Introduction to Data and Cyber-Security (DCS3101) - Assignment 4

Q1

Video 1 – Cybersecurity 101:

This brief video talks about the evolution of the internet throughout the years and what that means in terms of safety. To summarize the video in bullet points:

- You should know the “hazards” of the internet before you store all your important personal information on it and do what you can to protect them
- The internet wasn’t intended to be what it is today, it was developed when computers were huge and only big businesses, governments and universities had access to them. The point was to let the different computers talk to each other and form networks. These networks grew until we had personal computers in the 80’s, and then the development exploded. Soon people were talking, dating, shopping doing everything on the internet. More devices got involved, like phones, cars, elevators etc.
- All that came at a price however, it meant that the security wasn’t good. One computer could send another computer, an instruction to delete information or take over, aka viruses and malware. Or a person could steal another person’s identity by guessing, cracking or extracting a password. Vulnerabilities such as this will never completely go away because they are built into the internet’s architecture. Criminals steals millions of dollars, governments use them for surveillance etc.
- On the other hand, while the perfect internet would have perfect security, there would be serious breaches in privacy. Everything would be monitored and regulated by bots and humans limiting your access to what they deem safe.
- The good news is, even with our flawed internet, there are simple things we can do to protect ourselves and there are a lot of people committed to make the internet more secure.

Video 2 – Cyber codes:

This video talks about the importance of encryption. To summarize the video in bullet points:

- We send coded messages every day, in the form of e-mails, logging on to websites. We use codes all the time because we communicate our private messages in public. Without codes, sending information online over unsecure networks or networks with security holes would be like standing in times square and shouting your inner most secrets to a crowd of millions of people who are doing the same thing
- So, to protect our privacy we send the message as a code that can be read by the receiver and not others. We use these codes everywhere, to shop online and talk to our friends.
- This is not a new phenomenon, we have been using codes throughout the human history. It played a major part in wars for example.
- It is explained how keys are exchanged and how they are used. The concept of public key cryptology which we know is important to cybersecurity, and is widely used in encryption algorithms.

- Not all traffic is encrypted though, online payments usually are but browser history is not, nor are many text messages. This is due to the fact that the security in these instances may not be prioritized.

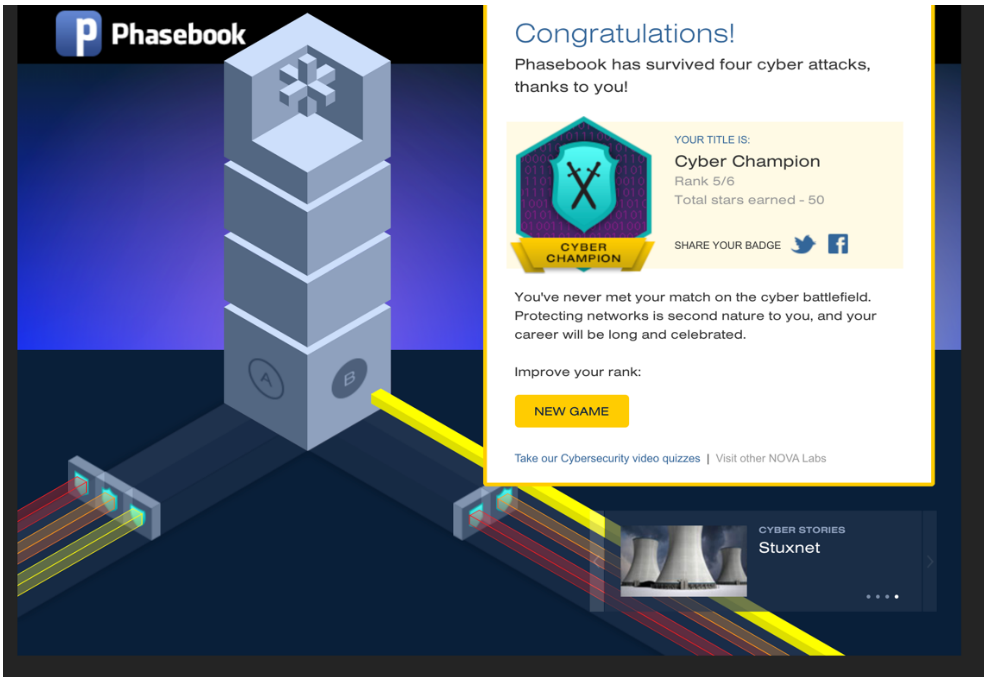
Video 3 – The secret lives of hackers:
This video talks about the role of a hacker in modern day. To summarize the video in bullet points:

- There are many different meanings associated with the word "hacker", such as a burglar, a spy or an inventor. To most people the term "hacking" has a lot of negative connotations, mostly related to something illegal. However, in broad terms hacking is creative problem solving that takes advantage of a property of things in unexpected ways. An example of this is when NASA engineers saved apollo 13 by using a book, a plastic bag and a roll of duct tape.
- Why do hackers hack? Many are driven by intellectual curiosity, they want to learn how a system works, the methodology behind it. Other hackers are like security forces who wants to defend fortresses of information. And of course, there are hackers with malicious ideas in mind.
- Between this, we have hackers who operate in a morally grey area. They might steal information to expose corruption or violate privacy in the name of national security. They consider what they're doing as just and for the greater good, while others see their actions as dishonorable.
- Assigning labels such as good, bad, wrong or right to hacking is not particularly productive, as it means so many different things and can take so many different shapes depending on the person and their intent.

Video 4 – A cyber privacy parable:
This video talks about the importance of privacy and how one should go about it .To summarize the video in bullet points:

- The video mentions a story about a guy named Tim who posted a personal picture online, without thinking about the consequences. Basically, by using social engineering skills an identity theft crime ring picked up the information about Tim using the picture he posted, and they managed to steal his identity including social security number, bank accounts and so on.
- Tim's story is obviously a worst cases scenario, but this still happens to regular people on a daily basis. Information that you post publicly can be stored by anyone who finds it.
- These problems will probably never go away, unless we invent a completely secure way of communicating and sharing information with eachother online
- In order to take some preventative actions, we need to be careful about what we post online, keep our software's updated and make passwords that are secure and different on different applications.

Q2



Congratulations!

Phasebook has survived four cyber attacks, thanks to you!

YOUR TITLE IS:
Cyber Champion
Rank 5/6
Total stars earned - 50

You've never met your match on the cyber battlefield. Protecting networks is second nature to you, and your career will be long and celebrated.

Improve your rank:

I managed to complete the different challenges.
The coding challenge where we would navigate through a maze was fairly simple in the beginning. As I got up to level 2 and 3 it required some thinking, but using the if/else which I have good experience with, I managed to complete the challenges.

The password-cracking challenge with “password duels” was pretty fun. It also got more difficult in level 3 especially, but it was nice to refresh on brute force attacks and it made me realize that some of my own passwords might honestly be embarrassingly easy to solve. The learning note from this challenge is to have strong passwords with different signs and to have different passwords for different applications, not the same one everywhere.

The social engineering challenge for me was the easiest one simply because of the fact that I receive these kinds of phishing attempts in my junk mail basically every single day, so to distinguish the phishing attempt from an actual message was pretty simple. The learning note from this challenge is to be vary of these kinds of attacks and never give up any sensitive information.

The network challenge was another fun one. Here we had to buy defenses to defend against a series of cyber-attacks. The learning note from this challenge is to realize the importance of security in big companies like “phasebook”. This is a company that relies on its availability and an attack like DDoS can have huge implications for these kinds of companies. So, to maintain good security, we must be aware of the different kinds of attacks and prioritize security so that we save ourselves from attacks that give us bigger consequences then they should have, had we invested in a good defence strategy early on.