CHECKLIST · SCAMS & SECURITY

# A VPN is a sealed envelope, not a bodyguard

Published 17 November 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/vpn-explained-cafe/

- [ ] **Use your phone's hotspot for work in public.** The ACSC suggests your personal hotspot instead of café or airport Wi-Fi.
- [ ] **Check the address bar before you log in on public Wi-Fi.** If Chrome shows "Not secure", don't type a password or card number there.
- [ ] **Ask your IT provider whether your business needs a VPN.** It matters most if staff need to reach files or systems on the office network.
- [ ] **Pick a reputable VPN provider if you pay for one.** All your traffic passes through its servers, so treat it like choosing a bank.
- [ ] **Keep phishing checks on even with a VPN running.** A VPN won't stop you entering your password on a fake login page.
- [ ] **Turn on automatic updates on your laptop and phone.** A VPN won't protect you from software security flaws, so the ACSC says to install updates as soon as possible.
- [ ] **If your IT provider gives you VPN details, use the built-in client.** In Windows 11, go to Settings, Network & internet, VPN, Add VPN, and choose Windows (built-in). On Android, go to Settings, Network & internet, VPN, tap Add, enter the details and tap Save.

NOTES



General information only, not legal, tax or financial advice. Check the full story and its sources before acting.