Cybersecurity

Fast facts

Cyber crime: the cost to small business

For a small business, even a minor cybersecurity incident can have devastating impacts. In the 2023-24 financial year, the average cost of cyber crime for small businesses increased to $49,600.

The most common ways cyber criminals exploit small business owners are by diverting payments, accessing business bank accounts, and fraudulently submitting tax returns in their names.

If your business is not actively managing its cybersecurity, you're putting at risk your assets, information, technology and reputation.

What is cybersecurity?

Cybersecurity is about protecting your technology and information from accidental or illegal access, corruption, theft and damage.

Cyber criminals look for access to information and data on your business, employees and customers.

Common online threats to your business include phishing emails and texts, malware, ransomware, data breach, hacking, identity theft and scams.

You are responsible for the cybersecurity of your business. To set up, improve and maintain it, you should:

- learn the basics
- take steps to protect your business
- know how to report and recover.

Learn the basics

Use these free government resources to learn the basics quickly:

- The Australian Signals Directorate's Australian Cyber Security Centre (ACSC)
- Exercise in a Box
- Cyber Wardens Program
- Small Business Cyber Resilience Service
- Scamwatch.

They will help you better understand cybersecurity and set up systems and processes so your business can reduce the risk of threats, as well as prepare to respond and recover from an attack.

Protect your business

Protecting your customers' personal information is a legal requirement for many businesses. There are laws about what personal information you collect from your customers and how you store it. Read the Office of the Australian Information Commissioner's guide for small businesses to learn more. Consult with a legal professional if you are unsure.

You should have a cybersecurity policy to protect your business from cyber attacks and respond to any incidents.

A cybersecurity incident response plan helps you minimise the impact of a cybersecurity incident and get back to business as soon as possible. Your cyber incident response plan should be included in your cybersecurity policy.

A digital ID, such as myID, set to the highest identity strength you can achieve, is the most secure way to access ATO online services and help protect you and your client's personal information.

These actions will help you protect your business:

- never leave your information unattended
- make sure each person who accesses government online services on behalf of your business has their own digital ID – do not share your digital ID
- keep your personal information private
- be vigilant about what you share on social media
- monitor your accounts for unusual activity or transactions
- remove system access from past employees and those who no longer need it
- make sure all devices, such as mobiles and laptops, have the latest available security updates
- use a spam filter on your email accounts
- use a secure wireless network.

Consider using eInvoicing in your business to make sending and receiving invoices easier, faster and more secure.

Stay informed of threats

Continually seek education and advice about existing and emerging threats to your business.

For example:

- check the ASD's regular reports, statistics and publications

- check the ATO's scam alert webpage for information and examples on the latest tax and super-related ATO impersonation scams
- sign up for alerts at cyber.gov.au and subscribe to Scamwatch email alerts to stay up to date on the latest cybersecurity threats and scams targeting small businesses.

Report and recover

The ACSC provides directions to respond to cyber threats and scams, as well as information to protect your business from further harm.

For further information and assistance regarding cyber crime, visit their where to get help page.

If you still need help or you are experiencing an incident, call the Australian Cyber Security Hotline on **1300 CYBER1 (1300 292 371)**. It's available 24 hours a day, 7 days a week.

Report all tax-related security incidents including data breaches to the ATO. Phone their Client Identity Support Centre on **1800 467 033** Monday to Friday, 8:00 am–6:00 pm AEST, so that they can apply measures to protect you, your business, staff and clients where necessary.

Review the Office of the Australian Information Commissioner's (OAIC) information about notifiable data breaches to make sure you comply with your obligations under the *Privacy Act 1988*, including the Notifiable Data Breaches (NDB) scheme.

Contact the Small Business Cyber Resilience Service for support to recover from a cyber incident or scam. Call them on **1800 595 160** or visit IDCARE to find out more.

Last modified: 27 Aug 2025