May BROOKS

MULTI-FACTOR AUTHENTICATION (MFA)

An extra layer of security,
Make it harder for unauthorized individuals to gain access to your information and accounts

What is MFA \ 2FA

Multi-factor-authentication (MFA), adds an extra layer of security to your sensitive accounts. MFA is achieved involves using at least two of the following factors:

Something you KNOW

Like a password, personal identifying number (PIN) or personal question

Something you HAVE

A code sent via a text message or email, generated by an authentication app or physical device

Something you ARE

Like fingerprint, facial recognition etc.

Most implementation include the use of two factors, usually a password or PIN with a One Time Password sent by text or generated by an app, hence most implementations are actual two-factor-authentication - 2FA.

Why use 2FA

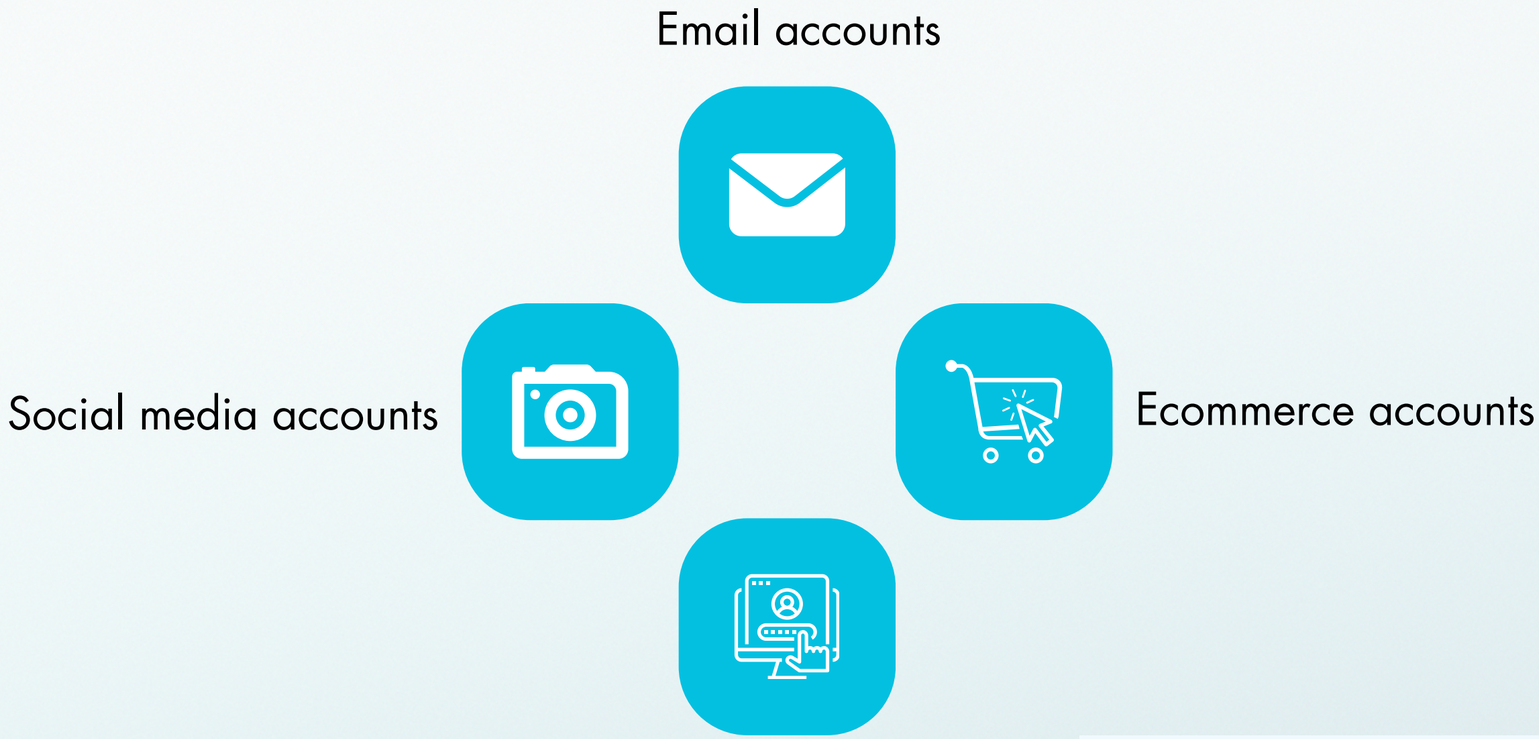
As mentioned in the Passwords Management guide - many people use the same password on various services. That means that a single credential exposure incident, can impact multiple accounts.
As we know, even the best passwords can be leaked in a data breach, not to mention, exposed by a sophisticated attacker.

Using 2FA reduces the chances of unauthorized individuals accessing your accounts, even if they have your password.

Knowing that your accounts are well-protected can give you greater peace of mind.

Where to use 2FA

Adding 2FA \ MFA is considered best practice to protect all your sensitive accounts, and especially:



Pro Tip: Enable 2FA on all services that allow it.

NEVER GIVE ANYONE

YOUR

ONE TIME PASSWORD

2FA step-by-step Guides

Google

Office 365

Tiktok

Instegram

WhatsApp

Facebook