



Small Business Cyber Security Checklist: 15 checks

Tick each one you can confirm. Each item says how to check it yourself and where the guidance comes from.

Business: _____ Checked by: _____ Date: _____

Accounts and access

- ☐ **1. Multi-factor authentication is on for email, Microsoft 365 and remote access**
Multi-factor authentication is one of the Essential Eight. With it on, a stolen password alone is not enough to get into an account.
How to check: Sign in to your work email in a private browser window. If the password alone gets you in, MFA is not on for that account.
Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)
- ☐ **2. Every account has its own strong password, kept in a password manager**
business.gov.au recommends strong passwords or passphrases and a password manager to create a unique password for each account, so one leaked password does not unlock the others.
How to check: Ask three staff whether any work password is reused elsewhere, shared, or written down.
Source: Cyber security checklist, business.gov.au
- ☐ **3. Staff only have the access they need, and everyday accounts are not administrators**
Restricting administrative privileges is one of the Essential Eight: malware that runs under an everyday account can do far less damage than under an administrator.
How to check: On a staff computer, open Settings, then Accounts. If the everyday account is listed as an Administrator, it has more access than daily work needs.
Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)

Devices and updates

- ☐ **4. Browsers, Microsoft Office, email and PDF apps are updated within two weeks**
At Essential Eight Maturity Level One, patches for office suites, web browsers, email clients and PDF software are applied within two weeks of release.
How to check: In Chrome or Edge, open Settings, then About. If it offers an update or asks to relaunch, updates are waiting.
Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)
- ☐ **5. Operating systems are up to date, and none is past the end of vendor support**
Maturity Level One applies workstation operating system patches within one month of release and replaces operating systems the vendor no longer supports.
How to check: On each PC, open Settings, then Windows Update, and check for pending updates. List any PC still on Windows 10, which Microsoft stopped supporting in October 2025.
Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)

☐ **6. Antivirus or endpoint protection is running on every computer**

business.gov.au lists antivirus software and malware filters among the basic precautions for every business.

How to check: On a Windows PC, open Windows Security, then Virus and threat protection, and confirm it is on and current. Check the laptops that rarely come into the office too.

Source: Cyber security checklist, business.gov.au

☐ **7. Microsoft Office macros are blocked for anyone who does not need them**

At Maturity Level One, macros are disabled for users without a business need and macros in files from the internet are blocked.

How to check: Ask whether anyone in the business actually uses macros. If nobody does, they can be switched off for everyone with a Microsoft 365 policy.

Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)

Email and payments

☐ **8. Email is filtered for phishing, malware and spoofed senders**

The Australian Cyber Security Centre recommends email authentication controls to help detect and block fraudulent emails, and spam and message scanning to filter harmful content.

How to check: Look in your junk or quarantine folder. If suspicious messages never land there, ask your email provider what filtering is in place.

Source: Protecting against business email compromise, cyber.gov.au

☐ **9. Any change to bank or payment details is confirmed by phone**

The Australian Cyber Security Centre advises a clear, consistent process to verify requests involving payments and account changes, using contact details you have checked separately.

How to check: Ask whoever pays your bills what they would do if a supplier emailed new bank details. The answer should be: call the supplier on a number we already have.

Source: Protecting against business email compromise, cyber.gov.au

Backups

☐ **10. Important data is backed up regularly, including Microsoft 365 email and files**

Regular backups of data, applications and settings are one of the Essential Eight.

How to check: Find out when the last successful backup ran, and whether it covers Microsoft 365 mailboxes, OneDrive and SharePoint, not just the office PC.

Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)

☐ **11. Restores are tested, and everyday accounts cannot change or delete the backups**

At Maturity Level One, restoring from backup is tested, and unprivileged accounts are prevented from modifying or deleting backups.

How to check: Restore one file from last week's backup. If nobody has tried a restore in the last few months, book one in.

Source: Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au)

People and policy

☐ 12. Staff know how to spot a scam and who to report it to

business.gov.au advises teaching staff about common cyber threats and making sure they know how to report a scam or potential threat.

How to check: Ask a staff member what they would do with a suspicious email. They should know not to click, and who to tell.

Source: Cyber security checklist, business.gov.au

☐ 13. You have a written cyber security policy that staff have read

A cyber security policy sets out staff responsibilities for data, devices, email, websites and social media.

How to check: Check that it exists, that it covers those five areas, and that new starters are given it.

Source: Create a cyber security policy, business.gov.au

Incident readiness

☐ 14. You have a plan for what happens if you are hacked

business.gov.au's emergency management plan covers how to report a cyber incident, how to tell staff and customers, and how to keep the business running.

How to check: Write down who you call first, and save the Australian Cyber Security Hotline: 1300 292 371.

Source: Develop an emergency management plan, business.gov.au

☐ 15. You know what your cyber insurance covers, if you have it

Cyber insurance can help with the cost of an attack, but, as business.gov.au notes, you need to understand exactly what you are covered for.

How to check: Find the policy and check what it says about business interruption, data recovery and ransomware, and which security controls the insurer expects.

Source: Types of business insurance, business.gov.au

Sources

Create a cyber security policy, business.gov.au: business.gov.au/online-and-digital/cyber-security/create-a-cyber-security-policy

Cyber security checklist, business.gov.au: business.gov.au/online-and-digital/cyber-security/cyber-security-checklist

Develop an emergency management plan, business.gov.au: business.gov.au/planning/business-plans/develop-an-emergency-management-plan

Essential Eight Maturity Model, Australian Signals Directorate (cyber.gov.au): cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight/essential-eight-maturity-model

Protecting against business email compromise, cyber.gov.au: cyber.gov.au/publication/protecting-against-business-email-compromise

Types of business insurance, business.gov.au: business.gov.au/risk-management/insurance/types-of-business-insurance

Couldn't tick everything? Book a free, obligation-free IT security audit with PC Madness. We check these areas on your actual systems and report what to fix first.

Call 08 9250 4554 or visit mspsecurity.com.au