Multi-factor authentication (MFA)

A stronger line of defence

If an attacker guesses your password, MFA steps in to stop them from progressing further and accessing your account. MFA works as a supporting authentication method after your password, by also requiring something you know, have or are to access.

What should you do?

01 Identify any accounts that don't have MFA enabled.

02 Where it is available, set up MFA through SMS codes, authenticator apps, biometrics or security keys.

03 Start with the important accounts:

- email accounts (to avoid anyone else requesting password resets)
- financial services (e.g. online banking)
- accounts that save payment details (e.g. PayPal, Amazon, eBay)
- social media accounts (e.g. Facebook, Instagram)
- other accounts that hold personal information (super accounts, myGov).

04 For questions on MFA related to work devices, contact your IT security team.

For MFA on personal devices, visit www.cyber.gov.au/mfa

Types of MFA can include:

Something you know (e.g. a PIN, password or passphrase)

Something you have (e.g. a smartcard, physical token, authenticator app, SMS or email)

Something you are (e.g. a fingerprint, facial recognition or iris scan)

For more information on MFA, visit: https://www.cyber.gov.au/mfa