If you already know how to create secure passwords, and you are aware that you should be using different passwords, you are probably thinking now about how to remember or store or manage them. It is definitely not an obvious topic, so I will describe different methods of storing passwords, so you can compare them and think which one are better than others for you.

In your head!

This method is effective if you have a good memory and a small number of passwords. However, the problem occurs if you need to remember a larger number of complex passwords, PINs, and other relevant information. Also, what happens if you forget your password? You will face a reminder procedure (if there exists one). In most cases it is fast, but in others, it may be problematic, for example, the bank account passwords or encrypted containers. So, the method might be good, but only in a few cases, like master passwords.

On the paper

I would usually not recommend this method of storing passwords. Especially, if they are stored in an easily accessible place, such as on your desk, under your keyboard, or stuck to your monitor. Any visitor can then see it written on a piece of paper. There were even cases where the passwords stuck to the monitor were visible for TV viewers during interviews!

But there are at least two cases when writing passwords on paper can be a good idea. Firstly, in your testament with indication for your family what this password is for and where to use it (just to make it easier for them). And secondly, keeping important passwords, stored somewhere deep and safe, in an envelope with a seal. This might be possibly stored for example in the safe deposit box. Such method could be good for rarely used but high value passwords, such as 12 word private keys for blockchain wallets.

“In the browser” password manager

While this method is easy, and allows you to use your passwords on any device without remembering them, by doing so, you allow the password manager provider to have access to your passwords. It can be either Google (if you use Chrome) or Mozilla (if you use Firefox). So the question arises: how much do you trust your

browser provider with your most sensitive data? However, because it is extremely simple to use and sync, it may be a good option for less-sensitive data, like passwords for hobby forums.

Commercial password storage providers

Some companies offer plugins for browsers, like 1Password, LastPass, or Bitwarden – that are quite good and usually have more options than built-in browser password managers. Although the issue with them is the same as with the browser passwords manager – you must trust the company with your passwords. Most of them have both free and paid options, so you can try those before buying the actual plan.

Also, you can ask yourself if those password managers are secure – there have been leaks in the past and if that happened to your selected provider, you might want to think again. Even when you trust the company that they won't use your passwords for malicious reasons, you should probably ask your chosen password provider: what if you get hacked? Keep in mind that you will still need a master password to unlock access to your other passwords.

Store in file

But absolutely not in plaintext, as there are many ways in which plaintext passwords can be easily compromised. You should use dedicated password manager. Of course, there is, again, a matter of trust for code developers, however there are always ways to check it. For example, KeePass and KeePassX are Open Source software that allows anybody to review source code to check if they are secure.

As per synchronization between multiple devices, you can just add your password file to any sync provider. The file is encrypted (with your chosen method: AES, Serpent, Blowfish, etc.), so it is secure, even if the cloud provider behaves maliciously or gets hacked.

But please be sure to remember your master password – without it, you will be unable to access your encrypted passwords – ever! Password file encryption in password managers is extremely serious, and even brute force will be problematic due to the usage of many rounds of encryption!

Use 2FA!

It is technically not the next method of storing passwords, but an additional layer of security. It is just another way of proving that you are an actual password owner. Second-factor authentication can take many forms: mobile text message, email confirmation, or Authenticator application (like Google Authenticator).

Choose the most foolproof protection

Unsure whether your passwords are stored securely or loooking for business solution for password management? Drop us a message and we can talk. We know best how to store passwords securely – after all, we have a lot at stake if our methods turn out faulty. Our Client’s data and business reputation are just two of many repercussions we would face if our passwords leaked. We are always happy to help! Our Client’s security is what matters the most.