This topic has made me understand the importance of access controls. I have always known that passwords must not be common but I never knew the current strength of hackers and that they can ‘brute-force’ 4 digits passwords easily. This topic also opened my eyes on how easy it is for hackers to access accounts of careless people.

Statistics have shown that majority of internet users use English words and phrases as passwords. Followed by the use of names and birthdays. Because of this general trend hackers, who can easily profile their desired targets, will be able to penetrate their account and cause mayhem.

The [';--have i been pwned?](https://haveibeenpwned.com/Passwords) is one the best to check if your password and email have been compromised. This tool should be maximized by web users. Cyber threats and risks are really increasing. More and more people are victimized by cybercriminals. That is why passwords must be improved.

A good password must have a large entropy. Often human-generated passwords do not have a good entropy because it is not random. Like I said before, humans create their passwords through habits or what is easily remembered by them. And because the password’s useability, humans tend to use them in different accounts. This frequent use of same passwords can easily compromise the data and files of the user.

In contrast, machine-generated passwords have larger entropy because it is always generated randomly. The length and use of multiple symbols also create more variables thereby strengthening the passwords. The issue, however, is that these machine-generated passwords are hard to memorize. Users are forced to write them into a paper or digital notebook. And these written passwords can be easily stolen or compromised.

However, now we have password managers. These are softwares or programs designed to keep the user passwords protected. Of course, these programs have almost the same security issues as the passwords, but they use stronger and more complex encryption. Also, these passwords are stored hashed and salted.

Even if these hackers are able to access these password databases, they may not be able to use what they find. When passwords are stored they are hashed. Then when the user utilizes his password, the password is hashed and compared to the stored hashed value. This then creates a strong security for passwords.

Hashing, means creating a set of different values or digits per password. These strings of data cannot be decrypted and reversed engineered; hence it is not practical for hackers to convert them into plain-text.

Now, because more and more hackers are using stronger programs and hardwares, simple hashing is not enough. Now passwords can be salted before hashing. Salting means adding random values or data in the password txt before hashing. This additional data ‘salt’ then adds complexity, which further prevents hackers from interpreting and retrieving the plain text password.

Cybersecurity is not only about securing data in the cyberspace. Though passwords are supposed to be secure, but there are instances that these passwords are retrieved by committed hackers. Sometimes, users unwittingly announced or showed their passwords to a lot of people. Hence, using only password is not safe anymore. That is why; Multi Factor Authentication (MFA) came into being.

MFA utilizes different form of authentications to ensure that only authorized users are able to access data or devices. MFAs use combinations of password, passkey, and biometrics. The most common MFA here in Finland is the use of password and passkey from the user own bank. The bank may provide a printed key-code list; or the bank can use its digital phone service to issue access tokens that can be validated by the user using the user cellphone.

Users are able to use simple passwords because MFA adds another safety net to possible unauthorized access on their accounts. Still, users must maintain practice of creating un-common passwords. They must avoid the use of common English terms or their use of birthdays. Good passwords are also composed of different characters that add complexity.

Stronger and more complicated access controls creates a strong defense that discourages hackers from even attempting. This access controls have larger valued entropy. Larger entropy means harder for hackers to access and break. More resources would be used to crack this complicated access controls. Cost to benefit ratio is skewed; it is more costly to try to access complicated controls.

Therefore, users must be more aware of the complexity of access controls. They can then choose the correct access controls for them. However, now companies are opting for the use of MFA. This then help secure the transactions and data of users. This good security infrastructure has prevented unwanted access and utilization of data and gadgets.

The issue is useability always. MFA entails more steps before access, sometimes network problems lead to access issues, while biometrics are not often detected by gadgets. A healthy balance must then be implemented, useability and security should always be considered.