Burrell, David 300209541
CYBR171 Assignment 2

Question 1.1:

Password: 123456
password strength checker: 1
how secure is my password: Instantly
the password meter: 4%

Password: qwerty123
password strength checker: 1
how secure is my password: Instantly
the password meter: 41%

Password: ncc1071
password strength checker: 3
how secure is my password: 2 Seconds
the password meter: 46%

Password: !@#$%^&*
password strength checker: 2
how secure is my password: 64 milliseconds
the password meter: 74%

Password: understandingbydivisionspite
password strength checker: 5
how secure is my password: 3 sextillion years
the password meter: 26%

Question 1.2:

Whilst they all agree that 123456 is the worst password, there is no unanimous best password of the 3, due to the different metrics used to give a decision. understandingbydivisionspite is vastly superior in 2 of the tests however, and with the password meter test it loses a lot for using consecutive lower case letters and only letters, changing it to understandingbydivisionspitE1 increases its score to 100%.

Question 1.3:

123456: 23,174,662 times.
qwerty123: 592,110 times.
ncc1071: 39 times.
!@#$%^&*: 2542 times.
understandingbydivisionspite: 0 times.

Question 1.4:

I would choose ‘understandingbydivisionspite’ simply because it has enough characters to make the task of brute forcing it take an exceptionally long time, and that it has not be pwned.

Question 1.5:

The simple risk is the same with putting your password anywhere untrusted, it may be taken. Password strength checker minimises this by using javascript and have it run client side so no information is send, and is stated by the author of the site to be trustworthy, but still not to trust it or him on principle. Have I been pwned is far more complicated as it needs to check your password against a source of pwned passwords, however the site has a long breakdown of the efforts and algorithms used to prevent your password being stolen.

Question 2.1:

Telegram: Yes it is encrypted by default, with additional client-client end to end encryption available.

Signal: yes it is encrypted by default, and even end-to-end encrypted by default as there is no other options.

Snapchat: Until recently it had not been encrypted in any way. Earlier this year they added end-to-end encryption.

Question 2.2:

Telegram: To avoid man-in-the-middle attacks telegram has secret chat end-to-end encryption and to verify your chat you can compare the encryption key image that ios set up between you and see if it matches or not.

Signal: Again this only offers end-to-end encryption and similarly to Telegram you can compare your ‘safety number’ or equivalent QR code with your chat partner.

Snapchat: unknown how to confirm, there is little information on snapchats encryption features.

Question 2.3:

Telegram and Signal: These are both open source programs, so all the code can be examined if need be, to confirm that they perform as stated and have no hidden features.

Snapchat does not have information available to the public in which these things can be confirmed, only good faith and Law.

Question 2.4:

I would recommend Signal from personal use, as well as endorsement from Edward Snowden.

Question 3.1:

The most obvious targets would be Ian or Harith, as we already have access to their usernames for logging in to the staff servers as well as a more personal connection to them to be able to manipulate.

Question 3.2:

The Password. Context in which target would be needing to log into the ecs portal via a phishing link

Question 3.3:

Have a phishing version of the website ready in which logging in is a must for continuing in completing the query from the source (any part of the course homepages should be enough). Redirect to the correct ecs website after logging in, having already logged the password.

Question 3.4:

Question 4.1:

Using co-conspirators to correspond with victims, using fraudulent certificates and information. Creating phony websites for fictitious dealerships. Using emotionally manipulative stories.

Question 4.2:

Because of the large amount of money being spent by the victims it would be believable that the affect heuristic of the victims would naturally be one leaning toward high risk thought processes, thus leading to elaborate and detailed pretexting being necessary on the part of the attackers in order to reduce the victims risk aversion and raise trust.

Question 4.3:

Look into the sellers history, look at reviews, try to find any negative view points at all. As hardly any online seller will have a perfect track record, having no negative reviews is rather telling.
The age of the account in question is worth looking at, newer accounts naturally are less trust worthy.
If possible check out the physical location of the business, or get a trusted person to do so if you have contacts in the city the seller is supposed to be from. Seeing the goods in person, or checking with a sellers business location should be proof enough of the object being real.

Question 5.1: