12.DC.PPI.2 Explain the individual risks of a data breach to an organization housing personal data.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of understanding that if an organization gets hacked, it can still harm the individual whose data was stolen.*
- ***9-12.SEC.DATA Formulate a plan to apply security measures to protect data in all three states.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of protecting data in its three states.*
- ***9-12.SEC.COMP Evaluate Defense in Depth strategies that can protect simple networks.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of layered strategies, such as firewalls, allow and block lists, changes to default passwords, access points, and network segmentation.*
- ***9-12.SEC.AUTH Evaluate authentication and authorization methods and the risks associated with failure.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of authentication and authorization methods, such as certificate, tokenbased, two-factor, multifactor, and biometric.*
- ***9-12.SEC.PHYS Analyze the different types of attacks that affect physical security.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of physical security attacks, such as social engineering, poor security policies, and malicious actors.*
- ***9-12.SEC.CTRL Justify the use of Defense in Depth and the need for physical access controls.*** *Clarification statement: At this level, student discussions should focus on previous standards as well as grade-appropriate examples of various physical access controls, such as proximity badges, PIN codes, and man traps.*

Learning Objectives:

1. Familiarize yourself with social engineering

2. Know why hackers use social engineering and how to plan an attack

3. Recognize the different types of social engineering attacks

4. Understand the importance of physical security

5. Learn about each type of physical security and how it works

6. Execute a social engineering attack

7. Learn how to bypass a live image

Background Information:

Before this module, it is important to review the Module 13 Slideshow and the Module 13 Outline. As background knowledge before teaching this module, it is important to understand social engineering, physical security, and specifically live images. The first section of module 13 is all about social engineering. Social engineering is essentially the act of hacking a person's psychology. It is basically the act of manipulating important people to try and gain access. Social engineering can be very simple because it is easier to trick a person than try and physically break into a computer system. This tactic is frequently used by hackers since physical/technical hacking is getting much harder with modern technology advancements. The four steps to a successful social engineering attack are reconnaissance, develop an attack plan, execute your plan, and write/submit your report (pentester). The types of social engineering attacks include baiting, phishing, whaling, Wifi Phishing, SMSishing, QR Code, and TinyURL. These attacks are further explained in the slideshow. The next section of the module is about physical security. Physical security involves the physical measures put in place to protect assets. Since cyber security focuses a lot on the technical measures to protect a computer system, physical security can easily be forgotten. However, physical security is also very important. The different types of physical security include doors, gates, locks, fences, codes, badges, card readers, sensores, ceilings, etc. Lastly, we will be discussing live images. Activity 2 will be all about live images. A live image is a USB or physical hard drive that contains an operating system. When it is connected to a computer, it runs on top of the computer's current operating system. The live image itself can then set new permissions (read, write, execute) to the files on the underlying operating system. This is an easy way for hackers to gain control.

For more information about the IT-Adventures Program, head on over to ://www.it-adventures.org/. If you have any questions or need help with the Cyber Defence Venue, feel free to email ita@iastate.edu

Link to IT-A website: http://www.it-adventures.org/

Powerpoint Lesson:

- Open "Module 13 Slideshow"
- Begin the social engineering section of the slideshow.
    - The videos on slide 5 are brief, and you should take the time to watch them as a class.
    - The video on slide 8 pulls together what has been mentioned on the previous slides. The video is about 20 minutes long and is suggested for the students to watch on their own time.
    - Explained the four steps of a social engineering attack (slides 9-13)
    - Introduce the different types of attacks (slides 14-22)
    - Have the students take a minute to reflect of how the social engineering can relate to the CDC (slide 23)
- Move on over to the next section titled "Physical Security"
    - Run through the different types of physical security
    - The videos in this section are short clips that show how the security measures work. They are recommended to watch for a better understanding.
- Finish the slideshow off by reintroducing the CDC on slide 34
- Guide the students into "Module 13 Activity 1" and "Module 13 Activity 2"

Activity 1:

- Provide the students with the "Module 13 Activity 1" handout
- This activity will have the students run through 3 scenarios of social engineering..
- Mentioned in the slideshow, social engineering can be very simple, so this activity is meant to have the students practice detecting attacks.
- Have the students read each scenario individually
- Then as teams, have the students discuss the reflection questions.
    - This will allow for students to practice their communication skills as a team.
- Lastly, the students should read the final section of the activity that offers tips on how to spot scammers.

Activity 2:

- Provide the student with the "Module 13 Activity 2" handout
- This activity will have the students experience the role of the red team (hacker).
    - Students will be breaking into a virtual computer using a live image.
- The students will also be seeing the blue team's side of view in this activity
    - After breaking into the computer, they will then work to patch up the VM.
- This activity will have the teams use the microsoft computer they created in past modules as well as their linux computer.

Additional Resources:

- Anatomy of a Spearphishing Attack
- Chris Pritchard - The Basics of Social Engineering - DEF CON 27 Social Engineeri…
- What is Social Engineering?
- This is how hackers hack you using simple social engineering
- GOOGLE!
- VMware Glossary

Material Used:

Module 13 Outline

Module 13 Slideshow

Activities:

Module 13 Activity 1

Module 13 Activity 2

Sources:

CRC Press, 2012. Jacobson & Idiorek, Computer Security Literacy: Staying Safe in a Digital World, 9781439856185