Passwords are indispensable part of using computers and mobile devices connected to the internet. We are using them on regular daily basis, almost everywhere: to our emails, bank accounts, cloud storage, account access; in work and at home.

Some passwords are easier to guess than others. What should we do to keep our accounts and data secure? Here are some ideas.

Passwords should be long!

One of hacking methods is using so-called *brute force attacks*. They are based on guessing every password possible. Hackers can attempt to brute force either directly into a system, or – if they obtained data – on password hashes. So why keeping passwords long is important?

Imagine guessing every possible password, staring from 3 letters. It will go like this: *aaa, aab, aac, aad* and so on. For modern computers with fast GPU it will take one *millisecond* to try all combination of 3 letter words. On 5 chars with numbers it will take 1 second. If we increase that number to 7 – It will take 29 minutes. With 8 chars it takes about 1 day, and with 9 chars it will take about 3 months.

Of course, hackers can use botnets to greatly speed up this process, but you can see how necessary time to crack password is increased with each char. So we need to use long passwords!

Passwords should not be one words

Another method used by hackers is using a dictionary. It means, that instead of going with each combination, like in previous example, hacker will only try words. Dictionaries can be very general. They may trying every word from *Encyclopedia Britannica*, or other especially crafted (for example for specific language) dictionary. That means hacker can try to break into your website making dictionary from all words actually used on your website, and their synonyms.

But – be aware! Dictionary for hacker is only a base for password! This means, that hacker trying to get into landlord's website will not only try passwords like landlord, home, renting, but also their modifications. Popular method is taking your starting year – landlord1990 – or with combinations – like LandlordCT90. You can see, that last password – LandlordCT90 – is quite long, but it's actually quite vulnerable to

dictionary attack.

Passwords are like tissues – should only be used once!

Imagine a situation, while you have very strong password, but you are using it everywhere: for your bank account, for your email, your smartphone, also for your PC account – but also for less meaningful things, like for automotive forum or for browser game. While breaking into banking account is obviously much more complicated, hackers also aim for less secured systems. Let's say now, that browser game had a bug, that allowed hacker to see whole database – with your email and password inside.

What will happen next? Hacker will try, if this password also matches your email – of course it does! Then he can go through your emails to find emails from your bank – like monthly statements – where your bank account number is present. And then, with both banking account and password, he can actually see all your funds in your account! Scary – isn't it?

To prevent that, my advice would be use different passwords everywhere. Of course, no one can remember hundreds of passwords – in that case you should use password manager, like Keepass, Bitwarden or 1password. If that is not a solution for you – then try making 3 different passwords, that you can remember – one for important, *high-level* things (like bank account), second for less important things (like email), and last one for things that have least meaningful information (like browser games). So you should consider different password storage options.

Of course, you should use 2 factor authentication (via text message, hardware key, authenticator app) especially for those *high level* services.

Long or complicated?

While considering password strength, two factors are considered most: one is password length, and second is amount of different characters used (like lower and uppercase, numbers, special signs etc). There is a thing called *entropy*, which is a measure of how unpredictable password is. The higher entropy, the better. Without going into details of how to calculate entropy, let's compare few passwords: first one will be *Kate1990* – this one has 8 letters, uppercase and numbers and is easy to

remember. Second is *De$.F9c1* – this one is very hard to remember, but contains also special signs. And third one – *Let-sPlayAt8AM* – which is longer, contains uppercase, special char, number, and is fairly easy to remember.

You already know, that first password would be easy to guess because of it would be found in dictionary attack. It's entropy is actually 27 bits, which is very low and should never be used. Not only it's prone to brute force attack, but also to dictionary attach. Second password is slightly better – it's entropy is 34 bits – although is very hard to remember and type. But third passwords' entropy is 70 bits – it's VERY strong and actually very easy to remember! For reference, for protecting bank account I would recommend using password, that has at least 60 bits of entropy – so this one would qualify.

Quick summary

I think, that this quick guide made it easier for you to understand how you should construct your passwords and what you should remember about when constructing a good passwords, that you won't forget. If you are concerned now, that your password might've been compromised, you can try to check at https://haveibeenpwned.com/. Of course, this guide doesn't cover everything, it's just a tip of an iceberg, but I think that from now on you will be able to make your data even more secure.