POWERFUL PROTECTION AGAINST CYBERCRIME
MULTI-FACTOR AUTHENTICATION

Criminals only need one attempt to succeed in accessing your most important accounts. Protect your valuable information by enabling multi-factor authentication where possible. The multiple layers make it much harder for criminals to attack and gain unauthorised access.

WHAT IS IT?

Multi-factor authentication (MFA) is a security measure that requires two or more proofs of identity to grant you access to your accounts.

HOW DOES IT WORK?

Multi-factor authentication typically requires a combination of something you know (pin, secret question), something you have (card, token) or something you are (fingerprint or other biometric).

Some MFA options include, but are not limited to:

- Physical token
- Biometrics/ fingerprint
- Email
- Random pin
- Authenticator app
- SMS

WHY?

MFA offers significantly more powerful security and protection against criminals. They might manage to steal or guess one proof of identity (such as your pin) but they still need to obtain and use the other proofs of identity to access your account.

WHAT TO DO IF THINGS GO WRONG
If you've been the victim of a cybercrime:

VISIT
cyber.gov.au for more advice on how to be secure online.

SIGN UP
To our free alert service cyber.gov.au/acsc/register and follow us on Facebook facebook.com/cybergovau

REPORT
Cybercrime to REPORTCYBER: cyber.gov.au/report

CONTACT
Call 1300 CYBER1 or visit cyber.gov.au