Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

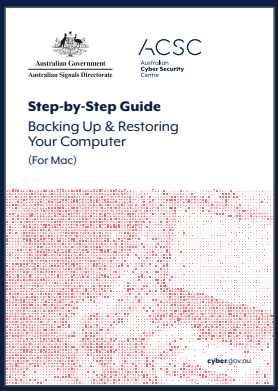
Small Business
Cyber Security Guide

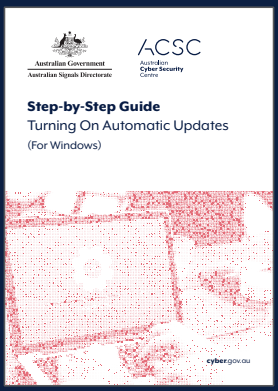
cyber.gov.au

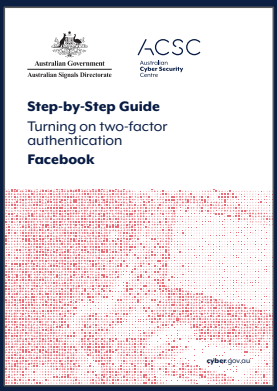
Supplemental Guides

For more cyber security advice to help keep your small business safe, refer to our *Small Business Cyber Security suite* available at cyber.gov.au

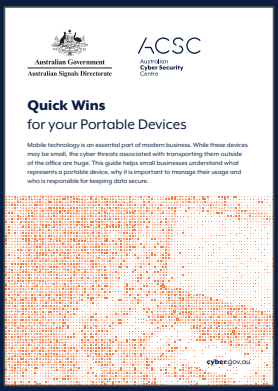
STEP-BY-STEP GUIDES







QUICK WINS



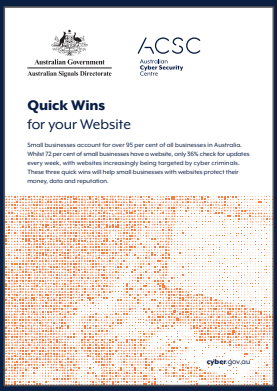


Table of Contents

Foreword

This guide has been developed to help small businesses protect themselves from the most common cyber security incidents.

A cyber security incident that impacts a small business can be devastating. Unfortunately, we at the Australian Cyber Security Centre see the impact of cyber security incidents each and every day, on individuals, large companies, and small businesses.

Luckily, cyber security doesn't have to be difficult. There are simple measures that if understood and implemented, can significantly avoid, or reduce the impact of, the most common cyber security incidents.

We understand that owners and operators of small businesses don't have much time to spend on understanding the complexities of the internet or establishing complicated responses to potential risks. But we also know that cyber security will underpin Australia's economic prosperity, and will allow small businesses to grow, innovate, and find new ways of creating value for their customers.

This Australian Small Business Cyber Security Guide has been specifically designed for small businesses to understand, take action, and increase their cyber security resilience against ever-evolving cyber security threats. The language is clear, the actions are simple, and the guidance is tailored for small businesses.

If you are learning about cyber security for the first time, or are keeping yourself up to date, this guide is an excellent place to start.

If you want to improve your cyber security further, you can find more information and advice on the ACSC website at: www.cyber.gov.au.

The ACSC is here to help make Australia the safest place to connect online.

The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia.

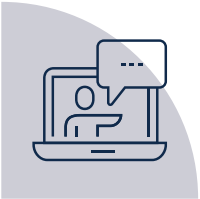
Cyber Threats
Key Areas

For a small business, even the smallest cyber security incident can have devastating impacts.

This section is designed to help small businesses stay alert and prepared. It identifies and explains the most common types of cyber threats and what you can do to protect your business.

Malicious Software
(Malware)

What? Unauthorised software designed to cause harm



Malware is a blanket term for malicious software including viruses, spyware, trojans and worms.

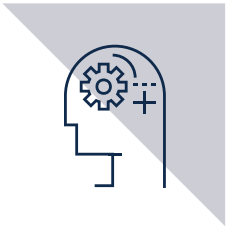
Why? Disrupt. Damage. Deceive.

Typically, for profit.

Malware gains access to important information such as bank or credit card numbers and passwords. It can also take control or spy on a user's computer. What criminals choose to do with this access and data includes:

- Theft
- Pranks
- Activism
- Espionage
- Other serious crimes.

Who? Anyone, anywhere



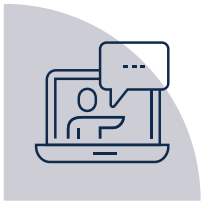
Malware creators can be anywhere in the world. They just need a computer, technical skills and malicious intent. Criminals can easily access cheap tools to use malware against you. It is not personal – they are not targeting you specifically – it is just business.

Protecting against malware

- ☐ Automatically update your operating system
- ☐ Automatically update your software applications
- ☐ Regularly back up your business' data

Scam Emails
(Phishing)

What? 'Dodgy' emails designed to trick recipients out of money and data



Pronounced '*fishing*', they are emails from individuals or organisations you 'think' you know. They mimic phrasing, branding and logos to appear 'real', before conning users to click on a link or attachment. Here, they defraud users by asking them to provide or confirm their personal information, such as passwords and credit card numbers, or to pay a fake account. They can also send an attachment, designed to look genuine, with malware inside.

Who? People with money – it is a numbers game

Phishing emails are typically sent to thousands of people. Even if only a small percentage of recipients fall for the scam, they can net significant data and sums of money.

- **Phishing** *(low sophistication, many targets)*
  Usually general emails with obvious warning signs, sent to thousands of targets
- **Spear Phishing** *(high sophistication, less targets)*
  Fraudulent and sophisticated messages sent to a specific individual, usually the business owner, receptionist or finance and payroll manager
- **Whaling** *(high sophistication, less and high value targets)*
  Spear phishing aimed at very big fish like CEOs

Where? Emails, SMS, Instant Messaging, Social Media

Phishing scams are not limited to emails. They are increasingly sophisticated and harder to spot.

Be cautious of:

- Requests for money, especially if urgent or overdue
- Bank account changes
- Attachments
- Requests to check or confirm login details.

Ransomware

NEVER PAY A RANSOM

You are not guaranteed to regain access,
and may be vulnerable to a second attack.

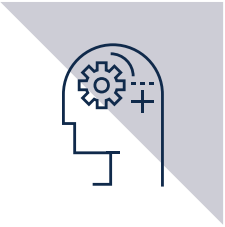
What? Certain malware that locks down your computer and files until a ransom is paid

Ransomware attacks are typically carried out via a malicious but legitimate looking email link or attachment. When downloaded or opened, most ransomware encrypts a user's files, then demands a ransom to restore access – typically payable using cryptocurrency, like Bitcoin.

Why? Money

Ransom, an age-old and effective crime, is now being committed online. Ransomware offers cyber criminals a low-risk, high-reward income. It is easy to develop and distribute. Also in cyber criminals' favour, most small businesses are unprepared to deal with ransomware attacks.

Who? Small, medium and large businesses



Many small businesses are often less security conscious, are less likely to implement cyber security measures, and spend less on cyber security measures.

Prevent and recover from ransomware

- ☐ Update operating systems
- ☐ Update sotware
- ☐ Backup your business

PROTECTING your money & data

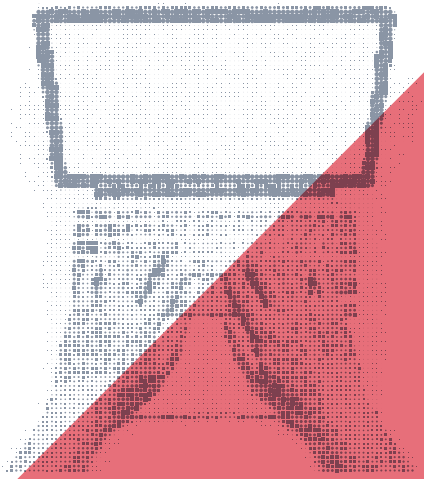
Software Considerations

Key areas

Securely organising your software can drastically increase your business' protection from the most common types of cyber threats.

For example, your operating system is the most important piece of software on your computer. It manages your computer's hardware and all its programs, and therefore needs to be updated, backed up and maintained.

Improve resilience, stay up to date and stay safe with these software considerations for small businesses.



Automatic Updates

What? Software updates

An **update** is a new, improved or safer version of a software (program, app or operating system like Microsoft Windows or Apple iOS) your business has installed on its computers or mobile devices.

An automatic update is a default or **'set and forget'** system that updates your software as soon as one is available.

Why? Safer. Faster. Better.

- **Better** online security
- **Improved** protection (in real-time, directly by the experts) from loss of money, data and identity
- **Enhanced** features and efficiencies for programs and apps.

When? Today & everyday

- **Turn on** or confirm auto-updates, especially for operating systems
- **Regularly check** for and install updates ASAP if auto-updates are unavailable, especially for software
- **Install updates** as soon as possible (if auto-updates unavailable)
- **Set a convenient time for auto-updates** to avoid disruptions to business as usual
- If you use **Anti-Virus software, ensure automatic updates are turned on**

NOTE: If your hardware or software is too old it may not auto-update and leave your business susceptible to technical, software and security issues. The ACSC recommends upgrading your device or software. Windows 7 and Microsoft Office 10 will be unsupported after 14 January 2020 and 13 October 2020 respectively.

Automatic Backups

What? Data backups

A **backup** is a digital copy of your business' most important information e.g. customer details, sales figures. This can be to an external, disconnected hard drive e.g. USB or to the Cloud.

An **automatic backup** is a default or **'set and forget'** system that backs up your data automatically, without human intervention.

Safely disconnecting and removing your back up storage device after each backup will ensure it is also not impacted during a cyber incident

Why? Safer & faster

- **Quicker and easier to get your business back up and running** if information is lost, stolen or destroyed
- **Protects credibility** of your business and help meets legal obligations^
- **Peace of mind** that you're always protected so you can focus your business efforts that deliver value

When? Today & everyday

- **Choose** a backup system that's right for your business
- **Test** you're able to restore your backup regularly
- **Store** a physical backup somewhere safe offsite

^ Certain industries have obligations to keep records for specific periods of time. Make sure you are aware of your business' data retention requirements.

Multi-Factor Authentication

What? A security measure that requires two or more proofs of identity to grant you access

Multi-factor authentication (MFA) typically requires a combination of something the user knows (pin, secret question), physically possesses (card, token) or inherently possesses (finger print, retina).

Why? Significantly more powerful security

The multiple layers make it much harder for criminals to attack your business. Criminals might manage to steal one proof of identity e.g. PIN, but they still need to obtain and use the other proofs of identity. Two-factor authentication (2FA) is the most common type of MFA.

Where? Accessing important internal and external accounts

Small businesses should implement MFA wherever possible. Some MFA options include, but are not limited to:

- Physical token
- Biometrics/ fingerprint
- Email
- Random pin
- Authenticator app
- SMS

People and Procedures

Key areas

Businesses, no matter how small, need to be aware of and consciously apply cyber security measures at every level.

Given small businesses often lack the resources for dedicated IT staff, this section addresses how you can manage who can access, and who can control your business' information, and the training of your staff.

Your internal processes and your workforce are the last, and one of the most important lines of defence in protecting your business from cyber security threats.

Access Control

What? A process to regulate *who* can access *what* within your business' computing environment

Access control is a way to limit access to a computing system.

It allows business owners to:

- Decide who they would like to give access privileges to
- Determine which roles require what access
- Enforce staff access control limits.

Why? To minimise risk of unauthorised access to important information

Many small businesses employ internal staff or outsource work to external suppliers e.g. website hosting companies.

Access control systems help you protect your business by allowing you to limit staff and supplier access to your computer:

- Networks
- Applications
- Files
- Sensitive data.

Who? Principle of least privilege

Depending on the nature of your business, the principle of least privilege is the safest approach for most small businesses. It gives users the bare minimum permissions they need to perform their work. This also reduces the risk of an 'insider' accidentally or maliciously endangering your business.

Quick wins

- ☐ **Restrict administrator privileges**
- ☐ **Do not share passphrases**
- ☐ **Remember to revoke accounts**

Passphrases

What? Using a phrase or sentence, not one word, as your password

A passphrase is similar to a password. It is used to verify access to a computer system, program or service. Passphrases are most effective when they are:

- **Used with multi-factor authentication** – *see page 12*
- **Unique** – *not a famous phrase or lyric, and not re-used*
- **Longer** – *phrases are generally longer than words*
- **Complex** – *naturally occurring in a sentence with uppercase, symbols and punctuation*
- **Easy to remember** – *saves you being locked out.*

Why? Greater security & more convenience

- **Harder to crack** against common password attacks
- **Easier to remember** than random characters
- **Meets password requirements easily** – upper and lower-case lettering, symbols and punctuation

Brute Force Attacks and **Dictionary Attacks**
both generate millions of password/passphrase attempts per second.

Where? For all fixed and mobile devices

Passphrases will significantly increase security across all of your business' devices. See below for a comparison of password vs passphrase security.

PASSWORD/ PASSPHRASE	TIME TO CRACK		EASY TO REMEMBER	COMMENTS
	Brute Force Attack	Dictionary Attack		
password123	Instantly Less than AU$0.01	Instantly Less than AU$0.01	Very Easy (too easy)	One of the most commonly used passwords on the planet.
Spaghetti95!	48 hours AU$587.50	Less than half an hour AU$6.10	Easy	Some complexity in the most common areas, and very short length. Easy to remember, but easy to crack.
5paghetti!95	24 hours AU$293.70	Less than 1 hour AU$12.20	Somewhat Easy	Not much more complexity than above with character substitution, and still short length. Easy to remember, but easy to crack.
A&d8J+1!	2.5 hours AU$30.60	2.5 hours AU$30.60	Very Difficult	Mildly complex, but shorter than the above passwords. Hard to remember, easy to crack (against BFA).
I don't like pineapple on my pizza!	More than 1 Year More than AU$107,222.40	More than 40 days More than AU$11,750.40	Easy	Excellent character length (35 characters). Complexity is naturally high given the apostrophe, exclamation mark and use of spaces. Very easy to remember, and very difficult to crack.

Employee Training

What? Education to protect your staff and business against cyber threats

A cyber security incident response plan can help to change the habits and behaviours of staff and create a sense of shared accountability in keeping your small business safe.

Your cyber security incident response plan teaches staff how to:

- ☐ Recognise
- ☐ Avoid
- ☐ Report
- ☐ Remove
- ☐ Recover

Why? Employees can be the first and last line of defence against cyber threats

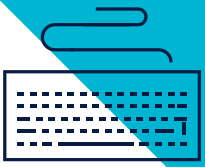
Employees make mistakes. As business owners, you have a legal responsibility to keep your business and customer information safe. That's why having a cyber security training program is vital.

When? Regular cyber security awareness and training

Cyber security is continuously evolving. Keeping everybody up to date could be the difference between whether or not a criminal accesses your money or data.

Quick wins

- ☐ **Incorporate, update and regularly repeat**
- ☐ **Create a cyber security incident response plan**
- ☐ **Reward employees who find threats**
- ☐ **Create a cyber security culture**



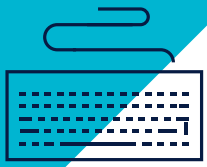
Summary Checklist

SOFTWARE CONSIDERATIONS

- ☐ **Turn on automatic updates for your operating system**
  - ☐ Set up a convenient time for these to occur
- ☐ **Turn on automatic updates for your software applications**
  - ☐ Set up a convenient time for these to occur
- ☐ **Back up your business**, keep backups separated and unconnected from your devices, and regularly ensure you can restore your backups
- ☐ **Enable Multi-Factor Authentication wherever possible**

PEOPLE AND PROCEDURES

- ☐ **Establish an Access Control System to determine who should have access to what**
  - ☐ Restrict administrator privileges to an 'as-required' basis
  - ☐ Do not share passphrases e.g. individual logins
  - ☐ Remember to revoke accounts when employees leave the business
- ☐ **Use strong passphrases**
  - ☐ Use with Multi-factor authentication
  - ☐ Longer
  - ☐ Complex
  - ☐ Unique
  - ☐ Easy to remember
- ☐ **Incorporate, update and regularly repeat cyber security training and awareness amongst your employees**
- ☐ **Create a cyber security incident response plan**
- ☐ **Reward employees who find threats**
- ☐ **Create a cyber security culture and encourage regular discussions**
- ☐ **Always be cautious of emails with the following**
  - ☐ Requests for money, especially if urgent or overdue
  - ☐ Bank account changes
  - ☐ Attachments, especially from unknown or suspicious email addresses
  - ☐ Requests to check or confirm login details.



Glossary

Anti-virus Software
A software program designed to protect your computer or network against computer viruses.

App
Also referred to as a mobile application, an app is a term for software that is commonly used for a smartphone or tablet.

Attachment
A file sent with an email message.

Authenticator App
An app used to confirm the identity of a computer user to allow access and control used within multi-factor authentication.

Biometrics
The identification of a person by the measurement of their biological features, e.g. fingerprint or voice.

Bitcoin
A digital currency (cryptocurrency), used on the Internet for various services.

Brute Force Attack
A type of attack that generates millions of character combinations per second.
They are effective against short or single word passwords.

Cyber Criminal
Any individual who illegally hacks a computer system to damage or steal information.

Data
Data is information including files, text, numbers, pictures, sound or videos.

Default Settings
Something a computer, operating system or program has predetermined for the user.

Dictionary Attacks
A type of attack that generates millions of potential attempts based on rules and databases. These are effective against less complex and commonly used passphrases.

Encryption
The process of making data unreadable by others for the purpose of preventing others from gaining access to its contents.

Network
A collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

Operating System
Software installed on a computer's hard drive that enables computer hardware to communicate with and run computer programs.

Software
Commonly referred to as programs, collection of instructions that enable the user to interact with a computer, its hardware or perform tasks.

Spyware
A program designed to gather information about a user's activity secretly – usually installed without a user's knowledge when they click a link.

The Cloud
A network of remote servers that provide massive, distributed storage and processing power.

Token
A physical device that can usually fit on a keyring, which generates a security code for use with networks or software applications.

Trojans
A type of malware that is often disguised as legitimate software, used by cyber criminals to gain access to users' systems.

Virus
A program designed to cause damage, steal personal information, modify data, send e-mail, display messages or a combination of these actions.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us

cyber.gov.au

call 1300 CYBER1 (1300 292 371)