PRINTABLE CHECKLIST • 24 OCTOBER 2026

SIX SIMPLE CYBER SECURITY CHECKS

For our money, online identity and everyday accounts.

Why this matters: On 21–22 October 2026, serious weaknesses were disclosed in PHP, software used behind many websites. The Australian Cyber Security Centre issued a critical alert. This does **not** mean your accounts have been hacked. These six everyday checks are a sensible way to protect yourself.

01 SECURE YOUR EMAIL FIRST

Your email is the key to almost everything. Someone with access may be able to reset other passwords.

- [ ] Open Gmail, Outlook or whichever email service you use.
- [ ] Turn on two-step verification (an extra check when you log in).
- [ ] Check that your recovery phone number is correct.

Do this one first.

02 CHECK YOUR MONEY

Open your banking app yourself today.

- [ ] Turn on transaction alerts and check recent bank and credit card activity.
- [ ] Check your daily transfer limit and lower it if appropriate.
- [ ] Never move money to a so-called “safe account” because someone calls you.

Hang up and call the bank using its official number.

03 USE DIFFERENT PASSWORDS

A stolen password should not unlock all your other accounts.

- [ ] Use different passwords for email, banking, shopping and social media.
- [ ] Store them in your iPhone Passwords app or another trusted password manager.

Never share your passwords or security codes.

CONTINUE YOUR SIX CHECKS

Your remaining checks

04 SECURE SOCIAL MEDIA & AI ACCOUNTS

Instagram, Facebook and AI accounts can also be taken over.

- [ ] Turn on two-step verification for Instagram, Facebook and ChatGPT.
- [ ] For Claude, protect the Google or email account you use to sign in.
- [ ] Review logged-in devices and sign out any you do not recognise.

05 CHECK YOUR PHONE & HOME INTERNET

Three practical checks make a difference.

- [ ] Turn on automatic updates for your phone and computer.
- [ ] Use Face ID, fingerprint protection or a strong phone passcode.
- [ ] Give your home modem a private administrator password, not its factory default.

Ask your internet provider to help if you are unsure.

06 STOP. CHECK. THEN CLICK.

Criminals may pretend to be your bank, a delivery company or someone you know.

- [ ] Never give an unexpected caller your password or a security code.
- [ ] Never install an app because an unexpected caller tells you to.
- [ ] If a message sounds urgent, go directly to the official app or website.

HAVE YOUR OWN WEBSITE? CHECK THIS TOO.

Wix, Squarespace and Shopify: These platforms generally manage the underlying server updates. You still need to secure your login.

WordPress, WooCommerce, Joomla, Drupal, Magento or custom PHP sites: Ask your host or developer whether affected PHP software has been patched, suspicious activity checked and a working backup confirmed. A site on this list is not automatically compromised.

IF IT FEELS TOO MUCH, PLEASE ASK FOR HELP. Print this checklist and take it to a trusted IT support person. Enter your own passwords and security codes. Please do not put it off.

Official information: Australian Cyber Security Centre: PHP security alert and Personal Cyber Security Handbook. For suspected compromise call 1300 CYBER1 (1300 292 371).

Outside Australia? These six checks are useful wherever you live.
For local alerts and advice, check your country's official cyber security agency.