PASSWORD SECURITY

In today's digital age, online accounts contain a wealth of personal and sensitive information that cybercriminals are eager to exploit. Here are expanded tips to help you create strong passwords and protect your digital identity:

USE A PASSWORD MANAGER

With so many online accounts requiring passwords, it can be tempting to use the same password for everything. However, this is a dangerous practice that can lead to all your accounts being compromised if one password is discovered. A password manager can help you generate and store complex, unique passwords for each of your accounts.

USE LONG, COMPLEX PASSWORDS

The longer your password, the harder it is for cybercriminals to crack. Aim for passwords that are at least 12 characters long. Each unique password should be a combination of upper case letters, lower case letters, numbers and special characters (like >,!?).

AVOID COMMON PASSWORD PITFALLS

Don't use easily guessable passwords like "password," "123456" or keyboard patterns such as "qwerty." Avoid using personal information like your name, birthdate or pet's name, as these can often be easily discovered by cybercriminals.

USE UNIQUE PASSWORDS FOR EVERY WEBSITE

Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts remain secure.

KEEP YOUR PASSWORDS PRIVATE

Never share your passwords with anyone, and be wary of phishing scams that try to trick you into divulging your login credentials.

By following these tips, you can significantly reduce your risk of falling victim to cybercrime. Remember, password security is an ongoing process, so make sure to regularly update your passwords and stay up to date on the latest cybersecurity best practices.

INDEPENDENT FINANCIAL™