business.gov.au (https://business.gov.au/)

Cyber security checklist

Protecting your business from cyber threats is crucial. Scams, email attacks and malicious software can cost a lot of time and money. They can also compromise your sensitive data and reputation. Follow these steps to strengthen your business against cyber threats.

1 Protect your business accounts, information and devices

The Australian Cyber Security Centre (ACSC) has information to help you protect your business and staff from cyber threats.

This includes:

- turning on multi-factor authentication
- using strong passwords or passphrases
- updating software
- backing up information
- protecting your business data
- educating employees.

> **Check out the small business cyber security guide** (https://www.cyber.gov.au/learn-basics/explore-basics/small-business)
>
> → Australian Cyber Security Centre

2 Protect your customers' information

You need to keep your customers' information safe. Losing or compromising their information will damage your business reputation and could have legal consequences.

Make sure your business:

- uses a secure online environment for transactions
- stores any personal customer information securely.

If you take payments online, find out what your payment provider does to prevent online payment fraud.

Australia has laws about what you can do with personal information you collect from customers. You need to understand the **Australian Privacy Principles** (https://www.oaic.gov.au/privacy/australian-privacy-principles) (APPs) and have a clear, up-to-date privacy policy. It's a good idea to display your privacy policy on your business website.

> **Learn more about protecting your customers' information** (https://business.gov.au/online-and-digital/cyber-security/protect-your-customers-information)
>
> → Protect your customers' information

3 Develop a cyber security policy

A cyber security policy helps your staff understand their responsibilities when they use or share:

- data
- computers and devices
- emails
- websites.

> **Find out how to create a cyber security policy** (https://business.gov.au/online-and-digital/cyber-security/create-a-cyber-security-policy)
>
> → Create a cyber security policy

---

4 Create an emergency management plan

An emergency management plan can help you respond to a cyber security incident and reduce its impact.

When creating your emergency management plan, you will need to consider:

- the process to report a cyber security incident
- how you will tell your employees and customers about a cyber security incident
- how to manage your business during a cyber security incident.

> **Download our emergency management plan template** (https://business.gov.au/planning/business-plans/develop-an-emergency-management-plan)
>
> → Develop an emergency management plan

---

5 Consider cyber security insurance

The cost of dealing with a cyber-attack can be much more than just repairing databases, strengthening security or replacing laptops.

Cyber liability insurance can help your business with the costs of an attack. But like all insurance policies, it is important to understand exactly what you are covered for.

> **Learn more about business insurance** (https://business.gov.au/risk-management/insurance/types-of-business-insurance)
>
> → Types of business insurance

---

6 Know where to get cyber security advice

It's important you know where to get support and advice on cyber security.

You can:

- call the Australian Cyber Security Hotline on **1300 292 371** (https://business.gov.autel:1300292371) for support preparing for and responding to cyber incidents
- get help with cyber resilience or recovering from an incident through the **Small Business Cyber Resilience Service** (https://business.gov.au/expertise-and-advice/small-business-cyber-resilience-service)
- get individual support through the **Digital Solutions – Australian Small Business Advisory Services** (https://business.gov.au/expertise-and-advice/digital-solutions-australian-small-business-advisory-services) program. This program gives small businesses low-cost, high-quality advice on digital solutions, including online security
- search online for non-government IT service providers or cyber security professionals.

7 Stay up to date on the latest cyber security risks

It's important to keep up with the latest scams and security risks to your business.

You can:

- become an **Australian Signals Directorate partner** (https://www.cyber.gov.au/become-asd-partner) to receive up-to-date information on cyber security issues and how to deal with them
- **sign up for ACSC alerts** (https://www.cyber.gov.au/about-us/register) or check their **alerts and advisories page** (https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories) regularly.

Read next

Learn more about cyber security for your business (https://business.gov.au/online-and-digital/cyber-security/cyber-security-and-your-business)

→ Cyber security and your business

Find digital tools and software for your business (https://business.gov.au/online-and-digital/digital-tools-and-software)

→ Digital tools and software