Kristin Roberts 0335355

Module 6 Summary:

Module 6 was about internet security. It covered different types of security threats such as phishing emails, denial-of-service-attacks, identity theft, etc. It also went over countermeasures to identify threats and how to protect against them such as using firewalls and programs to remove malware.

A topic that stood out initially was phishing attacks. My husband several times has wanted to open links in a spoofed email. One instance of this his from line appeared to be from an old colleague. We determined this to be a phishing attack. Luckily, he never opened the link. He has had this happen before, usually from what appears to be company sites, he has accounts to encouraging him to click links. I am grateful he checks with me before clicking things. He is too trusting.

I am sad to say my grandmother’s Facebook account has been hacked multiple times. She now has several accounts, and only one of them is legitimate. I use multifactor authentication on my Facebook account to have an additional code required to log in sent to my phone besides my username and password. Unfortunately, I only had single-factor authentication on my Instagram account, and it was hacked into and taken over years ago. Both of my computer teachers use password managers to keep track of their login information. I should utilize that program as well as I have had a terrible habit of using the same password for more than one account.

I was familiar identifying a padlock icon in the address bar to tell you the site should be safe. I wasn’t aware it was a type of SSL-EV certificate (Secure Sockets Layer – Extended Validation). The thing I take away most from this chapter was how a malicious URL could be hidden in an apparent safe URL with https in the beginning by including a @ symbol. Apparently, everything preceding the @ symbol in the URL is essentially forgotten. This is valuable information I will use in the future!