Staff cyber security checklist

A 50-point checklist to see whether your team knows how to spot scams, handle passwords and customer information, and work safely from anywhere. Each gap becomes a training topic.

Most security problems in small businesses don't start with clever hacking. They start with a person: someone who clicks a convincing link, pays a fake invoice, reuses a password or leaves a laptop unlocked. Good technology helps, but your team is the part attackers target first.

This checklist helps you find the gaps.

How to use it

Go through each section and tick an item only if you're confident **everyone on your team** knows it and does it. If you're not sure, leave it unticked.

Every unticked box is a topic to cover in your next team meeting, induction or training session. Start with the sections where you have the most gaps.

1. Scams and phishing

Fake emails, texts and calls are the most common way in.

- [ ] **Suspicious links.** Staff check where a link really goes before clicking, and go to important sites by typing the address themselves.
- [ ] **Unexpected attachments.** Staff don't open attachments they weren't expecting, even from people they know, without checking first.
- [ ] **Urgency and pressure.** Staff treat "act now", "your account will be closed" or "pay today" as a warning sign, not a reason to hurry.
- [ ] **Requests from the boss.** Unusual requests from a manager or owner, especially to pay money or buy gift cards, are checked in person or by phone.
- [ ] **Changed bank details.** Any email asking to change a supplier's bank account is confirmed by calling the supplier on a number you already have.
- [ ] **Fake invoices.** Accounts staff check new invoices and account numbers against real orders before paying.
- [ ] **Phone scams.** Staff don't give out passwords, codes or customer details to callers, however official they sound.
- [ ] **Targeted messages.** Staff know scammers use details from social media and LinkedIn to make messages look genuine.

- [ ] **Threats and blackmail.** Staff know not to reply to or pay threatening emails, and to report them instead.
- [ ] **Reporting.** Everyone knows how to report a suspicious message, and feels safe doing it, even if they've already clicked.

2. Passwords and sign-in

- [ ] **Two-step sign-in.** Turned on for email, banking, accounting, the website and ad accounts, and staff understand why.
- [ ] **Long passphrases.** Staff use long passwords made of several words rather than short, complicated ones.
- [ ] **One password per account.** Nobody reuses the same password across work accounts, or between work and personal accounts.
- [ ] **Password manager.** The business provides one, and staff use it instead of notes, spreadsheets or the browser on shared computers.
- [ ] **No sharing.** Each person has their own login. Passwords aren't shared by email, chat or sticky notes.
- [ ] **Sign-in codes.** Staff never read out or forward a sign-in code to anyone, including someone claiming to be from IT or the bank.

3. Customer and business information

- [ ] **Privacy basics.** Staff understand that customer details are protected under the *Privacy Act 1988* and know what they can and can't do with them.
- [ ] **Only what's needed.** Staff don't collect or keep personal information the business doesn't need.
- [ ] **Right recipient.** Staff check the "To" line before sending, because email address autofill is an easy way to send information to the wrong person.
- [ ] **Sharing safely.** Confidential files go through approved work tools, not personal email, personal cloud storage or free online converters.
- [ ] **Checking authority.** Staff confirm someone is allowed to see information before sharing it, even with colleagues.
- [ ] **Printing and paper.** Printouts are collected straight away and confidential paper goes in a secure bin or shredder.
- [ ] **Clear desk.** Confidential documents aren't left on desks or in meeting rooms.
- [ ] **Customer requests.** Staff know what to do when a customer asks to see, correct or remove their information.
- [ ] **Company cards.** Card details are kept secure and only used on trusted sites.
- [ ] **Reporting a mistake.** Staff know to report a data leak or a wrongly sent email straight away, so it can be dealt with quickly.

4. Working from home and on the move

- [ ] **Public wifi.** Staff avoid public or free wifi for work, or use the business's VPN or a phone hotspot.
- [ ] **Home wifi.** Home routers have a strong password and up-to-date software.
- [ ] **Locked screens.** Laptops and phones lock automatically, and staff lock them when they step away, at home as well as in the office.
- [ ] **Family and housemates.** Work devices aren't shared, and work calls and screens are kept private at home.
- [ ] **Public charging.** Staff charge devices with their own charger rather than unknown public USB points.
- [ ] **Travel.** Staff know the extra precautions for working overseas or on holiday.
- [ ] **Devices in cars.** Laptops, phones and documents aren't left in parked cars.
- [ ] **Work email for work.** Work email isn't used to sign up for personal accounts or services.

5. Devices and software

- [ ] **Updates.** Staff install updates promptly on computers, phones and apps, and don't keep postponing them.
- [ ] **Approved software only.** Staff don't install software or browser add-ons on work devices without approval.
- [ ] **Office documents.** Staff don't click "Enable editing" or "Enable content" on documents they weren't expecting.
- [ ] **USB drives.** Found or free USB drives are never plugged in. Removable drives used for work are encrypted.
- [ ] **Unfamiliar devices.** Staff notice and report unknown devices plugged into their computer.
- [ ] **Pop-ups.** Staff close suspicious pop-ups safely and never call phone numbers shown in them.
- [ ] **Ransomware.** Staff know the warning signs and to disconnect and report immediately rather than try to fix it themselves.
- [ ] **Video calls.** Meeting links aren't posted publicly, and hosts use waiting rooms or passwords for external meetings.

6. The office and physical security

- [ ] **Visitors.** Visitors sign in and are accompanied, and staff politely question people they don't recognise.
- [ ] **Tailgating.** Staff don't hold secure doors open for people they don't know.
- [ ] **Shoulder surfing.** Staff are careful entering passwords or viewing confidential information in public. Privacy screens are used where it matters.

- [ ] **Events and after hours.** Access to the workplace is controlled during events and outside business hours.

7. Everyday habits

- [ ] **Social media.** Staff think before posting about work, clients, the office or their role.
- [ ] **Checking sources.** Staff check where information comes from before believing or sharing it.
- [ ] **Training.** New starters get security basics in their first week, and the whole team has a refresher at least once a year.
- [ ] **Culture.** Leaders follow the same rules, and people are thanked, not blamed, for reporting a mistake.

Your score

Count your ticks out of 50.

- **45 to 50:** Strong habits. Keep training regular and review this list each year.
- **30 to 44:** Good foundations with some gaps. Pick the weakest section and cover it with the team this month.
- **Under 30:** Your team is your biggest risk right now. Start with sections 1 and 2, as scams and passwords cause the most damage.

Turn the gaps into a plan

1. **List your unticked items** and group them by section.
2. **Start with scams and passwords.** They're the quickest wins and the most common way in.
3. **Make it short and regular.** Ten minutes in a team meeting each month beats one long session a year.
4. **Back habits up with settings.** Turn on two-step sign-in, automatic updates and screen locks so good behaviour is the default.
5. **Check again in three months.**

Free help

- Scamwatch lists current scams targeting Australians.
- cyber.gov.au has free small business guides, and is where you report cybercrime.
- The Office of the Australian Information Commissioner explains your privacy obligations.
- Our cyber security fundamentals guide covers the technical basics to put in place alongside training.

Where Blend can help

We review who can access your ad, analytics and customer accounts, remove old access, and help you handle customer information in line with the Australian Privacy Principles. See our security and privacy services or get in touch.

This guide is general information, not professional advice for your situation. Read it online and find more free guides at www.blend-datastrategy.com/tools.