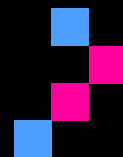


Cybersecurity Basics

For SMB



Initial
TECH

Overview

This simple, practical guide helps small businesses protect against common cyber threats using plain-English steps and checklists. It follows public guidance from the Australian Cyber Security Centre (ACSC), the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the UK National Cyber Security Centre (NCSC), and NIST. Start with the quick wins below, then work through each section.

How to use this guide

- 1) Pick what you are checking (computers, Microsoft 365, website, Wi-Fi).
- 2) For each section, tick the tasks done and note evidence (policy, screenshot).
- 3) Write any gaps into the action plan with owners and dates.
- 4) Repeat quarterly to keep protections current.

The Big 5 quick wins

- Turn on multi-factor authentication (MFA) for email, banking and admin accounts.
- Update software and devices automatically.
- Back up data using 3-2-1 (plus an offline/immutable copy) and test restores.
- Use a password manager and long passphrases; avoid shared accounts.
- Train staff to spot phishing; report suspicious emails.

1. Secure your accounts (Passwords + MFA)

Strong, unique passphrases and MFA stop most account break-ins. Avoid shared accounts and limit access to only what staff need.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Use a password manager for all staff	Choose a trusted manager; store unique passwords for each important account.		
Use long passphrases (15+ characters) for critical logins	Pick 4+ random words with numbers/symbols where allowed.		
Turn on MFA for email, banking, payroll and admin accounts	Enable MFA in account/security settings; prefer app prompts or passkeys.		
Avoid shared accounts or track who uses them	Create individual accounts; if sharing is unavoidable, keep an access list and change credentials when staff leave.		
Limit access based on role (least privilege)	Grant only what each person needs to do their job; review quarterly.		

2. Keep software and devices up to date

Out-of-date systems are the easiest way in for attackers. Turn on automatic updates for computers, phones, routers and apps.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Enable automatic updates on Windows/macOS/iOS/Android	Turn on auto-update in system settings for OS and apps.		
Update office routers and Wi-Fi equipment	Log in to the router; change default admin password; install latest firmware.		
Update website platform and plugins	Apply CMS/plugin updates (e.g., WordPress) monthly; remove unused plugins.		
Replace end-of-life systems	Plan to upgrade unsupported devices/software; isolate until replaced.		

3. Back up your information (and test restores)

Reliable backups are your safety net after ransomware, mistakes or failures. Use the 3-2-1 rule and keep one offline/immutable copy.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Follow 3-2-1: three copies, two media, one offsite	Keep local + cloud backups; store one copy offsite.		
Maintain one offline or immutable backup	Use disconnected storage, tape, or cloud immutability that cannot be changed.		
Automate daily backups for critical data	Schedule backups to run daily; verify they complete.		
Test restores quarterly	Restore sample files and at least one full system; record time to recover (RTO/RPO).		
Separate backup credentials from production	Use different accounts/keys; restrict admin access to backup systems.		

4. Turn on security software (email, endpoints, Microsoft 365)

Security tools block malware and phishing. Use built-in protections and keep them active.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Install endpoint protection (AV/EDR) on all devices	Use reputable security software; turn on real-time scanning.		
Enable Microsoft 365 protections	Turn on MFA, block legacy authentication; enable Defender/anti-phishing policies.		
Set up spam and phishing filters	Use your mail provider's anti-spam; flag external senders; block dangerous attachments.		

5. Secure your network and Wi-Fi

Your router is the digital front door. Secure Wi-Fi and separate guest access.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Change the router's default admin password	Create a unique, strong password; store it in the password manager.		
Use WPA3 (or at least WPA2) on Wi-Fi	Set Wi-Fi security to WPA3/WPA2-AES; avoid WEP.		
Separate guest Wi-Fi from business Wi-Fi	Create a guest network; block access to internal devices.		
Disable WPS and remote admin if not needed	Turn off easy-connect features and external management.		
Update router firmware regularly	Check monthly for updates; apply patches promptly.		

6. Harden your website and cloud services

Keep websites and cloud apps updated and configured securely; understand what the provider secures and what you must secure.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Use HTTPS and valid certificates	Ensure your site forces HTTPS; renew SSL/TLS certificates on time.		
Apply least privilege in cloud apps	Restrict admin roles; review access regularly.		
Turn on MFA in cloud accounts (M365/Google/AWS)	Require MFA for users and admins.		
Back up cloud data and configure versioning	Enable backups/snapshots; protect against accidental deletion and ransomware.		
Remove unused apps/integrations	Audit third-party add-ons; revoke what you don't use.		

7. Protect business data & privacy

Know what personal and business data you hold, where it lives, and who can access it; follow Australian privacy guidance.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
List your key data and where it's stored	Inventory customer, employee and financial data across devices and cloud.		
Minimise and centralise where practical	Reduce copies; keep important data in secure locations with access controls.		
Create a simple privacy notice	Explain what you collect, why, and how people can contact you.		
Plan for data breach notification	Know when and how to notify customers and the OAIC if a breach occurs.		
Review if the Privacy Act applies to you	Check OAIC small business guidance and exemptions.		

8. Prepare your staff (phishing & safe habits)

People are your first line of defence. Short, regular training and simulated phishing build a strong security culture.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Run short phishing awareness sessions	Teach staff to check senders, hover over links, and report suspicious emails.		
Provide an easy “report phishing” option	Use a mailbox or add-in button; thank people for reporting.		
Create simple dos and don’ts poster	Reinforce basics: MFA, updates, strong passwords, careful attachments.		
Include cyber in onboarding and exits	Issue accounts via a checklist; remove access when staff leave.		

9. Incident response quick plan

A written plan saves time and stress. Keep a hard copy in case systems are offline.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Decide who does what in an incident	Assign roles (lead, communications, technical, legal).		
List who to contact (IT, bank, insurer, police)	Include phone numbers and account details.		
Know how to report cybercrime	Use ReportCyber and call 1300 CYBER1 for advice.		
Practice the plan yearly	Run a short tabletop exercise; improve the playbook.		

10. Vendor & MSP checklist

Ask partners how they protect your data and services; include security in contracts.

Task	How to (plain English)	Status (Yes/No)	Evidence / notes
Ask MSPs about MFA, backups and monitoring	Request evidence of controls; define response times.		
Confirm data location and privacy posture	Know where data is stored; request privacy commitments.		
Set roles during incidents	Agree who leads and how to communicate.		
Review vendors yearly	Re-check security measures and contracts.		

Action plan (next steps)

Action	Owner	Due date	Resources needed	Status

References

- ACSC Small business cyber security guide & checklist
- CISA Cyber Guidance for Small Businesses
- NCSC Small Business Guide (UK)
- NIST CSF 2.0 Small Business Quick-Start
- OAIC small business privacy guidance
- ACSC Small business hub resources (cloud, MSP, ransomware, ReportCyber)
- Microsoft 365 Baseline Security Mode & hardening guidance
- Backup best practices (3-2-1-1-0 and immutable copies)