Unit 2 Critical Thinking Questions

1. **Imagine you work for a company that has a large profile in the community. Everyone knows about the good work your company does. One day you come home from work really annoyed at a decision that one of your coworkers made, and you decide to blast out a rant on Facebook about that coworker and your company, questioning your coworker's integrity. You tag the coworker in the post and make the post public. Though you haven't done anything illegal, you have crossed some ethical lines. What are they? What are some potential long-term consequences you might face professionally because of your public outburst? What might have been a better alternative response to this workplace situation?**

This action is known as flaming. This will not only make the other person look bad, but it may make you look even worse. Actions like this may also make the company look bad. As the company has a good reputation, that may be attacked through these actions. You will most likely be fired by the company, and you will gain a not-so-good reputation for complaining publicly about your co-worker(s). Instead of publicly ranting, it would have been best to take with the person one-on-one. Therefore, the whole public does not have to see this problem.

2. **Who is Aaron Swartz, and what did he do? Why do you think that his case is significant in terms of the unethical use of computers and networks? Do you think Swartz deserved to be prosecuted? Why or why not? Explain.**

Aaron Swartz was a computer programmer who was involved in many different things. He was one of the founding developers of RSS, Markdown, and Creative Commons (the organization). He also was involved in hacking as well. He was arrested in 2011 for hacking into an unmarked territory of MIT's network and systematically downloading academic journal articles. This case is significant because it shows how far some people will go, in terms of hacking. I'm not really sure as to if he should have been prosecuted or not. The hacking he did was a bit extreme, but I don't get exactly what the big deal about the articles was.

3. **Your friend is known around school for his business: creating and selling fake IDs using templates he "borrowed" from his mother's work computer. How would you approach this friend about his ethically and legally questionable business? Describe at least two approaches or actions that you might take.**

First, I would explain to him that this is wrong. Taking IDs templates and using them to make fake IDs is against the law. I would try to explain to him the legality issues of what he is doing. If he continues to do it, I would most likely mention this to somebody (as he is breaking the law here).

4. **You really want to watch a certain movie, but it's still in theaters, and you don't feel like going out. You know plenty of websites that will allow you to stream a bootleg (illegal copy) of the movie for free if you work around the pop-ups (which might be infected with malware) and if you don't mind a lower-quality image resolution. What decision do you make? To what extent do ethics factor into your dilemma?**

I would decide not to do this. As easy and tempting as it is to use this method, this is breaking the law. I basically would be watching the movie without paying anything. Think of a studio spending millions of dollars to make a movie, and not getting anything back from the people who watch the movie. That is what is going on here. I wouldn't feel right doing it.

5. **What does it mean to perform 'ethical hacking?' Describe what a bounty program is and evaluate how this is an example of ethical hacking. Name at least one reward and one risk a company might face in sponsoring a bounty program.**

Ethical hacking is where you hack, but instead of it being bad it is to help. For example, companies hire these kinds of people. They hire them to test their security networks, to see how secure they are. The hackers try to hack into them and provide insight on how to make their networks even more secure. A bounty program is a type of deal in which a company/website recognizes people for reporting bugs. A reward from this will be lots of people reporting bugs. If people see that they will get recognition for doing something, they will strive to do it. This will result in people sending in mass bug reports to the company/website. A problem may be is that they can't control at the beginning who participates I the program. That means hackers may contribute and trick the company into patching things or doing things that benefit them, not the company. But the company won't realize it at first.