🡺  **Your name: Amirhossein Sabagh**

**Student No.: 152956199**

**UserID: asabagh@mySeneca.ca**

Passphrase Manager

🡺 Advantages

With password managers, we reduce the risk of forgetting passwords; we do not need to memorize all of our passwords and take the risk of forgetting one when we want to login to a website. Our minds are not capable to memorize complex passwords with a lot of characters and/or having special symbols; therefore, if we want to rely on ourselves to remember the password, we mainly pick simple and short passwords and it is highly possible that we use the same passwords for multiple websites. With password managers, we can easily create more complex and longer passwords and do not worry about remembering them. The password managers also save us some time as we don't need to type in the password every time that we want to log in. Added to those mentioned, some of the password managers are able to store out credit card information as well.

🡺 Disadvantages

Trusting password managers is possibly the most important concern we have for whether choosing them as our safeguard or not. When password managers were first introduced to the public, people didn't trust them at first and were hesitated; but these platforms proved themselves as time has passed and made a good reputation for their security.

The password managers use a master password to give you access to their platforms. If we lose the main password or if hackers get access to it, we technically have given all of our credentials away. Another drawback to password managers is that they might not support all of our devices and browsers; we have to install the password managers app or software in every device we have.

Passphrase Generator

🡺 Advantages

The great thing about using passphrase generators is that they can create random long passphrases that include small or capital letters alongside digits. They can save those passphrases for us and act as a password manager. With passphrase generators, we can use a new password for every website and we don't need to use the same password over and over just because we cannot remember all those passwords.

🡺 Disadvantages

The passphrase generators can be hard to trust. Some of the fraud websites just generate a small number of new passwords, so they would be able to access our accounts later on. It is always better to generate the password for about 6 times and then use the passphrase generated for us. Another thing about passphrase generators is that they do not really do a hard thing and the passphrases they generate are mostly simple, but long, the combination of words. The passphrases do not include special characters as they have to be meaningful. We can create passphrases ourselves and therefore, cut the hand of the third website and reduce the privacy risk.

Use single sign on where possible

🡺 Advantages

Using SSO can reduce password fatigue. It makes our lives easier to remember one password instead of many. This way, we can come up with a much harder and longer combination for our single password. Using SSO simplifies everything: it improves identity protection, increases the speed as websites, especially larger ones like the hospital or government websites, do not have to deal with dozens of passwords in their databases. SSO is more secure, too.

🡺 Disadvantages

The same thing with the password manager happens with SSO; if the SSO account gets hacked, other accounts that were under the SSO's authentication will also get hacked. Another flaw to SSO is that when it is down, access to all connected sites would be stopped, too. Added to challenges mentioned, SSO is a little bit trickier to set up; it may need some advanced knowledge and even though the steps are explained, could result in errors and disappointment.

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

🡺

I use my web browser's password manager (Opera) for remembering my passwords and I set up the two-authentication if a website has one. I also have downloaded and set up some applications like Google authenticator for some of my more important accounts.

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

🡺

I won't pick a password for the websites that I know I will be using less often or are at risk of being a fraud; for those websites, I use the suggested password of my web browser.

When I want to check I did everything right, I try to see it from a hacker's perspective; "how hard it is to hack this account?" Then I try to find the issues and solve them.

My strategy for picking a complex password and setting up two-authentication or third-party applications is connected to the importance of that account. The more important the data in that account is to me, the more complicated it would be to crack my password

Why won't you use other methods?

🡺

The one thing I do not like about myself is that I don't rely on password managers or passphrase generators; I pick my passwords myself and sometimes use the suggested password. This activity showed me some great articles about password managers that lessened my fear and comforted me a little; I will probably choose one password manager and use it in the next days.

**🡺 What is the price of free?**Discuss and [*argue*](http://theconversation.com/no-youre-not-entitled-to-your-opinion-9978) your point of view in 250+ words. Before writing, see below; there is much food for thought.

🡺

Most of us believe that big internet companies like Google or social media platforms like Facebook, Snapchat, Twitter, and Instagram or messengers like WhatsApp and Telegram are free and we use them without paying a cent; the truth, however, is something different. Indeed, we are not Google's or Facebook's customers and the real customers are the companies that pay to advertise themselves by paying for the ad space; google has Google Ads, YouTube displays advertisements before and while playing a video for us, and Facebook has various ad popups in different locations of the website. The thing is that the real profit of these famous companies is not from the ads that they are showing to us; they take our data in exchange for the free service they are offering. They have gathered a vast database of personal information and that's what matters to them. These companies sell these data to other companies for a great amount of money and make their profit from that (not to mention the money they have made from selling crucial data to the governments). Not to judge unfair, I have to also add that although these companies have access to our personal information, they are obliged to not misuse them for bad purposes and they only use the data that will help them to provide us a more friendly environment. An example of selling our data for good purposes would be selling the information to the companies that have a special marketing target in mind and want to find the perfect customers for their products. All things said, maybe it was worth it to pay for using the services of these companies; therefore, we would engage less with interrupting advertisements and the companies would also treat our personal information with more care and respect.