Patel vrundaben Vijaykumar158605220 vvpatel20@mySeneca.ca  
Click or tap here to enter text.

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

1. Passphrase Manager

🡺 Advantages

One of the advantages of using a passphrase manager is that it helps us to create a password which is easy, long, random and strong with uniqueness. Secondly, it also provides us a great security by storing our passwords and credential for different accounts safely using strong encryption. Thirdly, it is timesaving as passphrase manager auto-fills in the password hence there is no need to remember or type the long passwords. Lastly, it works on multiple devices by storing the password of a particular account on different apps and browsers on another device hence if the password is updated, it immediately saves the password on the other devices too.

🡺 Disadvantages

One of the main disadvantage of using a passphrase manager is that if you forget or lose your master password, it can lead to a single point of failure as u can probably lose the access to all of the accounts at once whose passwords were managed by the passphrase manager hence it is always recommend to use a strong but also a memorable master password. Secondly, if one day the passphrase manager becomes unavailable due to technical issues, you might lose access to it hence you may lose your important information if your master password is not strong enough hence it gets hacked. Thirdly, some of the passphrase manager does not support some devices and browsers where it only supports two to three browsers mostly the google chrome, Microsoft explorer and Microsoft edge which limits us to use the other browsers of our choice hence we have to fall back to the browser we don’t like.

2. Passphrase Generator

🡺 Advantages

The advantages of using passphrase generator one is that it creates a secure and complex passphrase that is long, random, and strong which follows an algorithm of uppercase, lowercase, numbers, and special characters, that it can be difficult for hackers to guess or crack it. Secondly, it creates passphrase of different combination of random characters for different accounts hence it does not repeat the passphrase of one account for all other accounts and due to this there is no risk of affecting other accounts if one passphrase is forgotten. Thirdly, we don’t need to remember the long and complex passwords for the different accounts as the passphrase generator automatically creates the passphrases hence it leads to reduce of risk of creating weak passphrases that can easily be cracked by the hackers.

🡺 Disadvantages

one of the disadvantages of using passphrase generator is that if one day the passphrase generator becomes unavailable due to technical issues, you might have trouble to access the accounts as the passphrases created by the passphrase generator were hard to remember as they were complex and random. Secondly, some platforms may not allow the passphrases that are created by the passphrase generator as they might have some specific restrictions about character limit, not allowing some special characters.

3. Use single sign on where available

🡺 Advantages

One of the advantages of using single sign on is that it saves our time where we do not need to create different usernames and passphrases for all the different accounts, we can just have one user ID and passphrase and use it for several accounts. Secondly, we do not need to stress our minds to remember the user ID and complex passphrases for all the multiple accounts as we can just use one user ID an d passphrase for all the accounts. Thirdly, users can move between different applications without verifying the login detail repeatedly, once it is authenticated, for example we can access between Seneca resources, Seneca apps and websites once a student authenticates on the Microsoft authenticator by providing the code that pops up on the smartphones hence it also improves on security issues as we first use stronger authentication methods to login such as biometric authentication.

🡺 Disadvantages

One of the disadvantage of using single sign on is that if a person fully relies on it and one day it might suffer a technical issue where we might lose access to multiple platforms or apps. Secondly, due to any technical issue that affects the single sign on, we might lose access to all the accounts as we used one login details for several accounts which can lead to a single point of failure. Thirdly, if the hacker cracks the login details or account gets targeted, all the linked resources might get exposed as it uses only one set of credentials for all the accounts also if the apps does not use MFA then they are also jeopardized.

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

🡺To safeguard my passwords and digital life I always create my passwords that are very strong and complex which are combinations of uppercase letters, lowercase letters, special characters and numbers where I always avoid the common passwords. Secondly, I use passphrase manager which creates a strong and complex and random password for my accounts and helps me to autofill my login details on different browsers and apps. Thirdly, I always keep my Two-factor authentication enabled as it adds more security to my accounts.

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

🡺Enabling the Two-factor authentication is the best method for me because it makes my account more secure because when I try to login on other devices or apps it pops up a code on the screen and also sends notification on my phone where I have to access that code and scan my biometrics to further allow me or someone to login in the account hence if someone else tries to login, it will send me code with notification where I can just not allow them to login hence it reduces the risk of unauthorized access.

Why won't you use other methods?

🡺I wont use other methods because maybe some passphrase that are being created are weak and not strong enough which can be easily guessed by the hackers leading to expose of information and data. Also some passphrase generator creates a single passphrase that are used for all the accounts hence when there is a technical issue, a single point of failure can happen. These methods aren’t strong enough to survive the hacking techniques of today’s world.

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

🡺 **What is the price of free?**

Many current business websites provide us with free content but in return for personal information. Although many of us do so by signing lengthy and complicated terms and conditions contracts, but we do not see that they are asking us for our personal data in return. For example, Google keeps tracking our personal data in the chrome browser. When people originally joined Facebook, who in their right mind realised they were agreeing to this kind of surveillance? Although Facebook is free, but our privacy is what we pay with. Facebook also continues boosting the cost. Facebook claims that to target its users, it suggests ads and groups to join using the data it received from other businesses on its feed. Most people use social media like Facebook and browsers like google to find news and information online where when we click on the links that are provided by them, they automatically earn money there. Facebook may potentially utilise our activities to guide us towards communities that influence our political views or even our opinion of the coronavirus vaccination. It might utilize our life to develop its artificial intelligence, examine how people use websites and mobile apps, or for any other new application it could come up with in ten years.

The main issue with monopolies is that they provide users few viable options. We do have the choice to "disconnect" some of this information from our account via the disconnection of off-Facebook activity. But this does not imply that Facebook deletes our data, rather, it just stops using it to target us with advertisements throughout the Internet. Now, Apple started allowing iPhone users to instruct applications not to track them which limited Facebook's ability to obtain data from apps that don't also have access to our email address or phone number. For Android phones, Google has promised a similar setting, although both of it are temporary solutions.