Our digital lives allow us to access the world’s goods and services from anywhere. Consequently, we have an overwhelming number of accounts for which we must remember ~~passwords~~ *passphrases.* What are you doing to safeguard your digital integrity?

**Best practice is to have a unique, long passphrase for each account.   
Argue for and/or against the following potential solutions.**

Use a passphrase manager like LastPass, 1Password (Canadian), Bitwarden (Open Source)

* + <https://blog.mozilla.org/firefox/myths-about-password-managers/>
  + Google: [password manager comparison 2019](https://www.google.ca/search?q=password+manager+comparison+2019) (skip the ads)

Passphrase Manager

🡺 Advantages

Think of it as a safe where our passwords are collected. We have to open the safe to view login information, which takes additional steps for password managers to lock our safe and keep it safe from cybercriminals. Hackers cannot steal passwords because they do not know the primary password. Depending on the password manager, the login information is stored on the local computer or on a remote server running by the password manager and is kept safe. We don't need to look back when we forget our login information. Because it is installed on all devices and automatically fills in the password. We can create a strong and secure password using the password manager.

🡺 Disadvantages

It takes time to record all credentials in the password manager. The more log-in information we use, the more it will bother us.

Diceware and other strategies can be used to generate long passphrases and/or random answers to security questions.

* + <https://en.wikipedia.org/wiki/Diceware>
  + <http://world.std.com/~reinhold/diceware.html>
  + <https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/>
  + E.g. <https://www.rempe.us/diceware/#eff> to generate random PassPhrase Or [random.org](https://www.random.org/integers/?num=6&min=11111&max=66666&col=1&base=10&format=html&rnd=new) and <https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt>

Passphrase Generator

🡺 Advantages

Powerful password generation is possible. This makes it difficult for hackers to steal passwords. Also, users don't have to waste time thinking about combinations that can be difficult to guess.

🡺 Disadvantages

It's really hard to find our passwords again when we forget them. Because it made the password very difficult, it can be solved by finding the existing password or changing it to a new one, which also wastes a lot of authentication and time. If we generated a password with an online tool, our password could be stored online. If I save my password online without saving it myself, there is a possibility that I will be exposed to the risk of another hacking. In addition, each tool has a password feature that can be created, and it may be possible to look for other tools when it is created that do not match the characteristics required by each site or document.

I already have a User ID and Pass~~word~~phrase! Sign on with Google or Facebook or bank credentials rather than having an account for each website. This is also known as Single Sign On.

* + <https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/>
  + <https://www.itworldcanada.com/article/mobile-industry-organizes-to-unseat-facebooks-digital-identity-dominance/403809>
  + [Single Sign On issue](https://www.wired.co.uk/article/facebook-hack-beach-single-sign-on-social-login)
  + See <https://spin.atomicobject.com/2016/05/30/openid-oauth-saml/>

Use single sign on where possible

🡺 Advantages

If we set a different password for each site, it would be very hard to remember these. Also, if we forget the password, we have to waste time to find it again, which we can solve if we use single sign-on. The convenience of users will be greatly increased and security will be enhanced. In addition, operating expenses for login information can be saved, and everything can be managed with one login so that it can be managed efficiently.

🡺 Disadvantages

Because we connected other sites with one ID and password, if this login information is hacked, it is highly likely that all connected sites will also be hacked. If SSO's own server fails to function, other connected sites will also be inaccessible. In addition to hacking, the more we connect sites and sites with one login, the more our profile goes to the site administrator, which means that our privacy can become more and more public. For example, if I look at what I've searched for and I can see a search-based advertisement on my screen on another connected site

What do *you* do [IRL](https://www.google.com/search?q=irl)?

* + <https://howsecureismypassword.net/> 🡨 open source [project](https://github.com/howsecureismypassword/hsimp)
  + <https://tech.co/password-managers/how-secure-is-my-password>

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

🡺

I usually use software called Google Authenicator (Google OTP). In addition to entering the first log-in information, I receive 6 to 8 digits of disposable password and enter it at every login to use Google service and log in to other sites.

For sites that cannot use Google OTP, I tend to make passwords very difficult. It protects passwords and digital lives by combining capital letters, case letters, symbols, and numbers

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

🡺

Choosing a secondary login method makes the login method more difficult because it can protect my information strongly. Hackers won't be able to hack into my ID, especially since I have to enter my temporary password at the second login. The more difficult the login method is, the more stable it is.

Why won't you use other methods?

🡺

I didn't know that there were other ways to protect my login information. Also, because I am a student, I don't want to spend money on a company that manages my login information.

**Activity 2** of 2: (50 marks) **"If you're not paying for the product, you *are* the product."**   
**🡺 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.

🡺

There's no such thing as a free lunch. Except for the concept of ' volunteer service', all actions are done to benefit. Many people think that the platforms we use, such as Google, Facebook, Instagram, and YouTube, are free to use. But do they really serve us without any benefit? I'm sure not. We sign up as a member using the platform, and here we notify you about the protection of personal information through the terms and conditions of service. However, most users, including myself, sign up after agreeing to collect personal information without reading the terms and conditions. From here we're actually selling our information to them. Because we agreed. The platform then collects our personal information in the name of showing more relevant search results, connecting with people comfortably, and helping to share more quickly and easily with other users to better serve all users. And link this information to advertising. Platforms collaborate with advertisers. And based on the information and searches collected, they show us the advertisement accordingly. Then we are exposed to advertisements even if we don't want to.

Additionally, the U.S. IT media Recode reported the results of an analysis by advertising market analyst Zenith. "The U.S. digital platforms such as Facebook and Google are expected to attract $106 billion from companies this year for advertising costs," Ricord said. Divided by the number of U.S. adults (250 million), it amounts to 420 dollars per person per year and 35 dollars per month. In other words, if IT companies do not advertise, there is no reason to collect user data as it is now, but there is a possibility that they will charge users with service charges.