Stop reusing your passwords.

Criminals steal passwords from one website, then try them on your email, bank and social media. A password manager puts a stop to that.

THE PROBLEM

Same password everywhere

One data breach can unlock every account that shares it.

Easy to guess

Pet names, birthdays and "Password1" are cracked in seconds.

Fake login pages

Scam sites look real. A manager only fills in your details on the genuine site.

WHAT TO DO

1. **Use a password manager.** It creates and remembers a different password for every account, so you only remember one.
2. **Make the one you remember long.** Use a passphrase of four or more random words, at least 15 characters. Length beats tricky symbols.
3. **Add a second lock.** Turn on two-step login for your password manager and your email (see guide 2).
4. **Change a password only when you need to.** After a breach or a scare, yes. On a timer, no: it isn't needed.

WE RECOMMEND

Bitwarden

Open-source and independently audited. Works on your phone, computer and browser. The **free plan** covers unlimited passwords on unlimited devices. Premium (about US$20 a year) adds built-in login codes, security-key support, emergency access and password health checks.

bitwarden.com

Scan to visit

Sources: Australian Cyber Security Centre (cyber.gov.au) – Passphrases and Password managers · CISA (cisa.gov) – Secure Our World: Use Strong Passwords and Password Managers · NIST SP 800-63B Digital Identity Guidelines (15+ characters, no forced changes). Prices are approximate and in US dollars; check bitwarden.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