Password Hygiene

I'm not a magician, but I believe you're using the same password across different applications and websites. Not exactly? Then you're using the same password but with slightly different variations for each one (i.e., adding a number, removing a letter, etc...). Maybe you're using your favorite pet's name as your password. The point is that it's easy to remember. Well, you made it easier for hackers to get into your accounts. In this module, we will cover a crucial topic, password hygiene, which highlights the common errors people fall into when coming up with passwords and how to come up with almost unbreakable ones.

1- **Reusing the Same Password**

   Who would want to have a hard time remembering passwords? It's hard to keep track of different passwords across different platforms, so it's easier to use the same password for different accounts. Hackers love people with this mindset because once they crack your password, it's over. Even if your password is not easy to guess, you're still vulnerable to attacks that don't rely on guessing. Hackers have various ways of cracking passwords, one of them is when a company's database is leaked. Imagine you used this specific password on a website that's not really secured and a hacker gets access to this database and thus your password, say goodbye to your accounts.

2- Using Personal Information as Passwords

It's tempting to use your pet's name as your password as it's easy to remember. It's also tempting to use your birthdate, favorite TV show or movie, phone number, or even a combination of them all. Not to surprise you, but cracking such passwords doesn't even require hacking skills, it only needs someone who knows you. They know your dog's name, they know your birth date, they combine them both and suddenly, they have access to your account. Constructing your password with personal information, especially publicly accessible ones, puts your account at risk of compromise.

3- Password Sharing

Most of us share our accounts with our friends: Netflix, Disney+, Amazon Prime Video, Coursera, you've probably shared at least one. Don't get me wrong, the problem isn't your friend– it's their device itself. If your friend's device is infected with malware (i.e., bad malicious programs that can steal your data), that malware can capture login credentials in the background. In other words, you didn't only give your password to your friend – you also gave it to a hacker! Password sharing might be harmless, but in the wrong scenario, it could be the first domino to fall.

4- Not Changing Passwords Regularly

Let's be honest, who updates their passwords regularly? It's tiring to always keep track of new passwords – we barely remember our current ones! But let me tell you, updating your password regularly could save you from a big mess. Database breaches occur more frequently than we imagine,

which means your passwords might have already been leaked and you don't even know it. Thus, updating your password regularly greatly reduces the risk of getting your account hacked. Big companies force this policy on their employees for a reason, why shouldn't we?

Now that we've known what we're doing wrong with our passwords, how can we protect them? You may think it's cumbersome, but it's actually pretty easy.

1- **Make Complicated Passwords:**
   - Mix up your passwords with uppercase and lowercases letters, numbers, special characters.
   - Password length should be at least 12 characters.
   - Try avoiding using words that can be found in a dictionary, make up random words, or even splash random characters.

2- **Use a trustworthy Password Manager:** Coming up with strong passwords may take a lot of effort, let alone remembering them. Ease it on yourself by setting up a password manager that handles creating complex passwords and securely storing them on your device.

3- **Enable 2FA:** 2FA, or Two-Factor Authentication, adds an extra layer of security to your accounts. Even if your password got compromised, with 2FA enabled, they still can't access

your account. 2FA requires you to insert an OTP (One-Time passcode) sent to your phone number or email in order to get into your account.