Harsahbaj Singh 146457221 hsna27@mySeneca.ca  
The following activity contains some real-life experiences and jokes, hope they are not regarded as unprofessional.

**Activity 1** of 2: **(50 marks = 4 × 12.5)**

1. Passphrase Manager

🡺 Advantages 1) With a Passphrase Manager we don’t have to worry about where we should store our passwords as they are all stored safely at one single place making it convenient and easy for us.

2) Secondly Passphrase Managers often come with browser extensions that can be used to fill in the credentials and passwords automatically making it easy for us and reducing time and errors while filling in the passwords.

🡺 Disadvantages 1) Passphrase Managers are usually 3rd- party apps, and 3rd party apps often come with potential security risks so if a manager is to be used then a proper background check of the software or the company that’s behind it should be performed and a reliable and safe option should be choose.

2) If we keep all our passwords at one place then it comes with its own disadvantage that if the password for the manager is compromised then we are doomed as all our passwords are in it. (Its like instead of having different keys for different lockers we just have one and the thief end up finding that single key 🔫)

2. Passphrase Generator

🡺 Advantages 1) Passphrase Generator can create complex passwords on its own which are not easy to crack and usually comply with all the requirements of a strong password, hence improving security considerably.

2) Passphrase Generators can save us time and effort as sometime some websites have special requirements as the password should have Uppercase and lowercase and also special characters, so generally making these types of unique passwords on our own can be a real time and brain consuming task. Generator on the other hand can easily give us a secure and requirement fulfilling password in a matter of seconds.

🡺 Disadvantages => Passphrase Generators give long and complex passwords which are difficult to memorise, so they have to be stored somewhere safely too and that gives an additional task. Giving a real-life example (I used passphrase generator on my Seneca password and now every time I try and login, I have to type a long password containing at least 4 types of different special characters, good thing is Seneca server asks us to put in the password about every single time so I have it memorised by now.)

3. Use single sign on where available

🡺 Advantages 1) Single sign-in helps as it helps by making an umbrella structure as we now only need one credential to login into all other sites eliminating the need to remember different credentials for different sites. (For e.g. Using google mail to sign in to Facebook will make it easy for us as the credentials for google and Facebook would be the same and time will be saved.)

2) It is also more manageable as there would be only one single point of user management and all the permissions can be managed from one single location.

🡺 Disadvantages 1) With single sign in the security of the single sign in account should be increased as we are getting access to different domains with the same account, thus creating a single point of compromise meaning if that single sign in account fails then all the accounts connected with it can be accessed too.

2) If for some reason the access to the main (single-sign-on) account is lost then it would result in user inconvenience and losing access to all the other accounts connected with it too.

4. What do you do to safeguard your passwords and digital life?

🡺 To safeguard my passwords and digital life I usually start with not creating passwords that could be guessed very easily and using as much unique characters I could possibly use and from now on after listening to my professor I would start using a space at random places as it makes it difficult to guess. Another way I do to store my passwords safely is that I have kept a small pocket diary hidden somewhere in my house on which I write my passwords randomly not writing any domain or something with it for someone it would just be a single diary with random gibberish as there isn’t any domain name or website but for me, I remember which password is for which website or account. (Don’t try and sneak in my house to find it though ⚠️)

Why is that (or why will that be) the best method for you?

🡺 It is the best method for me because I have been using it for years and luckily it have kept me safe until now and hopefully it will carry on to do the same. It also is not a complex method and helps me keep my sane.

Why won't you use other methods?

🡺The other methods would be really complex for me with additional stress as what If I lose access to my single login account or what if the third-party password manager I use is compromised, these methods also have a disadvantage of not creating memorable passwords which for me result in increased time at login stages because what if I wanted to login at some other device at some other country where I don’t have any access to my password manager.

**Activity 2** of 2: (50 marks for 250+ words)

🡺 **What is the price of free?**

There is a dialogue in me favourite movie of all time “JOHN WICK” which states that, ‘Everything’s got a price \*$%$%’ and the same goes for our online endeavours if the product is for free then we are the product. The price of free being our precious data from our choices to our addresses we are sending all our data to these free domains starting from the biggest culprit of all the mighty ‘Facebook’. Since its inception Facebook have been intitled with multiple controversies with Mark Zuckerberg fighting the Winklevoss Twins and now with the recent Data-theft charges all the these free sites are working on the model of selling our data to each other like in daily life we see if I am talking with my friend about dog food on Instagram then my feed on both Instagram and sometimes even twitter would be filled by sponsored ads of dog food. This phenomenon tells and proves of data theft as the chat which other wise should be encrypted and private are being monitored by the companies resulting in data theft. This also works in a way that we give all our details from birthday to address, credit card information to these sites feeding their algorithms to develop more like in the movie ‘The social dilemma’ they have perfectly picturized how these social media sites use our data and information against us to develop their algorithms to make us more engaged with their product. This also a matter of worry as these free sites are often subject to feeding a specific agenda to people social media sites are free for us but they sometimes in turn manipulate the ideologies of the census as there have been past accusations of how censorship and other things have worked time to time to change how people think about a specific incident, so in that way the price of free is us unwittingly experiencing a change in our thought process (attack on our free will) . To end it all nothing digital comes for free, the fees of free is our subconscious and privacy which we are surrendering everyday to these corporate giants which should remain unnamed.