A password alone isn't enough.

Two-step login (also called multi-factor authentication or MFA) stops most account takeovers, even when a password is stolen. Some kinds are much stronger than others.

THE PROBLEM

Stolen passwords
Passwords leak in breaches and get tricked out of people every day.

Scammed codes
Fake sites can ask for your 6-digit code and use it straight away.

SIM swapping
Criminals can take over your phone number and receive your text message codes.

WHAT TO DO · PICK THE STRONGEST OPTION AVAILABLE

BEST	**Passkeys and security keys.** Nothing to type or hand over, and they only work on the real site.
GOOD	**Authenticator app.** Codes from an app on your phone. Much better than nothing, but a code can still be tricked out of you.
LAST RESORT	**Text message codes.** The weakest option. Switch up when you can.

Start with your email, password manager and banking. Keep your backup codes somewhere safe.

WE RECOMMEND

YubiKey

A small hardware key from Yubico. Touch it to sign in. It works with passkeys on thousands of sites. **Buy two** and keep a spare somewhere safe. From about US$30 (Security Key) or US$60 (YubiKey 5).

yubico.com

Scan to visit

Sources: Australian Cyber Security Centre (cyber.gov.au) – Multi-factor authentication and Passkeys · CISA (cisa.gov) – Secure Our World: Turn on MFA, and Phishing-resistant MFA fact sheet · NIST SP 800-63B Digital Identity Guidelines. Prices are approximate and in US dollars; check yubico.com.

APCSC is an independent business and is not affiliated with the Australian Government or the Australian Cyber Security Centre.

ABN 13 262 392 536 · © 2026