Harshil Prajapati175255215 hprajapati8@mySeneca.ca  
Click or tap here to enter text.

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

1. Passphrase Manager

🡺 Advantages

1. It's quite beneficial if you have difficulties remembering all of your Passphrase because you only need to remember one Passphrase in order to access all of the Passphrase stored inside the Passphrase manager, so you don't have to worry about it anymore.
2. Passphrase manager also provides the auto fill passphrase feature which have to be enable by the user according to their need.
3. User can store multiple data like the important banking passphrase, credit or debit card pin, pin of your jewellery box(locker), all the passphrase of purchased applications or subscription and many more.

🡺 Disadvantages

1. Many websites do not allow any third party passphrase manager to auto fill the passphrase
2. It will be a big trouble If someone crack the password of passphrase manager then he/she have access to all your data and passphrase inside passphrase manager.
3. Many of the passphrase manager have the annual subscription so user have to pay some amount to use the service.

2. Passphrase Generator

🡺 Advantages

1. Generates strong password with the different characters which is next to impossible to crack easily.
2. User don’t have to take stress to create any new password which is also not easy to crack.
3. Most of the passphrase generator create more than one password so users can select which one is convenient for them

🡺 Disadvantages

1. Most of the passphrase which is create by the passphrase generator is not easy to remember especially when you are not using passphrase manager to store your passwords.
2. Sometimes cannot be able to match the certain criteria to make the passphrase.
3. There is always a chance that all the passphrases that are generated by the passphrase generator store the data to server and could be easily hacked.

3. Use single sign on where possible

🡺 Advantages

1. It makes the process streamlines that user can access to their applications very conveniently.
2. All the resources and data can be access by the user by just using one user id and password that means user don’t have to remember different passwords to access different resources.
3. User no longer have to stress about the reset their passwords because there is only one password that have to be remember to access all the data or resources.

🡺 Disadvantages

1. It takes a long time to setup a single sign on.
2. Users have to create a strong password because it will give access to all the data and resources so user have to take care that the password is strong enough that not easily crack.
3. It is trouble when use for more than one user it might be crash.

4. What method(s) do you use to safeguard passwords and your digital life?

🡺 As I belong from the developer background, so I have some knowledge about the binary numbers so for particularly me I use to convert all my password and digital life to the binary code and then store it anywhere in my laptop or maybe in my phone.

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

🡺this is just because not everyone knows about the binary digit conversion so by any chance if someone have the access of my laptop or phone where I stored all my passwords then he/she cannot do anything except he/she knows how to binary conversion which is very rare.

Why won't you use other methods?

🡺so basically, I do not use the other methods like to store passwords in a private folder which can be access by a master pin also to use some third party password manager to store my passwords because that are so outdated and majority of people use this methods and even a chance of easily hacked by the hacker so I prefer some different method to store my passwords.

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

🡺 **What is the price of free?**

Let's use Facebook and Instagram as an example. These platforms are essentially free for users, and they do not require payment to use any of their features. However, users are paying for these services by providing their personal information, which is risky in the event of hacking. Hackers can access all of the user's information, including email addresses, phone numbers, your age, and many other details, including on Facebook and Instagram Even on social media, people frequently share personal images and other personal items that hackers may exploit inappropriately. As a result, although the applications are free for users, they nonetheless indirectly pay a lot for them. Another issue is that these applications are open to everyone, making it possible for anyone to use them. As a result, hackers frequently publish links for shopping for fancy things and other content that might cause problems for users who click on them. Users who provide information about their digital banking may experience money fraud in many cases.

Let's use YouTube as another example. Although it is free for all users, YouTube users are unknowingly paying for the service because many users encounter advertisements between their videos. These advertisements can be for anything, from new gadgets to delicious food, and they frequently convince users to order the advertised item even if it is not necessary. There are numerous instances where customers purchase food that is not worth the money simply because it looks wonderful and delicious. It might risk the health if this happen very frequently and also this can be consider the indirect way to pay for the free.