Unit 4 Critical Thinking Questions

1. **Fundamentally, what natural human tendencies does social engineering prey on? Which populations might be especially vulnerable to social engineering?**

Social engineering preys on our “bugs”, such as when if we see something shiny on the ground we have the natural instinct to pick up and look at it more. Anybody is vulnerable to social engineering, not just specific people.

2. **Come up with your own example of social engineering that might lead people to infect their computer (or device) with malware, something distinct from the specific examples covered in the unit (which were leaving a suspicious USB stick in public, someone calling you pretending to be your ISP and asking for account information, or sending a text saying you are being charged for a service you never agreed to).**

A fake receipt from Apple requesting that the customer confirm their purchase. A button in the email takes them to another page, and before they can officially confirm the purchase they need to confirm their information. Information such as name, email, address, finance information, social security number, etc. Once they enter the information and get to the end, they get an “error” saying that something went wrong. This is a staged part where they submitted a form and the hacker received the information, but the victim(s) got nowhere from it.

3. **For your state, what terms are used in the anti-bullying laws? Do the laws cover cyberbullying? What are the legal consequences for cyberbullying in your state? Finally, according to the website, what are some of the signs, effects, and solutions for cyberbullying (provide at least TWO examples for each category)?**

In Pennsylvania, it basically just describes what bullying is and makes it required that the schools address what it is. The laws do cover cyberbullying. It states, “Act 26, HB 229 (July 10, 2015): makes cyber harassment of a child a third degree misdemeanor, punishable through a diversionary program.”

4. **As a user, how might you recognize, report, and avoid social engineering attempts? Evaluate and explain various methods that you could employ to recognize, report, and avoid potential social engineering attempts.**

It actually isn’t the hardest thing to recognize social engineering attempts, there is a sort-of method to it. What I try to do is know what something normal looks like. If you get an email that doesn’t look like that normal, or if you get redirected to a site that does not look like that normal, then it isn’t the real thing. There always is something that gets messed up when people try to make it look just the same. To report these attempts, you can actually submit reports to the government, through the Cybersecurity & Infrastructure Security Agency.

5. **Name at least two sites, apps, etc. you have used in the past year that have had privacy policies. Either explain what was in those policies or explain why you didn't read the privacy policy. If you didn't read the policy, how might this negatively impact your privacy?**

Pretty much every site you use on the internet has a privacy policy. Two examples of these sites are Google and NBC News. In Google's privacy policy, they say that they collect a lot of information from you. Information such as web activity, location information, who you communicate with, etc. Now they say everything is secure with them (though as always I never 100% trust that kind of statement). For NBC News, it collects less information (since it is a news site as compared to a search engine site). Information they collect includes account information (of your account on that specific site), device information, usage, etc.