ever nimble
TECH EXPERTS

Document Name

Small Business Cyber Security Guide

***Disclaimer**: The information in these materials is provided as general information only. Nothing in these materials represents, and must not be relied upon as, legal advice. This information is not tailored to your business's specific needs and may not take into account all relevant laws that may affect you or your business. While every effort has been made to ensure that the contents of these materials are accurate, adequate or complete, it does not represent or warrant its accuracy, adequacy or completeness.*

Foreword

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

A cyber security incident can have devastating impacts on a small business.

We recognise that many owners and operators of small businesses don't have the time or resources to dedicate to cyber security. However, there are simple measures that a small business can introduce to help prevent common cyber security incidents.

Our Small Business Cyber Security Guide has been specifically designed for small businesses to understand, act, 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.

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 ransomware, viruses, spyware and trojans.

Why? Disrupt. Damage. Deceive.
Malware provides criminals with a way to access important information such as bank or credit card numbers and passwords.

It can also take control of or spy on a user's computer. What criminals choose to do with this access and data includes:

- Fraud
- Identity theft
- Disrupting business
- Stealing sensitive data or intellectual property

Who? Anyone, anywhere
Malware creators can be anywhere in the world.

All they need is a computer, technical skills and malicious intent. Criminals can easily access cheap tools to use malware against you. Criminals cast a wide net and go after the most vulnerable. Through implementing cyber security measures and staying alert to threats, you can protect your business from being the easy target

Protecting against malware

- Automatically update your operating system, software and apps
- Regularly backup your important data
- Train your staff to recognise suspicious links and attachments

Scan messages (Phishing)

What? 'Dodgy' emails, messages, or calls designed to trick recipients out of money and data

Criminals will often use email, social media, phone calls, or text messages to try and scam Australian businesses.

These criminals might pretend to be an individual or organisation you think you know or think you should trust.

Their messages and calls attempt to trick businesses into performing specific actions, such as:

- Paying fraudulent invoices or changing payment details for legitimate invoices
- Revealing bank account details, passwords, and credit card numbers (sometimes known as 'phishing' scams, cybercriminals can mimic official branding and logos from banks and websites to seem legitimate)
    - Giving remote access to your computer or server
    - Opening an attachment, which may contain malware
    - Purchasing gift cards and sending them to the scammer

Where? Emails, Social Media, Phone Calls, Text Messages
Phishing scams are not limited to emails. They are increasingly sophisticated and harder to spot.

Be cautious of urgent requests for money, changes to bank accounts, unexpected attachments, and requests to check or confirm login details.

Who? Businesses of all sizes
Scam messages can be sent to thousands of people, or target one specific person.

However, there are common techniques that criminals will use to try and trick your staff. Their messages might include:

- Authority: Is the message claiming to be from someone official or someone senior in the business?
- Urgency: Are you told there is a problem, or that you have a limited time to respond or pay?
- Emotion: Does the message make you feel panicked, hopeful, or curious?
- Scarcity: Is the message offering something in short supply, or promising a good deal?
- Current events: Is the message about a current news story or big event?

Feeling Unsure?

If you think a message or call might truly be from an organisation you trust (such as your bank or a supplier), find a contact method you can trust.

Search for the official website or phone their advertised phone number. Do not use the links or contact details in the message you have been sent or given over the phone as these could be fraudulent.

Ransomware

What? A type of malware that locks down your computer or files until a ransom is paid
Ransomware works by locking up or encrypting your files so that you can no longer use or access them. Sometimes it can even stop your devices from working. Ransomware can infect your devices in the same way as other malware. For example:

- Visiting unsafe or suspicious websites
- Opening links, emails or files from unknown sources

- Having poor security on your network or devices (including servers)

Why? Money
Ransomware offers cybercriminals a low-risk, high-reward income. It is easy to develop and distribute.

Ransoms are typically paid using an online digital currency or cryptocurrency such as Bitcoin, which is very difficult to trace. Also in cybercriminals' favour, most small businesses are unprepared to deal with ransomware attacks.

Who? Small, medium and large businesses
Small businesses can be particularly vulnerable, as they are less likely to implement cyber security measures that could help prevent and recover from ransomware.

Never Pay A Ransom

Paying a ransom does not guarantee a victim's files will be restored, nor does it prevent the publication of any stolen data or its on-sale for use in other crimes. It also increases the likelihood of a victim being targeted again.

If you experience a ransomware incident and require support, call the ACSC's 24/7 Hotline on 1300 CYBER1 (1300 292 371).

Irrespective of the decision to pay a ransom, victims are encouraged to report ransomware incidents to the ACSC at cyber.gov.au. Sharing information about incidents helps to protect other Australian businesses.

Prevent And Recover From Ransomware

- Regularly backup your important data
- Automatically update your operating systems, software and apps
- Where possible, require multi-factor authentication to access services
- Audit and secure your devices (including servers if you have them) and any internet exposed services on your network (Remote Desktop, File Shares, Webmail). Discuss this with an IT professional if you are unsure.

Software Considerations: Key Areas

Managing your software, data, and online accounts 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 regularly to ensure you are always using the most secure version.

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

Automatic updates

What? Software Updates
An update is an improved version of software (programs, apps and operating systems) you have installed on your servers, computers and mobile devices.

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

Why? Security

- Keeping your operating system and applications up to date is one of the best ways to protect yourself from a cyber security incident
- Regularly updating your software will reduce the chance of a cybercriminal using a known weakness to run malware or hack your device
- Saving you time and worry, automatic updates are an important part of keeping your devices and your data safe

When? Today & Everyday

- Turn on automatic updates, especially for operating systems
- Regularly check for updates if automatic updates are unavailable
- If you receive a prompt to update your operating system or other software, you should install the update as soon as possible
- Set a convenient time for automatic updates to avoid disruptions to

business as usual
- If you use antivirus software, ensure automatic updates are turned on

Note:

If your hardware or software is too old, it may be unable to update and could leave your business vulnerable to security issues.

The ACSC recommends upgrading your device or software as soon as possible.

As of 2020, Windows 7, Microsoft Office 2010 and Windows Server 2008 have reached end of support and are no longer secure.

Automatic backups

What? Data Backups

A backup is a digital copy of your business' most important information e.g., customer details and financial records. This can be saved to an external storage device 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 backup storage device after each backup will ensure it remains secure during a cyber incident.

Why? Simple Recovery

- Backing up is a precautionary measure, so that your data is accessible in case it is ever lost, stolen or damaged
- Allows your business to recover from a cyber incident (such as ransomware) and minimises downtime
- Protects credibility of your business and helps to meet legal obligations

When? Today & Everyday

- Choose a backup system that's right for your business. Consider what you can afford to lose in a worst-case scenario to help guide requirements such as how often you backup your data
- Test your backups regularly by attempting to restore data
- Always keep at least one backup disconnected from your device, preferably at an offsite location in case of natural disasters or theft
- Do not connect your backup to devices that are infected with ransomware or viruses

Note:

Certain industries have obligations to keep records for specific periods of time. Make sure you are aware of your 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 you know (password/passphrase, PIN, secret question)
- something you have (smartcard, physical token, authenticator app)
- something you are (fingerprint or other biometric)

Why? Significantly more powerful security
MFA is one of the most effective ways to protect against unauthorised access to your valuable information and accounts.

The multiple layers make it much harder for criminals to attack your business. Criminals might manage to steal one proof of identity such as your password, but they still need to obtain and use the other proofs of identity to access your account.

Where? Accessing important accounts
Small businesses should implement MFA on important accounts wherever possible, prioritising financial and email accounts.

Some MFA options include, but are not limited to:

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

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.

Given small businesses often lack the resources for dedicated IT staff, this section addresses how you can manage access to information in your business, secure your business accounts, and train your staff how to prevent, recognise and report cyber security incidents.

Access control

What? Managing who can access what within your business' computing environment

Access control is a way to limit access to a computing system. It helps protect your business by restricting access to:

- Files and folders
- Applications
- Databases
- Mailboxes
- Online accounts

- Networks

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.

Why? To minimise risk of unauthorised access to important information
Typically, staff do not require full access to all data, accounts, and systems in a business in order to perform their role.

This access should be restricted where possible, so that employees and external providers do not accidentally or maliciously endanger your business.

Access control systems and procedures allow a business owner or operator to:

- Decide who should access certain files, databases, and mailboxes
- Control any access permitted to external providers e.g., accountants, website hosting providers
- Restrict who has access to accounts such as supplier websites and social media
- Reduce potential damage if any accounts, devices, or systems are compromised
- Revoke access to systems and data when an employee changes roles or leaves the business

Access Control Principles

- Transition your employees from 'Administrator' accounts to standard accounts on business devices
- Review access permissions on digital files and folders
- Do not share accounts or passphrases/ passwords between staff
- Remember to revoke access, delete accounts and/or change passphrases/passwords when an employee leaves, or if you change providers

Passphrase

What? A more secure version of a password
Multi-factor authentication is one of the most effective ways to protect your accounts from cybercriminals.

However, if MFA is not available, then you should use a passphrase to protect your account.

A passphrase uses four or more random words as your password. For example, 'crystal onion clay pretzel'.

Why? Secure and easy to remember
Passphrases are hard for cybercriminals to crack, but easy for you to remember.

Create passphrases that are:

- Long: The longer your passphrase, the better. Make it at least 14 characters in length.
- Unpredictable: use a random mix of unrelated words. No famous phrases, quotes or lyrics.
- Unique: Do not reuse passphrases on multiple accounts.

If a website or service requires a complex password including symbols, capital letters, or numbers, you can include these in your passphrase. Your passphrase should still be long, unpredictable and unique for the best security.

Where? Your accounts and devices
If you are unable to use MFA on an account or device, it is important to use a passphrase to stay secure.

In these situations, a secure passphrase may be the only barrier between adversaries and your valuable information. Remember to make your passphrases unique, as reusing a password makes it easy for a cybercriminal to hack multiple accounts.

Consider Using A Password Manager

Password managers (which can also be used to store passphrases) enable good cyber security habits.

Having a unique passphrase for every valuable account may sound overwhelming; however, using a password manager to save your passphrases will free you of the burden of remembering which passphrase goes where.

Ensure that any password manager you use comes from a trusted and reputable source and is protected with its own strong and memorable passphrase.

Employee training

What? Education to protect your staff and business against cyber threats
Teach yourself and your staff how to prevent, recognise and report cybercrime.

Train your employees in cyber security basics, including updating their devices, securing their accounts, and identifying scam messages.

You should also consider implementing a cyber security incident response plan to guide your business and your staff in the event of a cyber incident.

This will help you understand your critical devices and processes, as well as key contacts that you can use to respond and recover.

Why? Employees can be the first and last line of defence against threats
Training can change the habits and behaviour of staff and create shared accountability in keeping your business safe.

Cyber security is everyone's responsibility.

When? Regular cyber security awareness and training
Cyber security is continuously evolving.

Keeping everybody up to date on cyber security threats could be the difference between whether or not a criminal gains access to your money,

accounts or data.

Teach yourself and your staff how to prevent, recognise and report cybercrime.

Cyber security awareness tips

- Train your staff to recognise suspicious links and attachments
- Provide updated cyber security training on a regular basis
- Create a cyber security incident response plan Encourage a strong cyber security culture
- Share examples of scam messages to help staff identify cyber security threats

Summary Checklist

Software considerations

Automatically update your operating systems, software and apps

- If you receive a prompt to update your operating system or other software, you should install the update as soon as possible
- Set a convenient time for automatic updates to avoid disruptions to business as usual

People and procedures

Manage who can access what within your business

- Use the principle of least privilege for access permissions
- Remember to delete accounts and/or change passphrases/passwords when an employee leaves

Where MFA is not possible, use passphrases to protect accounts and devices

- Passphrases are most effective when they are long, unpredictable and unique

Regularly backup your important data

- Always keep at least one backup disconnected from your device

Enable MFA on important accounts wherever possible

- MFA is one of the most effective ways to protect your valuable information and accounts
- Prioritise financial and email accounts for maximum effect

Train your staff in cyber security basics

- This may include updating their devices, securing their accounts, and identifying scam messages
- Provide updated cyber security training on a regular basis