



Home Cybersecurity Checklist

Simple steps to protect your home Wi-Fi, devices, accounts and family online, written for people who are not IT experts.

You do not need to be a tech expert to stay safe online. Work through these checks at your own pace, and tick each one when it is done. If something is unclear, ask a family member or get in touch with us.

Household

Date checked

Your home network and devices

Done	Item
☐	Router and Wi-Fi are secured Change the router's default admin password, use WPA2 or WPA3 security and choose a strong Wi-Fi password.
☐	Devices are kept up to date Turn on automatic updates for phones, computers, tablets and your router.
☐	Browsers are kept safe Keep your web browser updated, remove extensions you do not use and do not ignore security warnings.
☐	Downloads come from safe places Only install apps from official app stores or the maker's own website.
☐	You are prepared if a device is lost Turn on Find My iPhone or Find My Device, set a screen lock and know how to wipe a lost device.

Your accounts

Done	Item
☐	A password manager is in use It remembers strong, different passwords for every account so you do not have to.
☐	MFA is turned on for important accounts Start with email, banking, social media and your Apple, Google or Microsoft account.
☐	Account recovery settings are up to date Your recovery phone number and email address are current.
☐	Privacy settings are reviewed Check what your social media and apps share, and turn off location sharing you do not need.

Everyday safety

Done	Item
☐	Everyone knows how to spot scam emails and texts Be wary of urgent messages about deliveries, refunds, fines or accounts. Go to the website or app directly instead of clicking links.
☐	Important files and photos are backed up Keep a copy in the cloud or on an external drive, and check you can open it.
☐	Family online safety is discussed Talk with children about safe sharing, use parental controls where helpful and agree on who to tell if something feels wrong.

Think you have been scammed?

Contact your bank straight away if money or card details are involved. You can report scams at scamwatch.gov.au and cybercrime at cyber.gov.au.

Notes and things to follow up

Need a hand?

Omnicon I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.