CYBER171: Assignment 2

Lavanya Sajwan || 300381661

Question 1: Stealing the examination [20 marks]

Targets are the login details of any individual part of the ecs faculty, specifically can target Ian Welch. I know Ian's name, what courses he lectures, and am able to seek other information like his phone number, email and picture just by looking on the ecs website.

Steps I would give someone:

1. Seek information about the person you are targeting. In this case this is easy because as described as before a lot of information is on the ecs website.
2. Email from a fake account of a trusted place. In this case, email from the faculty. Make the username of the email semi match the email and they have to both seem as close as possible related to the faculty; e.g. ***ECS Faculty*** ecsfacultyvuw@gmail.com
3. Using this info, exploit the relationship by writing a long email explaining a fake scenario in order to get their login details to set the scene. Can exploit the network breach that occurred last year. Also keep in mind that spelling and grammar needs to be perfect as to not arouse any suspicions.
4. Go in for the kill; ask straight to the point while using a sense of urgency for the login details. "…due to this we **need** your username and login details in order to check whether you were part of the breach. There needs to be a response as soon as possible!

This process is called email phishing.

Question 2: Online marketplace purchases [10 marks].

Mechanisms:

1. Taking advantage of the trusting nature of humans. They felt as since the sellers were selling off "credible" websites they would be legitimate and they didn't have to be cautious making a payment.
2. They gained the confidence of buyers by opening American bank accounts so that people would feel more confident making a transaction to people within the states.
3. They took advantage of the fact that they were hidden behind a screen - people can't make accurate judgements in the absence of body language and speech signals through a screen.

Avoiding:

1. Thoroughly scan emails being sent.
   - make sure display name matches the email
   - if any links included look strange don't click
   - if grammar and spelling isn't accurate it is not legitimate
   - usually websites like PayPal don't send wire transfer information, you're meant to send directly through PayPal itself as it has a 100% fraud safety guarantee so if something does go wrong you can get your money back
   - if it used urgency nah fam
   - because they were imitating certain websites there should've provided valid contact details
2. They should've talked to someone directly so you could judge the situation based on how they talked back
3. Generally don't wire transfer large sums of money without seeing a face attached to the supposed name

4. Ask to view the products and ask a lot of questions about the products. If they were real sellers they would know a lot of information about the products

Question 3: Assessing Risk [10 marks].

Risk assessment occurs in the fourth phase of operations security process (but it ends up being a cycle anyway). During this stage the risks are ranked either qualitatively or quantitatively based upon their potential impact. While reading both articles they both come to the conclusion that humans underestimate risks that are in their control such falling in a shower, while humans also overestimate risks that are out of their control such as a plane crash. In the context of cybersecurity, overestimation can occur in the ranking of the risk network breaches if a company has had breaches in a shorter amount of time, thus manipulating the perception of how frequently they actually may occur in a broader sense and changing the possible "rank" in the qualitative process or the probability in the quantitative ranking. Underestimation can occur in events that don't occur frequently such as human data breaching. A way to automate ranking is being worked on in order to get around the flaws of quantitative and qualitative risk analysis.