Securing your accounts

The combination of username and password has long been the standard way of authenicating users when they log into a website, service, etc. This combination is what keeps our personal messages with friends and family, our emails, our pictures and all the rest that is online from being accessed by everyone. They are the gatekeepers to our online presence which is why it is so important that they are secure. We are tought many things in school, but nobody ever told us how to choose a good password and how to secure our online accounts so it is obvious that most people don't know how to do it. This is where this guide hopefully comes in handy.

1st Step: Get a Password Manager

The most important thing in my opinion is to have different passwords and possibily different emails and usernames for different websites. Since nowadays it is not unusual to have dozens of online accounts, it can be very hard to keep track of all login data. Here is where Password Managers come in. These are apps that can be installed on your phone, laptop or tablet where all your passwords are stored in one place. Some of them are more barebones and don't do a lot more than store passwords, others offer features like random password generation, password synchronization and password sharing. I have tried different password managers, but the best one I have found up until now has been Bitwarden. This password manager is Free and Open Source, but also offers paid plans for more advanced functionality. I reccomend starting with the free version, which is more than enough in the beginning. You can always upgrade later.

2nd Step: Choose a strong Master Password

The Master Password in conjunction with your email address is what is needed to access your Vault. The Vault is where all of your passwords are stored. It goes without saying that this password needs to be extremely secure. One common misconception is that for a password to be secure it needs to be hard to remember and some weird combination of characters. This is true for your other passwords in your Vault, but not for your Master Password. Instead of thinking of it as a pass**word**, I would rather think of it as a pass**phrase**. The way an attacker will crack your password is either by using a Wordlist attack, with a Brute-force attack or through Social Engineering. The latter is (possibly) mitigated by using things like Two Factor Authentication, the former two are what a good passphrase should avoid from working. The longer your passphrase, the more possible combinations there exist and thus the longer it will take for a computer to crack it. What I do is I try to think of a silly but easy to remember phrase. An example could be: "*Fred Westerson walks on rotten Bananas*". This passphrase should take around 10,826,447,514,211,228 centuries to crack. Pretty secure, right?

3rd Step: Start changing your passwords

This is probably the most tedious part since you need to go in and change every password from every online account you have. I suggest you do this step by step and change a password the next time you use an account. If you had to think about a new random password for each account, you'd run out of words to use fairly quickly. This is why Bitwarden (and other password managers) have a password generation feature. Just go into the app, create a new password and click on the circular arrows next to the password box. I suggest you to use a password that has around 25 characters and that uses numbers, upper and lower case letters as well as special

symbols. This way you have a very secure password, but not too long so that it is impossible to type out if you cannot copy paste it once for some reason.