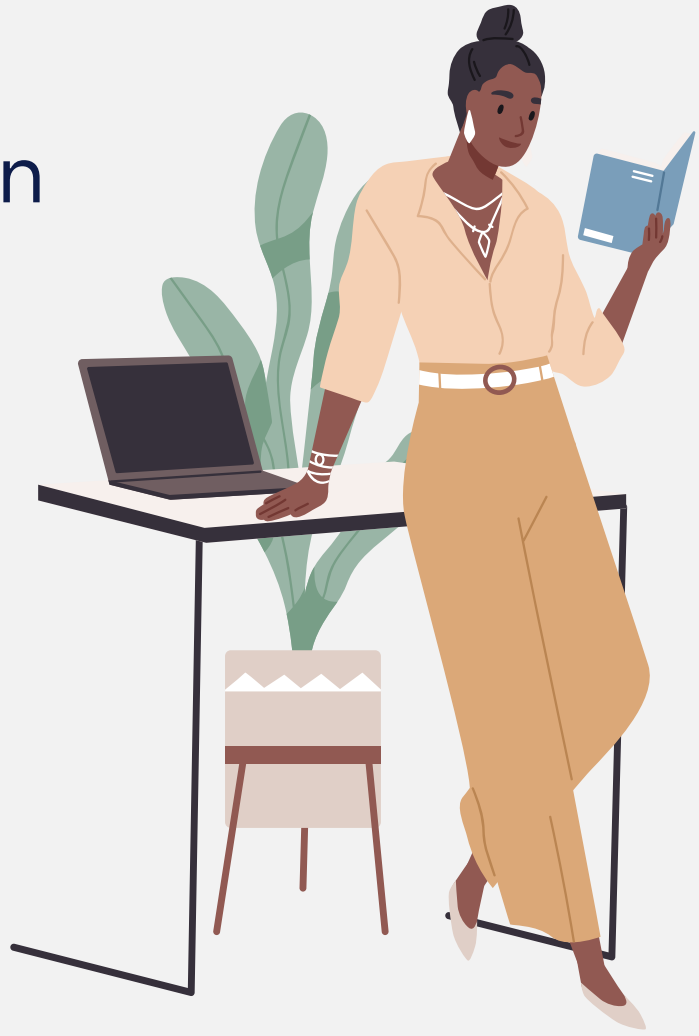
Digital_Support_Tasmania

Staying Secure

What to do when things go wrong online



A Cyber Safety and Resilience Guide for Small Business - Be Prepared not Panicked.

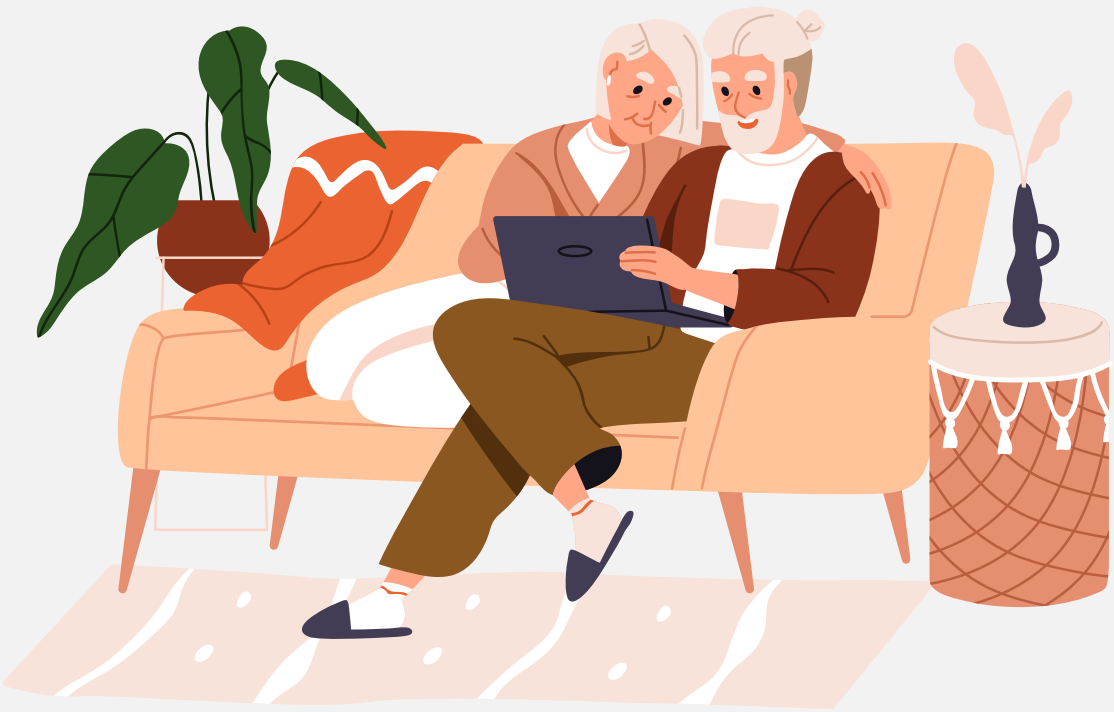
Department of State Growth

Tasmanian Government

Staying Secure -

Cyber Safety Made Easy

May 2025

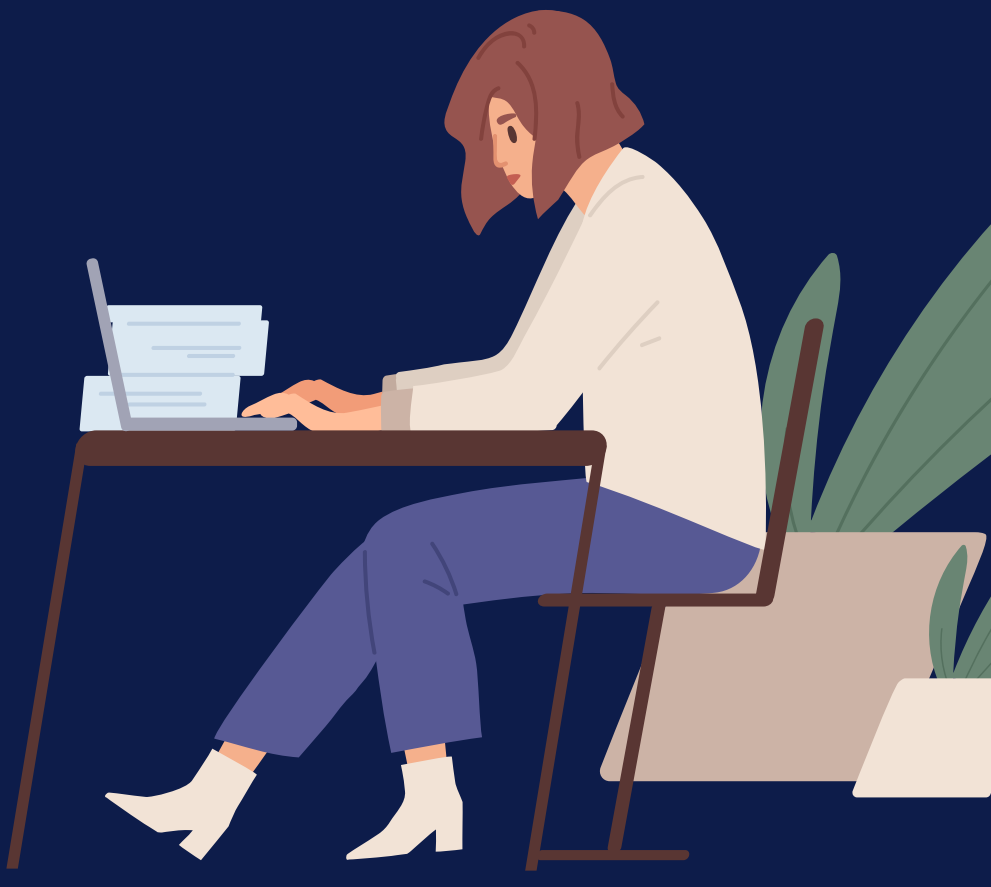


Welcome!

Small businesses make up 97 per cent of businesses in Tasmania and are a critical part of our economy. Since the COVID disruption, businesses are increasingly using technology to conduct their business, whether it is processing transactions using an EFTPOS machine, collecting customer's data and personal information or hosting a website. The use of technology in everyday business is now the new normal.

Being connected safely has never been more crucial not just to your business but to your customers and to the economy. The Australian Cyber Security Centre in their 2023 – 24 report, noted that there was an 8 per cent increase of reported cybercrimes costing small businesses an average of almost $50,000. While this is concerning, there are ways for you to protect yourself and your customers. After all, any disruption to the technology you use may impact your business significantly.

This booklet has been created with your business in mind. It includes some questions for you to answer that are specific to your business and steps you should take to protect yourself and your business.



Introduction

The importance of Cyber Security

As a small business, you collect sensitive data, personal information data and even commercially confidential data. The last thing you want is for that data to fall into the wrong hands. You might think as a small business, why would anyone want to attack your business?

No matter what kind of business you run, a cyber attack can cause serious harm. Whether you are a hairdresser who uses an online booking system that stores your client's contact and payment details or a manufacturer storing commercially confidential data such as designs and proprietary processes online - hackers can steal sensitive information, disrupt your operations, and damage your reputation. This can lead to lost income, unhappy clients/customers, and costly down time that can be hard to recover from. In short, cyber attacks can affect any business, causing both financial losses and long term damage.

We don't leave our house unlocked or our car with the keys in the ignition - because we know someone could break in or steal it. Cyber security is no different. Just like we take steps to protect our physical property, we need to take steps to protect the information stored on our computers and systems.

Many small businesses think they are too small to be targeted, but hackers know that small businesses often have weaker security than large companies. Taking simple steps - like using strong passwords, keeping software updated, and training your staff to spot scams - can make a big difference in protecting your business.

Additional Resources

For further support, these resources offer practical assistance to help protect your business from cyber threats:

Organisation	Contact Details
IDCARE Provides free, confidential support from expert Case Managers.	**Visit idcare.org or call 03 7018 2366**
Australian Cyber Security Centre (ACSC) For immediate support during a cyber incident, contact the ACSC Hotline. The team provides expert advice and can help you manage and recover from cyber attacks. The hotline is available 24 hours a day, 7 days a week.	**Visit cyber.gov.au or call 1300 292 371**
ACSC: Small Business Cyber Security Guide Covers cybersecurity basics, actionable steps, and checklists tailored for small and medium businesses.	**Access the guide at Small Business Cyber Guide** **Visit cyber.gov.au**

Are you prepared?

Follow this flow chart to find out if your business is prepared for a cyber incident...

Step 1: Are you aware of any cyber risks to your business?

- Do you and/or your staff know how to spot and avoid scams (e.g. phishing)?
- Do you have a plan if your business is hacked or if your system is hacked?
- Is access to your business data limited to only specific staff member(s)?

YES

NO/UNSURE

Step 2A: Are you confident that your business could respond effectively to a cyber incident?

- Do you and/or your staff know who to contact and what immediate steps to take if a cyber attack or data breach occurs?
- Is there a written, up-to-date incident response plan that is easy for staff to follow?
- Are important business and customer data regularly and securely backed up?

Step 2B: Take simple actions to build awareness and protect your business.

- Learn how to spot common scams like phishing emails or fake invoices.
- Stay aware of cyber threats that could impact your business (e.g. scam emails, stolen devices).
- Use strong passwords and keep your computer programs updated.

After you do these things, go to Step 2A.

YES

NO

NO/UNSURE

Step 3A: Do you have a documented, up-to-date incident response plan?

- Does your incident response plan clearly outline actions, roles, and responsibilities for responding to incidents?
- Do you and/or your staff know your roles in case of an incident?
- Is your response plan stored in a secure, accessible location?

Step 3B: Review your business operations

- Check where and how you collect, store, or use business or customer data.
- List all the ways your business handles data—like sending invoices, emailing clients, or keeping customer information.
- Decide if the data you handle is sensitive or could cause problems if lost or stolen.
- Ask your staff what information they use or store in their daily work.
- Make sure only trusted people have access to important information.

These steps help you understand your risks and get ready just in case.

When ready, go to Step 3A

YES/NO/UNSURE

Step 4: Review, update and/or Create

- Check your current incident response plan to ensure it reflects your business's latest risks, processes, and contact details.
- Update the plan based on lessons learned from recent incidents, tests, or changes in your business operations.
- If you don't have a plan yet, create a clear, easy-to-follow document that outlines how to respond to cyber incidents, including roles, communication steps, and data backup procedures.

How can I protect my business?

Remember the acronym STAR

1. Stay secure

Set password requirements for your businesses devices – where possible, use multiple factor authentication (MFAs).Do not click on suspicious emails and attachments.

2. Train staff

Ensure you and your staff undergo cyber security training.
Learn about the latest threats occurring around the world and be on guard for those types of attacks.

3. Act fast

If you or one of your staff accidentally clicks a link or encounter a suspicious activity such as an email from an unknown sender, respond quickly by calling 1300 292 371 (Australian Cyber Security Centre Hotline).

4. Refresh regularly

Check your security settings regularly and update your operating systems when notified.

You are now a STAR in protecting your business!

Glossary

This section provides simple definitions for key cybersecurity terms.

Term	Definition
Cyber Incident	A cyber incident is when something goes wrong with your computer systems or online accounts due to a cyber threat. This could include things like being hacked, getting a virus, losing access to your files, or someone stealing your business information. Cyber incidents can stop your business from working properly and put customer data at risk - so it's important to be prepared and know how to respond.
Data back up	A data backup is a copy of your important files and information that is stored in a safe place. You should back up data regularly so you don't lose everything if something goes wrong - like if your computer is hacked, breaks down, or files are accidentally deleted. Backups can be saved on an external hard drive, USB stick, or a secure cloud service. Regular backups mean you can recover your business information quickly and keep running.
Data breach	A data breach is when someone gets access to private or sensitive information without permission. It can happen if a hacker breaks into your system, if someone accidentally shares data, or if a device is lost or stolen. This can include things like customer names, emails, credit card numbers, or business files.
Hacker	A person who tries to gain unauthorised access to computers, networks, or data, often to steal information or cause harm.
IDCARE	A Small Business Cyber Resilience Service delivering free, tailored one-on-one assistance.

Glossary Cont.

This section provides simple definitions for key cybersecurity terms.

Term	Definition
Incident Response Plan	An incident response plan tells you what to do if something goes wrong. For example, being hacked or losing an important file. It should list what steps should be taken in the event of a cyber incident and who to contact.
Long password	A long password means using at least 12 characters, made up of a mix of letters (both upper and lower case), numbers, and symbols. The longer and more complex your password, the harder it is for hackers to guess or crack it (e.g. WdWlwa9p0!).
Multi-factor authentication (MFA)	A security process that requires users to verify their identity using two or more methods, such as a password and a code sent to their phone.
Phishing	Phishing is when someone tries to trick you into giving away personal or business information—like passwords or bank details—by pretending to be someone you trust. It often happens through emails, text messages, or fake websites that look real but are designed to steal your information.
Virtual Private Network	A secure way to connect to the internet that hides your location and encrypts your data, making it harder for hackers to see what you are doing online.

Notes

Disclaimer

This guide is provided to help small businesses understand and improve their cyber security. It offers general information and practical steps but does not cover every possible situation or risk. Following the advice in this guide does not guarantee your business will be fully protected from cyber attacks.

Cyber security is always changing, and new threats can appear at any time. We recommend that you regularly update your knowledge, review your security practices, and seek professional advice if you have specific concerns or face serious incidents.

The Department of State Growth and its partners are not responsible or liable for any damages, losses or expenses incurred as a result of the reliance on information contained in this guide. Use it as a helpful tool, but always stay alert and informed.

Tasmanian Government

Department of State Growth
4 Salamanca Place
Hobart TAS 7000 Australia

Phone: 1800 440 026
Web: https://www.business.tas.gov.au/managing/cyber_security