Table of Contents

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

***Activity 2*** *of 2: (50 marks for 250+ words)****………………………………………………………..………………………………3***

[Citation 3](#_Toc137409749)

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

1. Passphrase Manager

🡺 Advantages

a. Passphrase managers are secure and reliable because they store the information given by the uses in encrypted form.

b. Passphrase managers are better than humans because human memory can forget a lot of passphrases, but a passphrase manager remembers all passphrases. (M.J. KELLY, 2019)

🡺 Disadvantages

a. Passphrase managers have a single master passphrase which is used to access all the passphrases stores in the passphrase manager, any other person knowing/accessing that master passphrase can lead to some serious trouble.

b. While using a Passphrase manager, an extra step is added while getting to log in to your account. Every time you login an extra access is needed by the passphrase manager in order to grant you access to that account. (Thepsiri, 2022)

2. Passphrase Generator

🡺 Advantages

a. Passphrase Generator generates a random passcode containing various alphabets, numbers and symbols which helps in creation of a strong passphrase.

b. With the help of Passphrase generator, each and every website can have a different passphrase which can help in protecting rest of the accounts if one is hacked. (The Complete Guide to Password Generators – What They Are and Why You Need One, 2022)

🡺 Disadvantages

Passphrase Generators generates different long random passphrase for different log ins. In case you don’t have access or don’t remember the passphrase, then it is very difficult to recover the account.

3. Use single sign on where available

🡺 Advantages

a. Using single sign on leads to less need and less creation of passphrases for different accounts which means having a single strong passphrase for the sign on provider can be of great security. (Stokes, 2017)

b. Often, the sign on provider is big resourceful corporation having the capital for security research which means the master passphrase’s security is not compromised.

🡺 Disadvantages

a. Using a single sign on feature means that the passphrase that is being used to sign on to that account should be very strong, secure and reliable. In case, if that passphrase is exploited, then on each account login is made with that account is on the risk of hacking.

b. In case the user wants to do a guest login or wants to use private mode, then logging in to accounts is not possible without accessing the single sign in account.

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

🡺 In order to safeguard my passwords and digital life, I use a password manager (1Password), which stores and generates strong passwords for me.

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

🡺 For me using a password manager is the best method of being safe online because by using a password manager and password generator, I don’t rely on my memory to remember all the strong, randomized passwords created by the random password generator.

Why won't you use other methods?

🡺 I don’t use any other methods because I think using the password manager is the most reliable and best possible way to store/generate passwords and be safe online. By depending on my memory, I can forget some of the passwords later on and by using a single sign in option, I find it difficult to login where I haven’t already used/accessed the single sign in account.

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

🡺 **What is the price of free?**

Since the ancient times the word free stands for without any price or charges, but in the modern times capitalistic world has changed the notion associated with this word and now it is a saying that, “if you don't buy the product, you arethe product.”

In the era of internet, advertisement is the main source of revenue for most of the big tech companies and in order to maximise their profits, these corporations have started to collect user’s data to be as specific and personalized as possible to increase the click through rate of these advertisement banners and generate more profits. Sometimes the data collected by these corporations is further sold to many companies in return of some profit/capital. John Lanchester once wrote in an essay, "Facebook, in fact, is the biggest surveillance-based enterprise in the history of mankind. It knows far, far more about you than the most intrusive government has ever known about its citizens. It's amazing that people haven't really understood this about the company. What Facebook does is watch you, and then use what it knows about you and your behaviour to sell ads. I'm not sure there has ever been a more complete disconnect between what a company says it does – 'connect', 'build communities' – and the commercial reality." (Elizabeth Renzetti , 2017)

Moreover, some of these so-called free applications and websites are just a compromised version of a paid version which is also being sold by the company. In order to increase the sales, slowly and gradually when users are hooked to the free version of that app, the company decreases the features associated with the free version and asks for a price for the feature that used to be free (Example: The verification mark on the Twitter app used to be free, but now it has a subscription model and users have to pay for being verified as a human).

To summarise, I just want to say that in this world there is nothing as a free product, if you have a choice, often you should choose the one having some price to pay because by doing that, the revenue of that product is through the direct payment made by you and not by your data which is being collected by the application.

# Citation

Elizabeth Renzetti . (2017, September 16). *Facebook, you’re like a bad boyfriend and it’s about time we break up.* Retrieved from The Globe and Mail: https://www.theglobeandmail.com/opinion/facebook-youre-like-a-bad-boyfriend-and-its-about-time-we-break-up/article36281554/

M.J. KELLY. (2019, October 8). *Five myths about password managers.* Retrieved from The Mozilla Blog: https://blog.mozilla.org/en/privacy-security/privacy-security-tips/myths-about-password-managers/

Stokes, N. (2017, May 6). *Should You Use Facebook or Google to Log In to Other Sites?* Retrieved from Techlicious.com: https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/

*The Complete Guide to Password Generators – What They Are and Why You Need One.* (2022, December 19). Retrieved from Passcamp.com: https://www.passcamp.com/blog/the-complete-guide-to-password-generators-what-they-are-and-why-you-need-one/

Thepsiri, T. (2022, October 28). *3 Advantages And Disadvantages Of Password Managers.* Retrieved from Kelsercorp.com: https://www.kelsercorp.com/blog/password-managers-pros-cons-advantages-disadvantages