Name: Nicholas Defranco

Student id: 106732183

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

1. Password manager

Advantages & disadvantages

Pros

You only need to remember one password A.K.A. the “strong master password” (Malaika, 2016) which authorizes you to access and manage the rest of your passwords. Password managers also auto generate a password when it realizes that you are creating a new account to a new website. There are generally very easy to use. The password database is encrypted, where the only way it can be decrypted is with your key which is password.

Cons

If a user is using a password manager that comes with a browser such as google smart lock, a malicious attacker can capture all the keys someone has typed to log in into there account, and from there the attacker has access to all the user’s accounts (Lindros 2017).

<http://www.centurylinkbrightideas.com/pros-cons-password-managers/>

How will this avoid the reuse of the same password on different sites? ﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿

When you attempt to create a new account on a new website, the password manager will automatically create a randomly generated long password that you can use as your password will be saved in the password manager for the future when you plan on logging in again. Dashline does this as mentioned by Nicholas Malaika.

How will this help you remember different passwords on different sites?

If the user is authorized, it can auto fill user name and password forms for you when it realizes you are returning to a website that you have already have an account for. This is very convenient because all the user must do is press the enter key.

If you (will) use this, why so? If not, why not?

I will use this because it is very intuitive, it notifies you of password strength of existing passwords you store in there. If dashlane realizes the password is easy to crack, it will recommend you create a new password. This can easily be done as there is a feature that lets you create a newer stronger password (long) which is auto generated. According to Malaika, dashlane uses Amazon Web Services which is very reliable and secure. All passwords are organized in a database easy for a user to change at any time. A password manager is perfect to protect login information to various websites. It also encrypts your passwords, so the only way passwords can be accessed is with the password for the entire database which means the company that owns the service cannot access your data unless they know your password.

<https://blog.dashlane.com/a-skeptics-guide-to-password-managers-and-security/>

1. PassPhrase
   1. Advantages & disadvantages?

Pros

Spaces in passwords are not often allowed so it would be least expected to be used in a password. When they are used it is difficult to crack them as the whitespace character is hard to work with.

It avoids the need to think of a random password since humans cannot do that, they like to enjoy to keep things simple but predictable since “language is predictable” (Lee 2015).

\*\*\*extra\*\*\*

When I was completing an assignment for my C programming class, I came across a problem where whitespace by default was taken as a delimiter. We had to learn how to stop the standard input from doing that. So it makes sense why sites do not allow it very often.

Cons

There are not helpful for logging into online websites as crackers can monitor keystrokes. That means a lot of wasted effort someone did for a website password (Lee 2015).

* 1. How will this avoid the reuse of the same password on different sites?﻿﻿﻿﻿﻿﻿﻿﻿﻿﻿

Using a passphrase is far easier to remember as they are not cryptic to a human reader. Making is easy to remember passwords as they are very close to sentience’s in an actual language.

* 1. How will this help you remember different passwords on different sites?

The passwords are very close to an actual human language (English) making them easy to remember. Yet they are surprising difficult for computers to crack since whitespace is very uncommon and the more words that are added the amount of guess the computer has to make increases exponentially (Lee 2015).

* 1. If you (will) use this, why so? If not, why not?

I will use this, because having a passphrase is hard to crack due to the length of passphrases compared to passwords which is much shorter. These passwords are created yourself and not with a password generator which could possibly be pseudo-random created passwords. You also do not need to pay for a service or even trust a service to manage and create passwords. It is very simple process that anyone can do to create a strong password yet easy to remember as it will not include known phrase to any other person (Reinhold 2018).

They are good for encrypting anything that is local on your device since a cracker can track keys on a website form using various types of malicious JavaScript code making the whole process useless (Lee 2015).

<http://world.std.com/~reinhold/diceware.html>

<https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>

1. I already have a User ID and Password!   
   ==> use OpenID Connect or OAuth 2.0 or SecureKey (your bank credentials)
   * What are the advantages & disadvantages of signing on to various sites with your Google or Facebook account or bank credentials?

Pros

It is easy to log into a new website by using an existing account. It is easy to recall your account since it has the exact same information as a previous account that was made already. Developers also do not need to worry about storing passwords in a database, as they will only need to verify the information as the account comes from another source (Lightfoot 2016).

Cons

Since it is only one account being used to log in, if it is used on a website with poor security and it gets cracked, it will crack all your account information and identity for all the sites you used the same account for. Your main account whether it is a social media account or a google account etc. (your main account), shares information and receives information from the other sites. This information is used for mainly advertisements in the social media, which is given to companies that will advertise their product to you.

* + <https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/>
  + See <https://spin.atomicobject.com/2016/05/30/openid-oauth-saml/>

Do you have another approach to managing your credentials on all your online accounts? If so, what is it, and why do you use it instead of other approaches?

This is not a different approach but thought it would be worth mentioning

I personally use google smart lock to manage my passwords as I use google chrome as my main browser which always prompts me if made a new account, whether I want to save my user name and password for a website. This can also occur if I am logging in and I haven’t saved the password at all (whether it being I never logged in using my google account or never gave google an answer when they prompted me). I found it very useful because it can auto complete forms for me and all I am required to do is press the enter key when I want to log in. I must be logged in into my google account to account first. In the password setting in the chrome settings, you can view all the accounts with their associated website that google is storing. One interesting thing is, even though I am logged in into my google account I cannot see my passwords by default unless I press the eye icon which then it prompts me for my Microsoft account information, adding an extra layer of security.

**Activity 2**: **What is the price of free?**  
**Discuss and *argue* your point of view in 200-250 words.** (50 marks)

**If you're not paying for the product, you *are* the product.**

* Is using Facebook, Google, SnapChat, InstaGram, etc. really *free* to the end user?

No, it is not free. When we hear the word free, we think about the monetary value of something. However, it has a deeper meaning in this context. This is because these companies still need to make money. It is not free because they implicitly charge you for your privacy. You give them information about you, such as your browsing history on the site, who you like and follow. All this information is given to advertising companies which will advertise products based on the information that was given to them (Stokes 2017).

* Who owns the content of your life?

Only the end user owns the content of their life as it is their identity. Large corporations do not care for the privacy of their users even if they may say they do. They take it to make a profit. However, an identity is unique to one person.

* Is the benefit you gain worth the bargain? Are your sure what bargain is?  
  *Cui bono?* A Latin legal term: For whose benefit?

No, the benefit is not worth the bargain, as all the user appears to get out of it is advertisements which could annoy users. Depending on how often they show up on the screen. However, it is the only way to get access to their applications. Many average users are unaware of the bargain that they agree too as they believe that the application is free, so it is a win on the user, however Tim Berners-Lee mentions that we give data to the companies which they have full control over. They could sell it to another company, give it to the government and so on. This business model clearly benefits companies.

* Does using social media create a security hole and/or an opportunity for identity theft?

Social media creates a security hole because people can be watched 24/7 which is an issue because companies can find out a lot of personal information such as your schedule in the day, such as knowing all your posts online. This kills freedom of speech and people can be tracked if people say something controversial about a certain topic (Berners-Lee).

Continuing my point, taking info from part 1 section 3, people who use the same account on multiple sites can be vulnerable. If the other site has weak security. If their account gets cracked because of it. They can do very malicious things like sell your data on the dark web.

As you mentioned: “You are posting your life on the internet” (Mckenna, Week 10, slide 13);

* Is what Facebook and Google *do* consistent with what they *say* they do?

Google and Facebook’s goal are to provide a very good user experience. They always try to make their applications and websites easy for the user use. They want to make sure that even people who are not very savvy can understand the applications to allow a broader audience to use their products. However, according to Tim Berners-Lee, the companies hide important information in the terms and conditions about sharing personal data about their users to other companies and sources. They try to make it hard to let the average user understand that their data is being used by a company to make money.

References

Malaika, N. (2016, May 2). *A Skeptic’s Guide to password Managers and Security. Retrieved Nov 14th, 2018 from* [*https://blog.dashlane.com/a-skeptics-guide-to-password-managers-and-security/*](https://blog.dashlane.com/a-skeptics-guide-to-password-managers-and-security/)

Lindros, K. (2017, May 12). *The Pros and Cons of Password Managers. Retrieved Nov 14th, 2018 from* [*http://www.centurylinkbrightideas.com/pros-cons-password-managers/*](http://www.centurylinkbrightideas.com/pros-cons-password-managers/)

Reinhold, A. (2018, Oct 19). *The Diceware Passphrase Home Page*. *Retrieved Nov 14th, 2018 from* [*http://world.std.com/~reinhold/diceware.html*](http://world.std.com/~reinhold/diceware.html)

*Lee, M. (2015, Mar 26). Passphrases That You Can Memorize – But That Even The NSA Can’t Guess. Retrieved Nov 14th, 2018 from* [*https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/*](https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/)

*Stokes, N. (2017, May 6). Should You Use Facebook or Google to Log in to other Sites?. Retrieved Nov 14th, 2018 from* [*https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/*](https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/)

*Lightfoor, J. (2016, May 30). Authentication and Authorization: OpenID vs OAuth2 vs SAML. Retrieved Nov 14th, 2018 from* [*https://spin.atomicobject.com/2016/05/30/openid-oauth-saml/*](https://spin.atomicobject.com/2016/05/30/openid-oauth-saml/)

Berners-Lee, T (2017, Mar 12). *Tim Berners-Lee: I invented the web. Here are three things we need to change to save it. Retrieved Nov 14th, 2018 from* [*https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet*](https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet)

Berners-Lee, T (2017,Nov 16). Tim Berners-Lee on the future of the web: 'The system is failing'. Retrieved Nov 14th, 2018 from <https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality>