IF YOUR PASSWORD SLIPS, MFA WILL STOP INTRUDERS

Multi-Factor Authentication (MFA) adds an extra layer of security by requiring multiple methods to verify your identity. It's like locking your front door and needing a key and a fingerprint to get in.

What is the second validation?

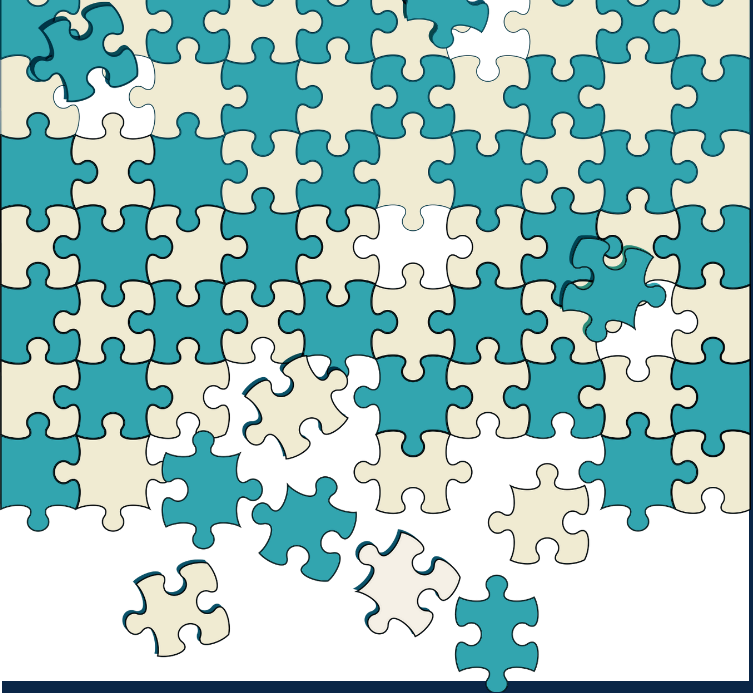
Your second validation will come from something **you know** (a code, a string of characters or a passphrase), something **you have** (a physical security token or an app), or something **you are** (facial recognition or a fingerprint scan).

How does MFA make me more secure?

MFA reduces security risks by adding an additional layer of defence. If a cyber-criminal doesn't have access to your second device or know the code, then they cannot access your accounts, even if they have the passphrase.

Activate MFA wherever possible

Many services have mandatory MFA enabled. If you have not enabled MFA on your accounts, it is highly recommended to check the settings and turning it on if available.



KEEP DEVICES UPDATED

Updates don't just fix bugs, they close gaps that could be used for cybercriminals to sneak into your system. When you update your device, you're protecting not just your files, but everyone you connect with.

QUICK TIPS

Don't stop at your laptop or phone. Remember to update:

- Your work phone or laptop (if you see an update notification, click it).
- Your personal phone or tablet.
- That old tablet or laptop at home you sometimes use for Netflix or kids' games.
- Smart gadgets — like speakers, TVs, or watches — if they connect to the internet, they need updates too.

An update today prevents a problem tomorrow. The small updates you do at home and work all add up to a stronger cyber culture.

Habits that build a cyber safe culture

Big culture → Big impact.

WHY CULTURE?

Cyber culture isn't built by rules — it's built by people.
The way we share, the habits we form, and the choices we make every day protect not just ourselves. They protect our family, friends, workplaces, and our community.

HOW TO MAKE A STRONG AND SECURE PASSPHRASE

Passphrases are essential for protecting personal and government information from falling into the hands of cyber criminals. Having secure passphrases reduces your risk of identity theft and fraud.

Use long passphrases

Passphrases are longer and more complex than typical passwords, making them much harder to crack. Choose a random sequence of words (e.g., "PurpleMonkeyDeskLamp") that doesn't follow any predictable pattern.

Avoid common passwords

Simple and frequently used passwords (e.g., "123456," "Password1!") are easy targets for AI. Avoid using anything easily guessable, like personal information or words found in a dictionary.

Enable multi-factor authentication

MFA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone. Even if your password is compromised, MFA can prevent attackers from accessing your accounts.

Use a password manager

Password managers can generate and store complex, unique passwords for each account. This eliminates the need to remember multiple passwords while ensuring that all your accounts have strong protection.

Update passwords when needed

If you suspect you are part of a breach or if your credentials have been compromised in a data leak, change your password as soon as possible. Updating passwords reduces the chance that older credentials can be used against you.

Monitor for data breaches

Use services that notify you when your email or password is part of a data breach. By staying alert to leaked credentials, you can take immediate action to secure your accounts.

RED FLAGS OF WEAK PASSWORDS

- Using personal information, such as names or birthdates, especially if found on social media.
- Short passwords under 12 characters.
- Common phrases or dictionary words like "welcome123" or "Qwerty12345!"
- Reusing passwords across multiple accounts.