Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Commonwealth Bank

Small business cyber security guide

Content Complexity
SIMPLE

cyber.gov.au

Introduction

For a small business, even a minor cyber security incident can have devastating impacts.
This guide includes basic security measures to help protect your business against common cyber security threats. As a starting point, we recommend the following three measures:

- Turn on multi-factor authentication
- Update your software
- Back up your information

This guide might include measures that are not relevant to your business, or your business may have more complex needs. After completing this guide, we recommend small businesses implement Maturity Level One of the Essential Eight. If you have questions about this advice or cyber security more broadly, we recommend you speak to an IT professional or a trusted advisor.

Visit cyber.gov.au to read our full guide, including how-to advice for each measure.

Table of Contents

Threats to small businesses

Scam messages

Scams are a common way that cybercriminals target small businesses. Their goal is to scam you or your staff into:

- sending money or gift cards
- clicking on malicious links or attachments
- giving away sensitive information, such as passwords.

Cybercriminals may try and scam your business through email, text messages, phone calls and social media. They will often pretend to be a person or organisation you trust.

Phishing attacks

Of particular concern to small businesses are **phishing attacks**. These scams often contain a link to a fake website where you are encouraged to log in to an account or enter confidential details.

Phishing attacks typically compromise your account passwords. Cybercriminals often use this method to "takeover" the social media accounts of small businesses and hold them to ransom.

Ways to mitigate

If a message is from a known entity and seems suspicious, use caution. Contact the person or business separately to check if message is legitimate. Use contact details you find through a legitimate source, for instance by visiting the business's official website, and not those contained in the suspicious message.

Learn more about identifying scams and phishing attacks with the following resources:

- Recognise and report scams
- Learn how to spot phishing scams
- Detecting Socially Engineered Message

Case study:

An employee at a courier company received an email from one of their executive staff, asking that they purchase 6 x $500 MasterCard prepaid credit cards. The executive told her to keep it confidential as the cards would be gift vouchers for staff members. Once purchased, the employee was asked to photograph both sides of the cards and send them through to the Executive as proof of purchase.

As instructed, the employee went to a post office and used her personal credit card to purchase the gift cards. She replied to the executive's email and sent through photos of the gift cards as proof.

After returning from the post office, the employee gave the physical cards to the executive – who had no knowledge of them. On review, **all emails about the gift cards came from a random email address and were not from the executive's legitimate email account. It had been a scam.**

Email attacks

In addition to scams like phishing, a common email attack against small businesses is **business email compromise** (BEC). Criminals can impersonate business representatives by using compromised email accounts, or through other means – like using a domain name that looks similar to a real business. Aside from stealing information, the goal of these attacks is usually to scam victims into sending funds to a bank account operated by the scammer.

Ways to mitigate

The best defence against email attacks is training and awareness for your employees. Ensure your staff know to always be cautious of emails with the following:

- requests for payments, especially if urgent or overdue
- change of bank details
- an email address that doesn't look quite right, such as the domain name not exactly matching the supplier's company name.

While these attacks can be devastating, the mitigation measures are easy and cost almost nothing. **When staff receive emails like this, the most effective mitigation is to call the sender to confirm they are legitimate.** Do not use the contact details you have been sent as these could be fraudulent. Introduce a formal process for staff to follow when payment requests are received or bank details are changed.

Learn to protect your business from BEC scams and email compromise with the following resources:

- Business email compromise
- Protect your business from email fraud and compromise
- What to do if your business has been targeted by email fraud or compromise

Case study:

A small construction business received an email from their supplier saying they had changed banks. The supplier provided new account details for invoice payments. Because the email seemed legitimate, **the construction business did not call the supplier to confirm the change in bank account details.**

The business paid an invoice from the supplier for over $70,000. The following day, another employee mistakenly paid the same invoice again for an additional amount over $70,000. In total, over $150,000 was paid to the new bank account.

When the business rang their supplier to ask if they could refund the duplicate payment, the supplier advised those banking details were incorrect. An investigation was launched immediately, and the supplier discovered that one of their email accounts had been hacked and was sending out fraudulent bank account details. **No funds were recovered.**

Malicious software

Malware is a blanket term for malicious software designed to cause harm, such as ransomware, viruses, spyware and trojans. Malware can:

- steal or lock the files on your device
- steal your bank or credit card numbers
- steal your usernames and passwords
- take control of or spy on your computer.

Malware can stop your device from working properly, delete or corrupt your files, or allow others to access your personal or business information. If your device is infected with malware, you could be vulnerable to other attacks. The malware could also spread to other devices on your network.

Your device can be infected by malware in a number of ways, including:

- visiting websites that have been infected by malware
- downloading infected files or software from the internet
- opening infected email attachments.

Ransomware

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cybercriminals might also threaten to publish or sell data online, unless a ransom is paid.

Ways to mitigate

While anti-virus or security software can help protect you from malware, no software is 100% effective. Staff must be vigilant with emails, websites and file downloads, and regularly update their devices to stay secure.

See the following resources for more information on protecting your business from ransomware:

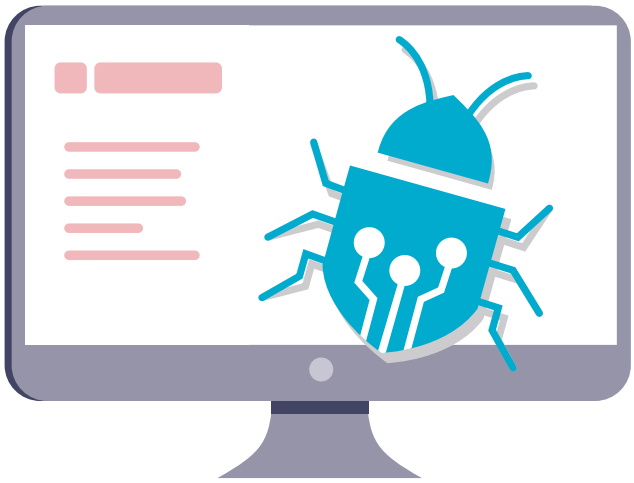
- Ransomware
- Protect yourself against ransomware attacks
- What to do if you're held to ransom

Case study:

Employees of an auto parts store came into work one morning and were not able to boot their server computer. When their IT provider got access to the server, they found a window open that said all the computer data had been encrypted. The note demanded they pay a ransom in bitcoin to unlock the files.

There was a backup drive plugged into the computer, which had also been encrypted. They tried to connect more backup drives, but the files were automatically encrypted within seconds. **They had failed to remove the ransomware before attempting to recover their data and lost every backup file they had.**

The only option left was to factory reset the server and start fresh with a new system. Their business lost many years of data and had to start over.



Secure your accounts

Turn on multi-factor authentication

Multi-factor authentication (MFA) makes it harder for cybercriminals to access your accounts.

MFA adds another layer of security to your account. It is one of the most effective ways to protect your accounts from someone getting access, so you should use it wherever possible. Anyone who logs into your account will need to provide something else in addition to your username and password. This could be a unique code from a text message or an authenticator app. For more information, read our advice on MFA, available at **cyber.gov.au/mfa**.

✓ **Turn on MFA wherever possible, starting with your most important accounts.**

Implement access controls

Restricting user access can limit the damage caused by a cyber security incident.

Access control is a way to limit access to certain files and systems. Typically, staff do not require full access to all data, accounts, and systems in a business. They should only be allowed to access what they need to perform their duties.

Restricting access will help limit the damage caused by a cyber security incident. For example, if a staff member's computer is infected with ransomware, with proper access controls it might only affect a small number of files rather than the entire business.

✓ **Ensure each user can access only what they need for their role.**

Use strong passwords or passphrases

Protect your accounts from cybercriminals with a secure password or passphrase.

Many small businesses face cyber attacks as a result of poor password behaviours. For example, reusing the same password on multiple accounts. You can use both password managers and passphrases to create strong passwords.

A **password manager** acts like a virtual safe for your passwords. You can use it to create and store strong, **unique** passwords for each of your accounts. If you have a lot of accounts, this removes the burden of remembering unique passwords. You don't have to remember the passwords or the accounts they belong to, as it is all recorded in your password manager.

For accounts that you sign into regularly, or that you otherwise don't want to store in a password manager, consider using a passphrase as your password. Passphrases are a combination of random words, for example 'crystal onion clay pretzel'. They are useful when you want a secure password that is easy to remember. Use a random mix of four or more words and keep it unique – **do not reuse a passphrase** across multiple accounts. For more information, read our read our advice on passphrases and password managers, available at **cyber.gov.au/passphrases**.

✓ **Use a password manager to create and store unique passwords for each of your important accounts.**

Manage shared accounts

Sharing accounts can compromise security and makes it difficult to track malicious activity.

In a small business, there may be legitimate reasons why staff need to share accounts, but it should be avoided as much as possible. When multiple staff use the same account it can be hard to track activity back to a specific employee and even harder to track cybercriminals breaking in. Unless you change the password, employees could also continue accessing accounts even after they have left the business.

✓ **Limit the use of shared accounts and secure any that are used in your business.**

Protect your devices and information

Update your software

Keeping your software up-to-date is one of the best ways to protect your business from a cyber attack.

Updates can fix security flaws in your operating system and other software, so that it is harder for a cybercriminal to break in. New flaws are discovered all the time, so don't ignore prompts to update. Regularly updating your software will reduce the chance of a cybercriminal using a known weakness to run malware or hack your device. If you need help, the ACSC has published guidance on updates.

If your device or software is too old, then updates may not be available. If the manufacturer has stopped supporting the product with updates, you should consider upgrading to a newer product to stay secure. Examples of systems that no longer receive major updates are the **iPhone 7** and **Microsoft Windows 7**.

For more information read our guidance on updates, available at **cyber.gov.au/updates**.

✓ **Turn on automatic updates for your devices and software.**

Use security software

Security software such as antivirus and ransomware protection can help protect your devices.

Use security software to detect and remove malware from your devices. Antivirus software can be set up to regularly scan for suspicious files and programs. When a threat is found, you will receive an alert and the suspicious file will be quarantined or removed.

Many small businesses can **use Windows Security** to protect themselves from viruses and malware. Windows Security is built-in to Windows 10 and Windows 11 devices and includes free virus and threat protection. You can also use it to turn on ransomware protection features on your device.

For alternative products and options, read our advice on antivirus software, by searching *antivirus* on cyber.gov.au.

✓ **Set up security software to complete regular scans on your devices.**

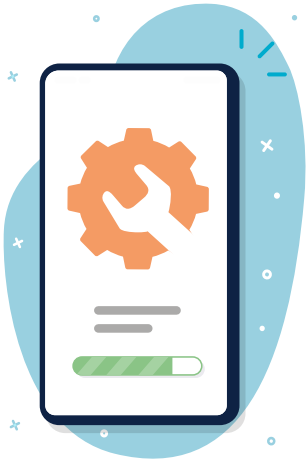
Back up your information

Regular backups can help you recover your information if it is lost or compromised.

Backing up important information should be a regular or automatic practice in your business. Without a regular backup, it could be impossible for you to recover your information after a cyber attack.

There are many methods and products you could use to back up your information. For detailed advice on backing up your business, read our advice for backups, available at **cyber.gov.au/backups**. The best option will vary for each business, so speak with an IT professional if you are unsure.

✓ **Create and implement a plan to regularly back up your information.**



Secure your network and external services

Protect your business from a cyber attack by addressing potential vulnerabilities in your network.

The devices and services in your network can be a prime target for cybercriminals. Many of these systems can be complex to secure, so discuss the following recommendations with an IT professional.

- **Secure your servers**: If you use a NAS or other server in your home or business, take extra care to secure them. These devices are common targets for cybercriminals because they often store important files or perform important functions. There are many mitigation strategies required to protect these devices. For example, it's important to ensure any server or NAS devices are updated regularly. Administrative accounts should be secured with a strong passphrase or multi-factor authentication.
- **Minimise external-facing footprint**: Audit and secure any internet exposed services on your network. This might include Remote Desktop, File Shares, Webmail and remote administration services.
- **Migrate to cloud services:** Consider using online or cloud services that offer built-in security, instead of managing your own. For example, use online services for things like email or website hosting rather than running and securing these services yourself.
- **Improve your router's security:** Follow our guidance on ways to secure your router, including updating default passwords, turning on "Guest" Wi-Fi for customers or visitors, and using the strongest encryption protocols. Search *router* on **cyber.gov.au** for more information.
- **Understand your cyber supply chain:** Modern businesses often outsource multiple services. For example, using a Managed Service Provider to maintain their IT. Security issues with these services or providers could have a significant impact to your business. For detailed advice on cyber supply chain risk management read our Cyber Supply Chain Guidance on **cyber.gov.au**.

✓ **Speak to an IT professional about ways to secure your network.**

Harden your website

Websites are a prime target for cyber attacks.

Protect your website from being hijacked by following some basic security measures:

- secure your website login with multi-factor authentication or a strong password
- regularly update your website's content management systems and plugins
- back up your website regularly so you can restore it after a cyber attack.

The ACSC has additional resources available for website owners. Search for these resources on **cyber.gov.au**:

- Quick Wins for your Website
- Implementing Certificates, TLS, HTTPS and Opportunistic TLS
- Domain Name System Security for Domain Owners
- Preparing for and Responding to Denial-of-Service Attacks

✓ **Read through the ACSC resources on website security.**

Reset your devices before selling or disposing of them

The data on your old devices could be accessed by strangers.

If you do not dispose of your devices securely, cybercriminals could access the information on it. This could include emails, files and other business data. Remove all information from your business devices before selling, trading or throwing them away. For example, by doing a factory reset. This will help wipe any information and restore the device to its original settings.

For advice on resetting your devices, read our guidance on how to dispose of your device securely. Search *dispose* on **cyber.gov.au**.

✓ **Perform a factory reset before selling or disposing of business devices.**

Keep your devices locked and physically secure

Restricting access to your business devices will reduce opportunities for malicious activity.

Limiting physical access to your business devices is a simple way to prevent data being stolen or other malicious activity. Business devices should not be kept where unauthorised staff or members of the public could access them.

Use security controls to further protect your business devices. At a minimum, they should be locked with a passphrase, PIN or biometrics. Ensure these devices are set to automatically lock after a short period of inactivity.

✓ **Configure devices to automatically lock after a short time of inactivity.**

Protect your business data

Data held by your business is an attractive target to cybercriminals.

Data breaches are on the rise – don't let your business fall victim. It's important to understand what data your business holds, and in what locations. Once you're aware, use the recommendations in this guide to help protect your data from being accessed by cybercriminals. Some small businesses may also have additional obligations under legislation.

- **Consolidate your business data.** You might have data stored across numerous devices or services. When data is decentralised, it increases the number of systems you have to keep secure and backed up. Numerous systems can also create more opportunities for a cybercriminal to attack. Where possible, store your business data in a central location that is secure and backed up regularly. Centralising your data can create a bigger breach if your systems are compromised, so ensure this central location is adequately protected with secure configurations and restricted access. Speak to an IT or cyber security professional for advice.
- **Know your obligations for protecting data.** Some small businesses may have legal obligations for handling personal information they collect. Read the Office of the Australian Information Commissioner's guide for small businesses to learn more, available at **oaic.gov.au**. Consult with a legal professional if you are unsure.

✓ **Understand the data your business holds and your responsibilities to protect it.**

Prepare your staff

Educate employees

Employees with good cyber security practices are your first line of defence against cyber attacks.

Your employees should have an awareness of cyber security, including the following topics:

- common cyber security threats such as business email compromise and ransomware
- protective measures including strong passwords or passphrases, MFA and software updates
- how to spot scams and phishing attacks
- business specific policies (for example, processes for reporting suspicious emails or for validating invoices are genuine before paying)
- what to do in an emergency.

The ACSC website has resources for most of these topics at cyber.gov.au/learn. You might consider other ways of educating your employees, for example with a formal course or internal training. However you decide, remember that cyber security training isn't a once-off requirement and should be refreshed periodically.

✓ **Determine how cyber security awareness will be taught in your business.**

Make an emergency plan

An emergency plan could reduce the impact of a cyber attack on your business.

When responding to a cyber security incident, every minute accounts. Having an emergency plan means your staff can spend less time figuring out what to do and more time taking action.

Consider the following questions when creating your emergency plan:

- What is the process for your staff to report potential cyber security incidents?
- Who do you contact for assistance? For example, IT professionals and your bank.
- How will the incident be communicated to your staff, stakeholders, or customers?
- How will you manage business as usual, if any critical systems are offline?

Make sure your staff are familiar with the emergency plan, including any roles or responsibilities they may have. Maintain a hard copy of the plan in case your systems are offline when you need it.

✓ **Create an emergency plan for cyber security incidents.**

Stay informed

Become an ACSC partner to receive the latest information from the ACSC.

Stay informed of the latest cyber threats and vulnerabilities by becoming an ACSC partner. This service will send you monthly newsletters and alerts when a new cyber threat is identified.

Cyber security is a rapidly evolving field. Cybercriminals actively exploit vulnerabilities within minutes of their discovery. Staying informed of the cyber security landscape will help your business to understand the threats it is likely to face and how to protect against them.

✓ **Register your business with the ACSC Partnership Program.**

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.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre