Cyber security fundamentals: where to start

Where to start securing your business, your customer data and your staff accounts: two-step sign-in, updates, backups, access, scams and what to do if something goes wrong.

You don't need a security team to make your business much harder to attack. Most incidents that hit small businesses start with something simple: a stolen password, an old account nobody removed, a fake invoice, or software that hasn't been updated. This guide covers the basics, in the order we'd tackle them.

Start with the government's top three

The Australian Signals Directorate's small business advice says: "As a starting point, we recommend the following three":

1. **Turn on multi-factor authentication.** Also called two-step sign-in. It means a stolen password alone isn't enough to get into an account. Start with email, banking, accounting software, your website and your ad accounts.
2. **Update your software.** Turn on automatic updates for computers, phones, browsers and business apps. Updates fix security holes attackers already know about.
3. **Back up your information.** Keep regular backups of important data, store a copy separately from your main systems, and test that you can actually restore from them.

Know what you need to protect

Make a simple list of:

- **Your important accounts:** email, banking, accounting, website, domain name, shop platform, customer database, social media and ad accounts
- **Where customer and staff information is kept,** and who can see it
- **Who has admin access** to each system

You can't protect what you don't know you have.

Control who has access

- **Give each person their own login.** Shared logins make it impossible to tell who did what, or to remove one person's access.
- **Give people only the access they need.** Most staff don't need admin rights.

- **Remove access promptly** when staff, contractors or agencies leave. Check ad accounts, analytics and social media too; these are often forgotten.
- **Review access regularly,** at least a few times a year.
- **Use a password manager** so everyone can have long, unique passwords without writing them down.

Protect against scams

Many attacks target people, not technology.

- **Check payment changes by phone.** If a supplier emails new bank details, call them on a number you already have before paying.
- **Be wary of urgency.** Messages that pressure you to act immediately, pay now or log in to "fix" something are a common trick.
- **Train your team** to spot suspicious emails and texts, and make it easy and safe to report them. Our staff cyber security checklist shows where to start.

Secure your devices and email

- Use screen locks on phones and laptops.
- Turn on the security features already built into your email and office software.
- Keep work data on work-managed devices or approved apps where you can.

Plan for when something goes wrong

Write a one-page plan covering:

- Who to call first (your IT provider, your bank)
- How to lock accounts and change passwords quickly
- Where your backups are and how to restore them
- How to report it

In Australia, you can report cybercrime and cyber security incidents through the Australian Signals Directorate's cyber.gov.au website, which also has a "Have you been hacked?" guide.

Know your privacy obligations

If your business handles personal information, the *Privacy Act 1988* may apply. The Office of the Australian Information Commissioner says the Notifiable Data Breaches scheme generally covers organisations "with an annual turnover of more than $3 million", along with some smaller businesses, for example those that "hold health information and provide a health service" or "trade in personal information". If you're covered and a breach is likely to result in serious harm, you may need to notify affected people and the OAIC. Check the details at oaic.gov.au.

Even if the scheme doesn't apply to you, telling customers promptly and honestly when their information is at risk is the right thing to do.

Next steps

Once the basics are in place, the Australian Signals Directorate recommends working towards Maturity Level One of the Essential Eight, a set of eight mitigation strategies. Their free small business guides and the Essential Eight are at cyber.gov.au.

Where Blend can help

We review who can access your ad, analytics and customer accounts, tidy up old access, and help you handle customer data 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.