Daily Lesson Plans – Lesson 5

Instructional Days: 8 – 10

Topic Description: In this lesson the students will “practice” safe computing. We will discuss, demonstrate, and become familiar with Anti-virus and cleaner programs, firewalls, passwords and passphrases, biometrics, encryption and key loggers. We will discuss how the world has changed with the stuxnet virus and emphasize that we must stay knowledgably vigilant in the face of new technology to keep up on security for the sake of our privacy.

Objectives:

The students will be able to:

- Describe the way in which programs and techniques that secure our privacy works and why we need them.
- Demonstrate how we use safe computing programs and techniques.
- Develop strategies to make our lives more private and our computers more secure.

Outline of the Lesson:

- Discuss our current method of security, passwords, their pros and cons. (40)
- Demonstrate with passphrases, followed by biometrics and encryption how we can make our security even better. (40)
- Discuss ways viruses and malware get into our computer with email and web surfing as well as how people can get our information with key loggers. (20)
- Discuss and demonstrate ways in which social media and other internet activities can be dangerous (50)
- Discuss and demonstrate device awareness. People are watching you when you use your devices in public places, not always with malicious intents but your information is leaking. (15)

Student Activities:

- Determine new passphrases to use instead of the passwords they currently have.
- Students break into groups of two and encrypt a message for another group
- Students test the md5 encryption algorithm and online password crackers
- Students explore virus and malware removal programs
- Students discover photo meta data on photos they take with their own smart phone. with the Exif program
- Students participate in a smartphone activity that demonstrates the dangers of people shoulder surfing while that use their personal devices

Teaching/Learning Activities:

- Discuss our current method of security, passwords, their pros and cons.
  - Use the Computer World website to see some of the worst passwords in the last 5 years. It’s a good idea to see if any students use these passwords currently. STOP THEM IF THEY DO!
  - Use a tool to check your password and randompassword.com
  - Discuss with the students what makes a good password compared to bad passwords. Discuss variety of character, length and then discuss how a long

    - password is better than a short one. DO THE MATH!! Refer to the PowerPoint for this discussion.
    - Drive the point home with a demonstration on their smart phones. Ask for everyone who uses a code to log in. Find out how many digits are in their pin. Likely it will be 4 at least and 6 at most, we can then talk about how many password combinations possible.
- Demonstrate with passphrases, followed by biometrics and encryption how we can make our security even better.
    - Have students come up with passphrases of their own. They should be at least 16 characters. I find the students have a hard time coming up with memorable passphrases. The teacher needs to prime that pump.
    - Use the weird and crazy pictures in the Lesson 5 resource folder name "passphrases", they are memorable and strange.
    - Other things you may try are things they love or love to do. Make sure it's not too simplistic, try to get it unique to them, not "I Like Basketball".
    - Also talk to the students about changing some of the letters in the phrase. O becomes 0 and 5 becomes $, and e's becomes 3's. They will be able to come up with something unique to them.
- Discuss ways viruses and malware get into our computer with email and web surfing as well as how people can get our information with key loggers
    - Email is one of the easiest ways malware can get into the system. Discuss phishing and spear phishing and other types of attacks.
    - Downloading unknown files or going to unknown websites can be problems. Many websites will install malware, usually with the surfers help, that will steal information as it pleases. Viruses can come from both websites and email. Remember viruses and malware are simply programs.
    - Have the students look up the definition of a key logger and so they can discover the definition. It can be installed in my ways. With a keylogger on the system everything that is typed goes right into a file for later reading. PASSWORDS AND ALL.
    - Stuxnet, the virus that changed everything
- Discuss and demonstrate ways in which social media and other internet activities can be dangerous
    - Pew research has some interesting statistics on Teen Social Media Use as of 2012: Refer to the PowerPoint for those statistics.
    - Let's try an exercise. While the students are around campus before the next class, have them take a picture of something around campus with their phone. Don't take it of another person, just a building or some other object. Email it to teacher's email so everyone can see if we can find out where it was taken around the campus.
    - Use the ExifPro 2 Image Meta Data view and look at the information associated with the picture.
    - The students must understand the data that goes along with the photo. I can be turned off and now Facebook and other social media sites are starting to strip that information from the image.
- Discuss and demonstrate device awareness. People are watching you when you use your devices in public places, not always with malicious intents but your information is leaking.
    - Do you know what's going on around you when you're on your device? Maybe you should.

Resources:

- Computer World Worst Passwords Article
- Random Password website password Checker
- The Free Edition of Spybot - Search & Destroy Anti-Malware and Anti-Virus Software
- Malware Bytes
- Exif Pro 2 Software for viewing Photo Meta Data
- Safe Computing Practice PowerPoint

Notes For the Future:

- This lesson is the best of the 5. I demonstrate many of the tools and techniques for protecting their computers, network and information.
- Exif Pro has a big impact if you do not let them know why they are taking pictures, especially when someone turns in an old photo instead of a new one.
- Explaining why longer passwords work better than shorter ones is good but students still do not want to make passwords long.