Mohdeep Singh109600239 msingh820@mySeneca.ca  
Click or tap here to enter text.

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

1. Passphrase Manager

🡺 Advantages

1. Enhanced Security: This help improves security by generating complex, strong &unique password for online accounts.

2. Convenience and Easy to use: if we use this, we just need to remember single master password to access all our passwords. Passphrase manager also automatically filled all the login credential. We don’t have to type again ang again.

3. Cross-platform sync: Manager typically offer synchronisation across multiple devices & platforms.

This means we can access our passwords though any device or platform.

🡺 Disadvantages

1.Single point failure: Since passphrases manager store all the passwords in one central database, if someone get the control of the manager, it could lead to so many troubles. Its like lottery for the other person who is trying to get in your computer.

2. Trust in the provider: We always must make sure that we are installing the password manager from a reputed site or firm as we are giving the most important information to handle.

3.Cost and subscription: While some of the password managers are free of cost but most of them charge fees.

2. Passphrase Generator

🡺 Advantages

1. Complex and strong password. Passphrase generators generate unique and random password for each service we use. This makes hacker or another unauthorized person hard to guess the password.

2. Time Saving: Creating and logging with a strong password manually can be time consuming and lead to frustration. Passphrase generators fill the blanks in one click. This saves a lot of time.

3. Avoidance of personal information. A lot of people use their personal information while using password. This could be a problem as it can be easily guessed and obtain.

🡺 Disadvantages

1. Dependency on generator. If I synced all my passwords with the passphrase generator and somehow if I don’t have generator or forgot the master password, then I can’t login to any of my account. Its hard to remember long and unique password.

2. Overreliance on Generated Passwords: Although password generators produce secure passwords, some users may get comfortable and stop using other security precautions in favour of just using generated passwords. The generated passwords should be used in conjunction with additional security measures including two-factor authentication.

Passphrase generators might not be available everywhere or compatible with every type of computer, operating system, or application.

3. Use single sign on where available

🡺 Advantages

Here are some key points advantages of Single sign on

1. Convenience for users

2. Saves Time and Efforts

3. Enhanced User productivity by focusing on the work rather entering login credentials again and again.

4. Cost saving

🡺 Disadvantages

Here are some key points disadvantages of Single sign on

1. Single point of failure. If one main password is compromised, all the account will be on high risk.

2. Limited compatibility. SSO may not be available with all applications and websites.

3. dependency of third-party providers. Users must rely on third party providers while sharing their information. Unauthorised access to several websites and applications may result from any breaches or vulnerabilities in the provider's infrastructure.

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

🡺

1. Password Manager

2. Strong and unique passwords

3.Regular passwords updates.

4. Keep software up to date

5. Use antivirus and firewall protection

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

🡺 to make sure my passwords are secured I use.

A good password manager like 1Password

And a smart antivirus and firewall. Norton Antivirus

Why won't you use other methods?

🡺If I use a good and secured password manager, I don’t have to worry about all other things.

My password manager will take care of everything from smartphone to laptop.

It will make life easier and much faster. I don’t have to memorise long passwords and typed every time.

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

🡺 **What is the price of free?**

"If you're not paying for the product, you are the product," is a widespread viewpoint on the economic structure of many internet services and platforms. It implies that those platforms capture, analyse, and monetize our personal data, behaviours, and preferences while we utilise free goods and services. This created the hyper-personalization era, in which businesses use user data to offer experiences that are highly customised and focused. Let's explore the subject in more detail.

-> Free Products and Data Collection: Businesses frequently use free goods and services to compile huge amounts of customer data. This data consists of details about surfing patterns, search history, interactions on social media, and more. Insights into user behaviour, tastes, and demographics are gained through the collection and analysis of this data by businesses, which may then be utilised for a variety of things, including targeted advertising.

-> User Data Monetization: Businesses use the user data they gather to make money through targeted advertising, individualised suggestions, or data sales to third parties.

-> Security and Ethical Issues: The hyper-personalized world brings up significant privacy and ethical issues. Users could feel unhappy knowing that their personal information is being gathered, examined, and utilised for business purposes without their knowledge or consent. User security and privacy may potentially be put at risk by data breaches or corporate misuse of personal information.

In conclusion, in the age of digitization, the price of "free" goods or services frequently involves the exchange of personal information. In exchange for access to these free services, users submit their data, which businesses then profit through hyper-personalization and targeted advertising.