Unit 1 Lab

1. **In terms of shaping the future of cybersecurity in the United States, how influential do you think the Russian hacking efforts of the 2016 election compare to things like the Creeper Virus, Morris Worm, or Captain Zap's hacking of the AT&T online computer system? What aspects of this incident could get in the way of the U.S. government responding effectively to the risks the hacking poses?**

The Russian hacking efforts of the 2016 presidential election can be compared to the Creeper Virus, Morris Worm, and Captain Zap hacking events because this is the first time a type of hack this bad has occurred. The Creeper Virus, Morris Worm, and Captain Zap hacking events were some of the first known serious cybercrime events that ever occurred. For this election hack, this is one of the first times a major election has been hacked in such terms as what happened. Since this is the first time something like this has happened, the government is new to it. Which means that responding to it may take slower since they are not used to these kinds of hacks, unlike others. This could get in the way of the U.S. government responding effectively and quickly to the risks that the hacking poses.

2. **If you take Galante's main premise about what made the United States so vulnerable to the Russian attack, what sorts of changes might need to be made to prepare us for a similar attack? Where should we focus our efforts?**

Since her main premise is that the US was so vulnerable for this hack to happen, that means we need to enact many changes to secure our elections from getting interfered. This includes going state by state making sure all the computer systems are secured. I recently saw a story in the news about a month or two ago that talked about how some states' election computer systems were out of date and unsecure. This is something that needs to be fixed, as outdated systems means unsecure systems. And with unsecure systems, that means they are more prone to get hacked over systems that are more secure. If we do these things, and even more, we can ensure that no hacks will occur when he have another election anytime in the future.

3. **How do you think Galante might respond to a hacker who says, "information wants to be free," a common slogan for those opposed to limiting access to information? Is information like the emails of the Democratic National Committee (DNC) being released by hackers truly "free" (as in, liberated, not no-cost) information?**

I believe that she may be mixed about that statement. I believe this because some information is meant to be viewed by the people of the world, but not all information. Some information, like private emails, are not meant for all people to see. Some of that private information may contain top secret operations going on in the government, which is not yet meant to be known by regular people. Information like the emails of the DNC being released by hackers aren't completely free, as in not all emails have been leaked. But enough were leaked for the public to get a sense of what was going on behind the scenes.

4. What is the difference between "factually correct information" and "the truth"?

Factually correct information means that it is not necessarily true, but the facts make it look true. The truth is what actually happened, regardless if the facts support it or not. The main difference between these two terms have to do with the factual evidence that support "what happened."

5. Imagine you were trying to explain the Russian hacking incident to a child (around 10 years of age) and why it was unethical.

The 2016 election hacking was a hack that occurred during the 2016 Presidential Election. A group of hackers gained access to the computer network of the Democratic National Committee, which is the governing body of the Democratic Party. The had access to it from July 2015 to at least June 2016. They began leaking information and emails from the network. The emails that were leaked included personal information about Democratic Party donors, with credit card and Social Security numbers. It was unethical because this was an invasion of many things, mainly an invasion of privacy. This information was not meant to be seen by the hackers, nor the people they leaked it to. Even though it may have helped people to see some things going on secretly, it still should not have been hacked as it is a criminal offense. It's just like all your emails getting leaked to everyone you know. Let's say something like this happened to the CIA, our country would be in deep trouble. Something like this happening to the CIA would result in the world knowing what our international plans are, and enemy countries would be able to plan against our plans. This hack goes to show how your email accounts being protected can go along way.