Unit 5 Critical Thinking Questions

1. **Determine if any software or hardware on your home network has any of the vulnerabilities mentioned in the most recent US-CERT bulletin. If so, what information do they provide for you to protect these vulnerabilities? If not, summarize what vulnerabilities were mentioned and describe what kind of network might have these vulnerabilities. How can you use these organizations and the information that they provide to help protect yourself and keep your online activity safe?**

I read the bulletin that was released on May 24th, 2021.

None of the vulnerabilities listed, that I recognized, apply to me. Cisco things showed up **A LOT**, as well as IBM. For Cisco, there was a risk that hackers could execute tasks that will not be good. For IBM, they had more to do with hackers being able to decrypt sensitive things. I can use resources like this to see if anything I use has any vulnerabilities. If I were to ever have any, I could take the steps needed to protect myself.

2. **Effective communication is essential in the workplace, especially when it comes to electronic communication. What are some appropriate communication concepts and/or strategies that could enhance oral and written communication in the workplace? Would these strategies also be appropriate for electronic communication? Explain.**

Communication is one of the most important things in the workplace. Oral communication, in my opinion, is the best form of it. Keeping communication during projects allows for things to get done in a smooth/timely manner. Important things to do that help include active listening, friendliness, confidence, empathy, and respect. All of these would be appropriate in electronic form, if not even more. This is because you have to be extra careful of how you tone things electronically as all the person is reading through that is text.

3. **Evaluate and explain what risks are involved in connecting to an unsecured wireless network in a public setting (like a coffee shop) that are not present for secured/password protected home networks. What are some basic ways that you can protect yourself if you use an unsecured connection? Explain.**

When you connect to an unsecured wireless network, you are connecting to a connection that is open to everybody with no security. If you use a network like this unprotected, you have the risk of your internet traffic being intercepted. Let's say you make an online purchase on a network like this, and someone intercepts it, they now most likely have the payment information you just used to make the purchase. If you want to protect yourself from something like this happening, you should use a VPN. It encrypts your traffic from your phone to the IPS of the network you are on.

4. **What is the importance of online identity management and monitoring? What are some of the negative consequences that those who do not manage and monitor their online identity might be open to? Explain.**

It is important because as the world becomes more dependent on the internet and as well as our increased usage of it, it is important that you have a good reputation on it. Job recruiters check lots of things you do on the internet when you want to get a job. If you don't check and manage it the right way, you can find yourself not being able to get jobs. The moral of the story is, don't do dumb things on the internet.

5. **Consider the current cybersecurity protections that exist on a national level. Evaluate how effective the current protections and procedures are. Would it be helpful to move to a more globally-representative system, and if so, how/why? Explain.**

I think the protections for the most part right now are fine. There are always going to be holes where people can get through, but that's normal when it comes to this kind of thing. I don't think moving to a global system would be the best thing, because if the system were to get hacked, the entire world would be in trouble instead of just one or two countries.