Unit 5 Lab

James Lyne

1. **What incident involving a USB drive does Lyne describe in the video that would be a good example of using social engineering to introduce malware onto a computer? What does this reveal, to you, about what parts of human nature social engineering can prey on?**

Somebody walks into a business and asks a receptionist to print something for him from a USB drive given. This reveals that anything can be used in a social engineering attack, anything. Social engineering is beginning to prey on every part of human nature, as hackers find new ways into tricking people to their benefit.

2. **For what ethical task might a company hire a cybercriminal in order to improve the company's cybersecurity?**

They do this to test their security. When they get attacked through this way, they note what went well and what went bad. They then can take those notes to better improve their security.

3. **How can cybercriminals prey on our fears about viruses to actually get us to install viruses on our computers?**

They can trick us into installing software that "will protect us from those viruses." The software that we install will actually contain the virus itself. This is a really good example of a social engineering attack.

4. **What is the "greatest lesson of social media and mobile devices" Lyne talks about in the video? Is there any recent scandal that helps illustrate his point that you can think of?**

He says " And herein is the greatest lesson of social media and mobile devices for all of us right now. Our friends, our families and our colleagues can break our security even when we do the right things." In all honesty, I'm not sure of any scandal that has happened recently like this.

Mikko Hypponen

1. **How have viruses evolved over the years, from the very first virus to contemporary viruses? What is an example of what "happens" to an infected computer in modern times versus in the 1980s?**

Viruses have evolved because of the evolution of technology and security. As security evolves and gets better, hackers still find ways around to do their business. Having a virus now is definitely worse than having a virus 40 years ago. This is because of the fact that we have more information stored on devices than then, also that everything is connected through computers now. If we get attacked now, almost all of our information is at risk. Back then, not as much information would have been at risk.

2. **How could industries like, say, banks or credit card agencies fight modern cybercrime that targets their users?**

They need to have really good security and firewalls that block every single possible entry point. If someone were to slip in at any point, then there is a really high chance that the attacker would be able to move around from that point.

3. **The first TED talk discusses the ways individuals can react to cybercrime, whereas the second video discusses more about how we can hunt down cybercriminals to end cybercrime. Which approach do you think is more effective in fighting cybercrime, and why?**

I think a mixture of both. We have to do whatever it takes to fight cybercrime and secure networks across the world. Knowing how to react to it, knowing what it is, combined with knowing what to do is a very good way in doing this. We need to make sure that we put a stop to cybercrimes, so that we can live in a world where everything we do is secure without the threat of our information being stolen.