PASSWORD STRENGTH AND MANAGEMENT

Passwords are the key to your online accounts, and they should be treated with care. A strong password can protect you from hackers. A weak password, on the other hand, can compromise your security.

- Use a combination of uppercase and lowercase letters, numbers, and symbols. This makes your password harder to guess or crack by brute force attacks. For example, instead of using "password" as your password, you could use **"P@ssw0rd!"** or **"p4S$W#rD*"**. Password strength is a combination of length and complexity referred to as entropy. Neither short and complex nor long and simple are considered strong.

- Avoid using common words, phrases, names, dates, or personal information as your password. These can be easily guessed by hackers who use dictionary attacks or social engineering techniques. For example, don't use your name, birthday, pet's name, favorite movie, or anything that someone can find out about you online or offline.

- Make your password long and unique. The longer your password is, the more secure it is. Aim for at least 8 characters but longer is better and avoid repeating the same password for different accounts. You can use a passphrase, which is a sentence or a series of words that are easy to remember but hard to crack. For example, you could use **"I+love+chocolate+cake+and+ice+cream"** or **"multimedia.GUILT.magnetic.CAFE.ticket"**.

- Use a password manager. A password manager is a tool that securely stores and generates passwords for you. It can help you create and remember complex passwords for different websites and apps, without having to write them down or reuse them.

- Change your password regularly and update it if it's compromised. Enable two-factor authentication (2FA) if possible. 2FA is an extra layer of security that requires you to enter a code or use a device to verify your identity when you log in to your account. The three common factors are:

- Something you know (password, answer to security questions)
- Something you have (WireXchange token, Google Authenticator code, SMS code)
- Something you are (biometrics)

As you can see here requiring a password and answering security questions is not multi-factor. They are two of the same factor.

- Treat your email with the highest security. People often prioritize banking or medical passwords as their most important, and they are important, but any email account you have tied to those systems is just as important if not more so. Almost every website has a mechanism to use email to reset a password. If you have a weak email password with no additional security and that email can be used to reset a complex banking password you've effectively lowered the complexity of the strong banking password to that of your email.