Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Humans the Weak Link

- Feel how you want about this topic and there is a saying that OPSEC is 10 % technical and 90% training.
- The end user will always be the easiest point of compromise in any system.

Building Security Awareness

- Security awareness: Is the knowledge and the attention shown by users with physical, logical, and administrate controls.
- **Protecting Data**: Regardless of the industry in which we operate, we will almost always have a need for protecting data of some variety. As we covered in Lesson 6, there are numerous laws and regulations that govern data, and compliance with them is one of the costs of doing business.
- **Passwords**: Always enforce certain levels of password strength at least eight characters, at least one upper case, at least one lower case, at least one symbol, at least one number. This would produce a password something along the lines of P@ssw0rd. The key is to balance the complexity of the password with the importance of what is being protected. Eight characters is probably fine for a site that stores family photos, but not recommend for a bank account.

Social Engineering

- **Social engineering:** is a technique that relies on the willingness of people to help others, particularly when the target is faced with someone that appears to be in distress, someone that is intimidating, or someone that we would normally expect to see in a given situation.
- **Pretexting:** is when we assume the guise of a manager, customer, reporter, or even a co-worker's family member. Using a fake identity, we create a believable scenario that elicits the target to give us sensitive information or perform some action which they would not normally do for a stranger.
- **Phishing:** is a particular social engineering technique and is largely employed through the use of electronic communications such as e-mail, texting, or phone calls. Most phishing attacks are very broad in nature and involve convincing the potential victim to click on a link in the e-mail, in order to send the victim to a fake site designed to collect personal information or credentials, or to have the victim install malware on their system.
- **Tailgating:** also known as "piggybacking," is what most people think of when they hear the term used. Quite simply, this is the act of following someone through an access control point, such as secure door, without having the proper credentials, badge, or key, normally needed to enter the door.

Network Usage and Admin Policies

- **Network usage**: perhaps more accurately **network awareness**, is an important concept to discuss with users. It is certainly the case today that a large number of people have access to numerous networks, both wired and wireless, from relatively restricted networks in the workplace to wide-open networks (largely wireless) in homes, coffee shops, and on airplanes.
- **Malware**: is any application that makes any unauthorized changes to a device. Malware can come from many sources and most commonly email.
- **Personal Equipment**: (Bring Your Own Device BYOD) use of personal equipment brings cost saves for the organization but can open up certain risks like data leakage, malware, and, intellectual property issues.
- **Clean Desk:** is a policy that sensitive information is not to be left out on a desk when it is to be unattended for any significant period of time, such as leaving for the day or going to lunch. This is typically followed up with a discussion on how sensitive data on physical media such as paper or tape needs to be disposed of in order to ensure that this is done properly, namely, the use of shred bins, data destruction services, media shredders, and so on.

Security Awareness and Training

- In order to communicate our desired information to users, we will most often use the vehicle of a security awareness and training program.
- **Gamification**: adding certain game elements to what we are doing in training.
- We can also gain the attention of our users through the use of security-oriented posters, **giveaways (pens, coffee mugs, etc.)**, newsletters, and a great number of similar devices.
- **Food Food Food**
- **Ineffective communication methods**: Mass email, Annual computer-based training, Death by point, and Outside trainers.