Password Management

Have you ever had one of your online-account been hacked? Did you keep your passwords securely?

Today, I am going to talk about what we can do to securely manage our passwords.

Save your passwords in a good place

10-years-ago, I forgot the password to my email and I also forgot how to get the password back. I lost the data in that inbox forever.

The reason I forgot was that is II had so many accounts and passwords, and I didn't manage them well. So, I tried out various methods to save my passwords:

- write them in a notebook
- save them in a document on my computer
- use password manager app

Make your password stronger

Another time, my social media account was hacked. The hacker sent a lot of messages to my friends asking for money. After that, I had to connect with my friends to explain what was going on.

If you don't want those hackers to guess your password easily, you have to follow some rules to strengthen your password, such as:

- use uppercase and lowercase at the same time
- use some numbers
- use some special character (s) `!"$%&()*+,-./:;#<>?_@\`
- do not use your birthday
- do not make your password too short

Furthermore, when you sign-up for an account, update the ways to gain entry again if you were to lose your password:

- include your phone number
- include your valid email address
- include your valid living address
- set sensible secure questions and remember the answers

Avoid hackers' attacks

I heard a story about how a popular YouTuber lost her account. One day, she clicked an attachment of a suspect email, then the bad thing happened. She found that she couldn't sign in to her YouTube account anymore; she was aware that a hacker had taken over her account. Fortunately, she got her account back, but that was a half month later. We could learn something from this story:

- don't open suspect emails
- don't click on suspect links

Raise your security level

You should enable **Two-Factor Authentication(2FA)** to raise your security level. 2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This second factor could come from one of the following categories(1):

- Something you know: This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern
- Something you have: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
- Something you are: This category is a little more advanced, and might include a biometric pattern of a fingerprint, an iris scan, or a voiceprint(2)

All in all, If you follow the advice above, I think you could manage your passwords well.

Cites:

1.2. https://authy.com/what-is-2fa/