



Australian Government
Australian Signals Directorate

cyber.gov.au

Small business cyber security handbook

Fundamental steps to protect your business and staff from cyber threats



Why **cyber security** matters for your business

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

This handbook includes basic security measures to help protect your business against common cyber threats. As a starting point, we recommend the following three measures:

- **Turn on multi-factor authentication**
- **Keep your software up to date**
- **Regularly back up your data**

This handbook might include measures that are not relevant to your business, or your business may have more complex needs.

We understand that small businesses have varying degrees of technical skills and resources impacting their ability to implement advice. If you have questions about this advice or cyber security more broadly, we recommend you speak to an IT professional, a trusted advisor or seek additional guidance at cyber.gov.au.





Top tips for small business

Implement fundamental cyber security controls	5
Educate staff on good cyber security practices	6
Restrict and monitor access to system and data	8
Use Secure by Design products and services	9
Implement and test cyber security incident response plans	10

Detailed advice for enhancing small business cyber security

Common cyber threats to small businesses	12
Securing accounts and identities	18
Protecting devices, systems and networks	21
Protecting business & customer data	27
People, training and incident readiness	30
Remote working security	31
Using AI securely in your business	33

Advanced cyber security advice for small business

Event logging	37
Post-quantum cryptography	38

Top tips for small business



Implement fundamental cyber security controls

Implementing fundamental cyber security measures helps protect small businesses from common cyber threats. Businesses should enable multi-factor authentication (MFA), use passkeys, use strong, unique passwords across all systems and accounts, and apply security patches as soon as possible. These measures reduce the risk of unauthorised access and compromise and form the foundation of good cyber security practice.

Set up multi-factor authentication

- MFA is when you need two or more different ways to verify you are the account owner before you log in. For example, after entering your password you might get a code on your authenticator app or need to use your fingerprint.
- It's an extra layer of security that verifies you are the true account owner.

Use passkeys

- Passkeys are a more secure way to log in to your online accounts than using passwords.
- A passkey lets you log in to your online account without having to enter a password for that account.
- A passkey is like a set of apartment keys kept in a safe. You need a PIN to open the key safe that gives you access to a key that allows you to unlock a door in the building.

Use unique and strong passwords (where use of a passkey is unavailable)

- Always use unique passwords for each of your online accounts.
- Never reuse passwords across multiple devices and services.
- Use a password manager to help securely store your passwords.
- Make your password long and hard to guess, especially if you are unable to use MFA.
- Keep your passwords private. Sharing them may put your data, devices and identity at risk.
- Change your passwords if you think they have been compromised.

Apply security patches

- Regularly update your systems, devices and applications to avoid security vulnerabilities that cyber criminals could exploit.
- Apply updates promptly, especially critical security patches for internet-facing systems such as websites.
- Monitor and act on vendor advice for newly discovered risks.
- Where available turn on automatic updates.
- Remove or replace device and software that no longer receives security updates.



Educate staff on good cyber security practices

Cyber security is continuously changing. As business owners, you have a legal responsibility to keep your business and customer information secure. Keeping your employees up to date on cyber security could prevent a cybercriminal accessing your business, money or data.

Cyber security awareness training

Cyber threats evolve quickly, so training should be ongoing rather than a one-time activity.

- Provide regular, up-to-date training sessions on common threats like phishing, ransomware and social engineering.
- Educate staff on safe browsing habits and how to avoid malicious websites.
- Emphasise the risks of downloading unknown files or using unsecured external devices.
- Promote security-first culture by emphasising that cyber security is everyone's responsibility.
- Create a positive cyber security culture by encouraging staff to report any suspicious activities.
- Provide up-to-date information and alerts in staff common areas.

Be aware of email security and phishing techniques

Being aware of email security risks and phishing techniques is essential for protecting your business from cyber threats. Cybercriminals commonly use phishing emails to trick users into revealing sensitive information or installing malicious software. If you are not vigilant, cybercriminals may gain access to and take control of your business email account.

Common email phishing techniques

- Email spoofing – cybercriminals imitate the sender's address so the email appears to come from a trusted source like your manager or IT team.
- Business email compromise – cybercriminals impersonate executives or suppliers to trick you into sending money, for example via a fake invoice. Always verify payment recipients before sending money.
- Malicious attachments – emails include infected files that install malware when opened.
- Credential harvesting – emails contain links to fake login pages that look real and are designed to steal login credentials.



Business email compromise

- Business email compromise is a form of targeted phishing, or spear phishing.
- Cybercriminals use email to pretend to be trusted business contacts.
- Cybercriminals can use this method of cyberattack to intercept invoices or payment requests.
- Their aim is to trick organisations or customers into sending money or goods.

Verify payment requests

Cybercriminals frequently use business email compromise to redirect payments or alter supplier banking details. Small businesses are often targeted because payment processes may rely on trust, email communication and limited verification processes. Establishing simple verification procedures, for example confirming an email address, can significantly reduce the risk of financial loss.

Data protection and privacy awareness

Regularly review and update organisational policies and privacy regulations and encourage staff compliance.

Explain the importance of data classification and train staff to handle sensitive and confidential information safely.

- Teach staff how to prevent accidental data leaks, such as verifying recipients before sending emails or files.
- Prohibit the installation of unauthorised software or applications on work devices.
- Encourage staff to promptly report any suspected data loss, leak or unauthorised access.
- Follow privacy laws, regulations and internal policies for data handling and privacy.



Restrict and monitor access to system and data

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. Only give staff the access they need to perform their duties. In addition to restricting access, it is important to actively monitor access to check if it is being used appropriately. Monitoring helps detect unauthorised access, unusual behaviour or potential security incidents.

Implement access control

Following the principle of least privilege is usually the safest approach for most small businesses. Under this principle, staff have the minimum permissions on systems they need to perform their work.

- Update or change key logins when you have staff turnover.
- When staff use computer systems, identify the staff who need administrator access to perform specific tasks.
 - Administration access allows users to do much more on a system than with standard access, such as bypass security controls. Therefore, it is very important to consider who requires this level of access.
- Create separate administrator accounts for staff with administrative privileges.
- Review access permissions regularly, especially when staff change roles, leave the business or are involved in a cyber security incident.

Regularly monitor access

- Track and log user activity across systems and applications.
- Review access logs regularly to identify unusual or unauthorised behaviour.
- Set up alerts for suspicious activities such as repeated failed login attempts.
- Conduct periodic audits to ensure access policies are being followed and remain effective.



Use Secure by Design products and services

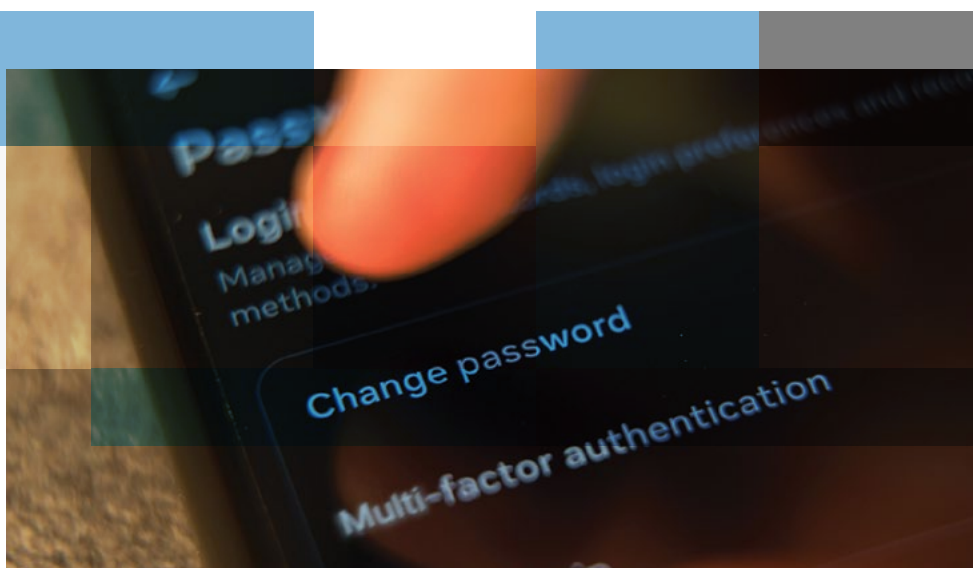
Secure by design is a security-focused approach to the design, development and deployment of products and services. As cyber threats grow more complex and widespread, it's crucial to use secure technologies and services that protect the privacy and data of users. We recommend choosing manufacturers and cloud service providers that prioritise security from the outset.

Choose trusted and reliable vendors

- Select well-known providers with good security reputations.
- Select vendors with compliance certifications where possible.
 - You can do this by checking the vendor's website (mostly under compliance, security or trust center pages) for certificate details. An example of compliance with a standard is compliance with ISO 27001. If you cannot locate compliance certifications on a vendor's website, request proof directly from the vendor.
- Use vendors that offer ongoing support and updates.

Security from the start

- Change default passwords immediately.
- Turn off features you don't need such as remote access features.
- Enable built-in security features (e.g. firewalls, multi-factor authentication).
- Perform regular backups.
- Follow vendor guides to reduce risks.



Implement and test cyber security incident response plans

A cyber security incident is when something bad or unexpected happens in a computer system. It can harm how a business works or cause problems with business functions. Creating and regularly testing a cyber security incident plan helps a business respond quickly and effectively when something goes wrong. We understand the ability of a business to implement and test a cyber security incident response plan can be dependent on what skills and resources it has available. As a starting point, businesses can refer to our [recover from a cyber incident](#) page for more information and resources.

Develop a cyber security incident response plan

- Identify common threats your business might face such as phishing, ransomware and business email compromise.
- Create step by step incident procedures including how to detect, contain, respond and recover from cyber incidents.
- Identify how and when to escalate, communicate and report.
- Clearly define staff roles and responsibilities explaining who does what during an incident.

Maintain and update the plan

- Regularly review and update the plan as needed.
- Update contact details and systems as the business goes through changes.
- Incorporate lessons learned from past incidents or near misses.
- Maintain staff awareness and basic skills.

Test and improve the plan

- Run simple drills periodically such as a phishing simulation.
- Check response times and decision-making effectiveness.
- Identify gaps and areas for improvement.
- Refine the plan based on test results.



Detailed advice

for enhancing small
business cyber security



Common cyber threats to small businesses

Cybercriminals target Australian business and organisations for financial gain. They may use ransomware attacks or data theft to conduct fraud or extortion. Cybercriminals are also likely to conduct multiple layers of extortion that disrupt business operations and damage the organisation's reputation. Below are examples of common cyber threats to small businesses.

Scam messages

Scams aim to trick you or your staff into sending money or gift cards, clicking harmful links or attachments, or sharing sensitive information like passwords.

Scam messages can arrive by various methods including email, text message, phone call or social media platforms. Cybercriminals often pretend to be a trusted person or organisation to make their scams seem real.



Phishing attacks

Phishing attacks often include links to fake websites that ask you to log in or enter sensitive information. If successful, cybercriminals can steal passwords, take over business accounts, such as social media, and demand payment.

Common warning signs

Phishing messages can be difficult to detect. Recognise these warning signs:

> Suspicious links

Links in phishing messages often lead to fake or harmful websites. Before opening a link, check the full web address and make sure it matches the official website exactly. Be wary of any link that has been sent to you by someone you don't know, even if it seems legitimate.

Don't open links if the address looks unusual or doesn't match the organisation.

> QR codes

QR codes can hide the destination of a link. Malicious actors can place fake QR codes on signs, posters or emails to redirect you to a malicious website. If you must scan a QR code, check for signs of tampering such as damage, alterations or placed over another code. After scanning, always check the full web address to make sure it's official.

> Fake websites and advertisements

Be careful of fraudulent websites and advertisements created by hackers that look real. A search result may show as 'sponsored' or 'advertisement', but this doesn't mean it is safe. Consider typing official website addresses directly into your browser rather than using a search engine.

> Unexpected phone calls

Malicious actors may call and pretend to be from a trusted organisation. Warning signs include:

- caller IDs that look real but may be fake
- a delay before the caller speaks
- requests for personal, financial information, passwords or authentication codes
- pressure to act immediately
- voices that sound unusual or too perfect (possible voice cloning).

If you are unsure, promptly end the call and contact the organisation using a trusted phone number from their official website.

> Unexpected messages

Be cautious of unexpected emails, messages or requests, even if they appear to come from someone you know.

Hackers can impersonate trusted contacts or take over legitimate accounts. Always verify unexpected or suspicious requests using contact details from a trusted source. Warning signs include:

- generic greetings like 'Dear customer'
- poor spelling, grammar, or layout in messages
- strange or misspelled email addresses
- messages that seem too good to be true.

> Requests to install software

Hackers may ask you to install software to fix a problem or access your account. This is often remote access software, which gives them control of your device. If installed, they may access your personal information, monitor your activity and intercept or approve authentication requests. This can allow them to gain access to your online accounts, even if MFA is enabled. They may also change account settings, change passwords and lock you out of your accounts.

Only install software if you have confirmed the request is legitimate, for example by looking into where the request came from. Do not allow remote access to your device unless you have verified the request via a trusted channel.

Getting started

If you notice a suspicious email, text or social media message:

- report it using the platform's reporting tools (where available)
 - block the sender and delete the message
- run antivirus or security software to scan your device and remove any suspicious programs
- monitor your accounts for suspicious activity.

If you believe your business has lost money or financial information has been compromised:

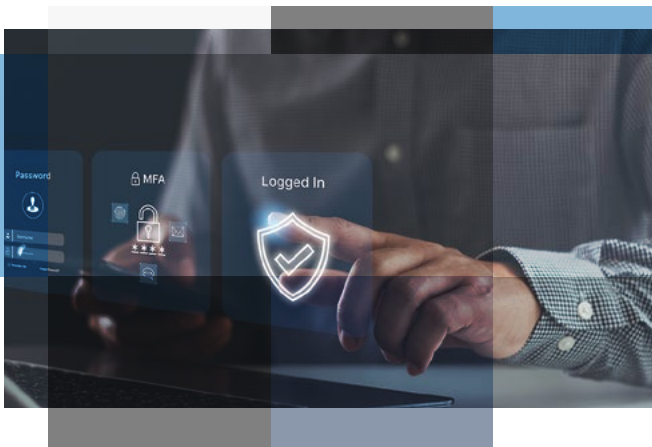
- contact your bank or financial institution immediately
- contact services such as myGov or the Australian Taxation Office if relevant
- report the incident to [ReportCyber](#).

Business email compromise

Small businesses are often targeted by email attacks such as business email compromise. In these attacks, cybercriminals impersonate a business, supplier, customer or staff member to trick people into transferring money, sharing sensitive information or changing payment details.

In some cases, cybercriminals gain access to legitimate email accounts and use them to send fraudulent requests. In other cases, they use email addresses or domain names that appear similar to those of trusted organisations.

Business email compromise can result in financial loss, data breaches, reputational damage and disruption to business operations. Small businesses are often targeted because payment approvals and account changes may rely on trust and email communications.



Getting started

- Use multi-factor authentication (MFA) and strong, unique passwords for all your email accounts.
- Make sure to set up recovery options and regularly review your email login activity to identify suspicious access attempts.
- Be cautious of unexpected requests involving payments, bank account changes, sensitive information or urgent action.
- Verify unusual requests using a trusted communication channel, such as a known phone number rather than contact details provided in the email.
- Only share your email address online if necessary. Consider using an alternative or alias email for general use.
- Delete email accounts you no longer use or monitor and consider deleting emails that contain sensitive or personal information. If a cybercriminal gains access to your account, they could find and steal this information.
- Protect your domain names and consider registering similar domain names that could be used to confuse your customers and staff. For example, pypal.com, payppal.com, pay-pal.com
- Teach staff how to identify suspicious emails and establish clear processes for reporting and verifying unusual requests.

Malware

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.

Getting Started

- Keep devices, operating systems and applications up to date.
- Use reputable security software.
- Be cautious when opening emails, attachments, links and files, particularly if they are unexpected or from unknown sources.
- Only download software and applications from trusted websites or official app stores.
- Avoid installing programs that are not required for your business.
- Teach staff how malware is commonly delivered and how to identify and report suspicious activity.

If you suspect a device has been infected, disconnect it from the network and seek assistance from an IT professional as soon as possible.



Ransomware

Ransomware is a common 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. Additionally, cybercriminals may also steal business information and threaten to publish or sell it online unless a ransom is paid, which is known as data extortion.

A ransomware attack can cause significant disruption to a business, resulting in downtime, financial loss, reputational damage and the loss of important information. Without reliable backups, recovering encrypted files may be difficult or impossible.

Regular backups that are tested and stored separately from your main systems are one of the most effective ways to reduce the impact of a ransomware attack.

Ransomware commonly spreads through:

- phishing emails
- malicious links
- unsafe websites
- compromised accounts
- infected downloads.

While antivirus or security software can help protect you from malware, no software is 100% effective.

Staff should be cautious when opening unexpected emails, attachments and links. Businesses should regularly update devices, enable multi-factor authentication and maintain reliable backups.

Getting started

- Regularly back up important business information.
- Enable multi-factor authentication (MFA).
- Keep devices and software up to date.
- Use security software and restrict administrator access to those who need it.
- Teach staff to be cautious of unexpected emails, attachments, links and file downloads.

If your business is affected by ransomware, do not pay the ransom. Paying does not guarantee that your files will be recovered or that stolen information will not be leaked or sold online. Seek assistance from an IT professional or report the incident through [ReportCyber](#).



Denial-of-service attacks

A denial-of-service attack is designed to disrupt or prevent access to online services such as websites, email services and online portals. This is usually done by overwhelming a service with large amounts of traffic, connections or requests, preventing legitimate users from accessing it. When multiple compromised devices are used to launch an attack, it is known as a distributed denial-of-service attack.

While denial-of-service attacks do not typically result in data being stolen or files being encrypted, they can cause significant disruption to business operations, impact customer access to online services and result in financial or reputational damage. Small businesses that rely on websites, online booking systems, email or internet-facing services may be particularly affected.

Getting started

Small businesses cannot always prevent denial-of-service attacks, but they can reduce their impact.

- Use reputable hosting, cloud and internet service providers that can respond to large volumes of malicious traffic.
- Monitor critical websites and online services for outages.
- Maintain up-to-date contact details for key service providers.
- Make sure your cyber security incident response plan includes procedures for responding to service disruptions.

If your business relies heavily on online services, such as a website, online store, or customer portal, consider discussing denial-of-service protection options with your service provider.



Securing accounts and identities

By enabling multi-factor authentication (MFA), using strong passwords and applying proper access controls, you can make it harder for cybercriminals to access to your accounts and limit the damage if an account is compromised.

Turn on multifactor authentication

MFA is one of the most effective ways to protect business accounts. It adds an extra step to logging in, such as a onetime code from an authenticator app, meaning a stolen password alone can't be used to gain access to an account.

Authentication methods



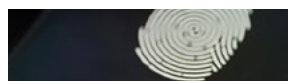
- **Passkey** – a more secure way to log in to your online accounts than using a password. Using a passkey helps to prevent cybercriminals tricking you to log in to a fake website.



- **Physical token** – a small device like a USB stick. It shows a new code on its screen at regular intervals. When you want to access an account, you need to check the token and enter the displayed code.



- **Security key** – a small physical token without a display screen. It's either plugged into your device via a USB port or connected wirelessly.



- **Biometrics** – with biometrics, your unique characteristics are used to confirm your identity. An example of biometrics is using your face or fingerprint to access your device or mobile apps.



- **Authenticator app** – applications that generate a random one-time password. Consider using a well-known authentication app, such as Google or Microsoft.



- **SMS / email code** – one-time codes received via SMS or email. This is the least secure option due to the ease in which SMS and email accounts can be compromised.

Getting started

Turn on MFA wherever it is available. Start with high-risk accounts like email, banking, cloud storage, accounting software and social media.

MFA settings are usually found under account security. Some services may call it two factor authentication or two-step verification.

Use strong passwords (where the use of passkeys is unavailable)

Weak or reused passwords are a common cause of cyber security incidents in small businesses. Each account should have a strong and unique password to help prevent cybercriminals from accessing multiple systems if a single account is compromised.

Where MFA is enabled, businesses should still use strong passwords and make them as long as practical with a minimum of 6 characters per password. Where MFA cannot be used, passwords should be at least 15 characters long.

Businesses should:

- use a unique password for every account
- avoid reusing passwords across multiple systems
- use a password manager to generate and securely store passwords
- change passwords if they are suspected of being compromised.

Use a password manager

Keeping track of different passwords can be challenging, but a password manager makes it easy. It helps you create, manage and store your passwords and passkeys in one secure place.

Password managers allow you to:

- create long, unpredictable and unique passwords
- store your account logins in one place from any device
- save time and effort by auto filling your account logins
- reduce the risk of someone intercepting your passwords.

Use a strong master password

Your password manager protects many of your important accounts, so it's important to secure how you access it. Using weak authentication is like putting your valuables in a safe and leaving the unlock code beside the door. Secure authentication should include a strong, unique master password along with MFA.

Getting started

Choose a trusted password manager and protect it with MFA and a long, unique master password. Add your business accounts and use the manager to create passwords that are at least 15 characters long. Start with your most important accounts.



Manage shared accounts

Shared accounts increase security risks and make it harder to track activity. Where shared access is needed, it should be tightly controlled.

Getting started

- Create individual accounts for staff wherever possible.
- Keep a record of shared accounts and who has access and reduce access where you can.
- Change login details when staff leave or change roles.

Implement access controls

Limiting access helps reduce the impact of cyber incidents. Staff should only have access to the systems and data they need to do their job.

Getting started

Review what each staff member can access and remove access to anything unnecessary, including files, applications and online accounts. Follow the principle of least privilege and only give administrator access to those who need it. Remove access promptly when staff leave.



Protecting devices, systems and networks

Most business systems are connected to each other and the internet, including computers, mobile phones, payment systems and smart devices. These connections help businesses operate efficiently and serve customers.

However, increased connectivity also increases exposure to cyber threats. Protecting your devices and networks is essential to keep your business and information secure. Follow these tips to reduce your risk.

Update your software

Software updates fix security weaknesses that cybercriminals can exploit to install malware or gain access to your devices.

New security flaws are discovered regularly, so it's important not to ignore update prompts. Devices or software that no longer receive updates can leave your business exposed. If a product is no longer supported by the manufacturer, consider upgrading to a newer, supported version to stay secure.

The easiest way to manage this is by enabling automatic updates wherever possible. This “set and forget” approach ensures your systems stay protected without requiring constant attention. You should still regularly check that updates are being applied across all devices used in your business, including computers, phones, and any systems your staff rely on for work.

Getting started

Update all devices, apps, and software through their settings menus. Where possible, turn on automatic updates so security fixes are applied as soon as they are available. If automatic updates are not an option, set reminders to check regularly and schedule updates outside business hours to minimise disruption.

Make sure all devices connected to your business network are also kept up to date, including servers and storage devices.



Back up your information

Regular backups help your business recover data if it is lost, stolen or damaged. Without reliable backups, it may be difficult or impossible to recover information after a cyber incident.

Backups should be done regularly or automatically as part of normal business operations. There are many backup options available, and the best approach depends on your business needs.

Getting started

Create a plan or procedure for backing up your business. This will be different for every business. Your plan should answer the following questions:

- What data is or is not backed up?
 - When do backups occur?
 - Where are the backups stored?
 - Who is responsible for managing the backups?
 - How long are the backups kept for?
 - How often are the backups tested?
- Think about all the places where your important information is stored. Are these locations included in your backup plan? For example, information held in your email or cloud accounts.

Use security software

Security software, such as antivirus and ransomware protection, helps protect your devices from cyber threats. These tools can detect and remove malware by scanning for suspicious files and programs and alert you when a threat is found.

Your device may have built-in antivirus software which most modern Microsoft and Apple computers automatically include. Third-party companies also sell antivirus software which tends to include more features than free software.

Getting started

- To learn more about Windows Security, search for “Windows Security” in your Start Menu. You should also visit Microsoft’s website for more information, including ‘how to use controlled folder accesses for protection against ransomware’.
- Set up your security software to automatically do regular scans, for example every week.
- Familiarise yourself with your security software, including what a legitimate alert looks like. This will help you avoid scams that pretend to be your antivirus software.



Secure your network and external services

Networks and connected services are common targets for cybercriminals and can contain weaknesses if not properly secured.

Because networks can be complex, it's important to identify and address vulnerabilities carefully. Consider discussing security measures and set-up with an IT professional to ensure your network and external services are protected.



Getting started

> Secure your servers

If you use servers such as a network attached storage at home or work, take extra steps to protect them. These devices are common targets because they store important data. Keep them updated and protect administrator accounts with strong passwords and MFA.

> Minimise internet-facing services

Review any services exposed to the internet, such as Remote Desktop, file sharing, or remote administration tools. Limit access and secure or disable services that are not needed.

> Migrate to cloud services

For many small businesses, reputable cloud services provide stronger security than self-hosted systems. Use trusted cloud providers for services such as email, file storage and collaboration. Enable MFA, review administrator access regularly, and remove unused accounts or third-party integrations.

> Improve your router's security

Secure your router by:

- changing default passwords
- using strong encryption
- keeping firmware updated
- enabling guest WiFi for visitors and customers.

> Understand your cyber supply chain

Businesses should understand what systems, information and accounts external providers can access. Access should be reviewed regularly and removed when it is no longer required. When engaging new providers, consider how they protect customer and business information.

Harden your website

Websites are a common target for cyber attacks and need basic security protections to reduce the risk of being compromised. To protect your website:

- secure login access with MFA or strong passwords
- keep content management systems and plugins up to date
- back up your website regularly so it can be restored after an incident.

Understand the threats

It is important to understand the major threats you may face as a website owner or manager. Understanding these threats can help you be more prepared for a cyber attack.

> Website defacement

Defacement is when a cybercriminal changes your website without you knowing. They can change its appearance and content, which may compromise your data and increase the risk of further attacks. They can even infect your website with malware, putting your visitors at risk.

Cybercriminals will use various tactics to access and deface your website. They may be able to gain unauthorised access to the back end, exploit vulnerability or use malware.

> Data breach

A data breach happens when a cybercriminal is able to access and export your data for personal gain. This may include sensitive data such as personal and financial details.

> Denial-of-service (DoS) attacks

A denial-of-service attack is when a cybercriminal directs large volumes of traffic to your website. It overloads available resources and prevents users from accessing your website. This can lead to significant disruptions to your business.



Choose a secure hosting service

Understanding the security features provided by your web hosting service is crucial. These features may be what stands between your website and any malicious attacks. When looking for a service provider, consider the following.

> How do they back up data?

Check if the provider performs data backups, and how often. Storing backups offsite is a more secure method. Make sure you know where and how they store backups.

> Do they mitigate against malware?

Check if the provider offers malware detection tools, such as scanning and antivirus software. They should also use preventative technology such as firewalls and encryption.

> What are their security standards?

Check if the provider offers integrated security features like MFA and DoS protection. Features such as a login activity panel and password-protected pages are also desirable.

Confirm where they are located and the security and privacy standards they follow. Providers outside Australia may be subject to different legal obligations.

Getting started

Enable autorenewal for your website's domain name to prevent accidental expiry. If your website is managed by an external provider or developer, speak with them about improving security controls and maintenance practices.

Make sure to use Hypertext Transfer Protocol Secure (HTTPS). HTTPS is an encrypted and more secure version of HTTP. It provides security for sensitive information such as passwords and credit card details. It also helps to keep your data private, making it hard for cybercriminals to read if they intercept it.

Limit website administration access to those who need it and only give users the privileges they need for their role. For example, developers can update the site configuration with administration access, while marketing staff can only publish web pages.



Reset your devices before selling, trading or disposing of them

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 wipe any information and restore the device to its original settings.

Getting started

Even if you follow the right steps, it may still be possible for someone to recover your information. If the information on your device is particularly sensitive, you could use a data destruction service or ask an IT professional to help you dispose of it securely.

Keep your devices locked and physically secure

Restrict access to business devices to reduce the risk of unauthorised access, data theft and malicious activity. Store devices securely and do not leave them in locations where unauthorised staff or members of the public can access them.

Apply basic security controls to all devices. At a minimum, protect devices with a password or biometric authentication and set to automatically lock after a short period of inactivity.



Protecting business & customer data

Data breaches affecting Australian businesses are increasing in scale, complexity and impact. As more business activity moves online, organisations have a responsibility to protect the personal information they collect from unauthorised access, disclosure, modification and loss.

To apply effective security measures, businesses must first understand what data they hold and how it is protected. The ASD's ACSC recommends using the free [Exercise in a Box](#) tool to:

- assess current data handling and cyber security practices
- identify strengths, weaknesses and areas for improvement.

Protect your business data

Apply appropriate security measures to protect it from unauthorised access. Some businesses may also have legal obligations to protect certain types of data, so it's important to be aware of these requirements and meet them.

Getting started

Consolidate your business data. Data stored across numerous devices or services increases the number of systems you have to keep secure and backed up. More 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 protected with secure configurations and restricted access.

Read the [Office of the Australian Information Commissioner's \(OAIC\) guide for small businesses](#) to learn more. Consult with a legal professional if you are unsure.



Key data security practices

The following practices will help businesses manage personal data securely and reduce the impact of a data breach.

Create a register of personal data

Businesses should understand:

- what personal data they collect
- where it is stored
- how it is used.

Maintaining a register of personal data, such as databases, systems, and data assets, supports effective protection and oversight. [The National Archives of Australia](#) provides guidance on maintaining information asset registers.

Limit personal data collected

Only collect personal data that is required to operate your business. Clearly define why the data is needed and how it will be used. Avoid collecting and holding unnecessary data as this increases risk if a breach occurs.

Delete unused personal data

Set clear policies for how long personal data is kept and when it should be deleted. Retention periods should be based on business needs, legal obligations and the sensitivity of the data. Removing data that is no longer required reduces exposure.

Control access to personal data

Restrict access so staff can only view or modify the personal data they need to perform their role. Strong access controls limit damage if systems are compromised and reduce the risk of misuse by insiders.

Encrypt personal data

Apply full disk encryption to devices such as laptops, servers and mobile phones that store or access personal data. Consider file level encryption for added protection. Check that data is encrypted when transmitted, such as when information is sent over the internet.

Back up personal data

Regular backups allow businesses to recover personal data if it is lost, damaged or encrypted by ransomware. Backups are a key defence against cyber incidents and physical events like fires or floods.

Report a data breach involving personal data

Businesses must understand and meet their reporting obligations if a data breach involves customers' personal information. All cyber security incidents should be reported through the ReportCyber portal or by calling 1300 CYBER1 (1300 292 371).

Affected customers or users should also be informed if their personal data may have been compromised.

Businesses covered by the *Privacy Act 1988* must report eligible data breaches to the Office of the Australian Information Commissioner (OAIC). An eligible data breach occurs when:

- personal information is accessed, disclosed or lost without authorisation
- is likely to result in serious harm to individuals
- cannot be prevented through remedial action.

Further guidance is available on the [OAIC's Notifiable Data Breaches](#) webpage.

People, training and incident readiness

Cyber security starts with your staff. Employees who have good practices are a critical defence against cyber threats. Clear response plans help reduce the impact of incidents and support business continuity. Staying informed through trusted sources and partnerships also helps your business prepare for evolving threats.

Educate staff

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

- Common cyber threats such as business email compromise and ransomware.
- Protective measures including strong passwords, 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 before paying)
- What to do in an emergency.

Cyber security training should be refreshed periodically, for example with a formal course or internal training. Learn more at cyber.gov.au/stay-secure.

Make and test an emergency plan

A cyber security emergency plan helps reduce the impact of an incident and supports faster recovery. When an incident occurs, having a clear plan allows staff to act quickly instead of deciding what to do in the moment.

Your plan should outline:

- how staff report incidents
- who to contact for support (such as IT providers or your bank)
- how you will communicate with staff, customers and stakeholders
- how the business will continue operating if critical systems are unavailable.

Staff should understand their roles and responsibilities, and a copy of the plan should be available offline in case systems are inaccessible.

Getting started

Identify the cyber threats most relevant to your business, such as ransomware or business email compromise, and consider how they could affect operations. Develop a plan that includes key contacts and response steps, and review and test it regularly. Use tools like [Exercise in a Box](#) to test your response and improve your readiness.



Stay informed

Stay informed about emerging cyber threats by joining the [ASD's ACSC Partnership Program](#). As a partner, you will receive regular updates, including alerts and newsletters on new threats and vulnerabilities.

Cyber security is constantly evolving, and vulnerabilities can be exploited quickly after they are discovered. Staying up to date helps you understand current risks and take timely action to improve security.

The program also allows you to engage with the ACSC and a broader network of partners, sharing knowledge and strengthening cyber resilience across the Australian economy.



Remote working security

Working remotely can introduce additional cyber security risks, as home environments may not have the same protections as office networks. Without proper safeguards, devices, accounts and data may be more vulnerable to cyber threats.

It is important to stay vigilant and follow secure practices to protect your devices, connections and information while working remotely.

Improve your network security

Make sure to secure your Wi-Fi network and router to prevent unwanted access. Cybercriminals will target weaker networks, putting your sensitive data at risk.

To improve your network security, you should:

- change your default Wi-Fi network name and password
- change your router's default username and password
- use the strongest Wi-Fi encryption available
- keep your router up to date
- disable remote management and Universal Plug and Play
- enable guest Wi-Fi if required.

Consider segmenting your network by purpose or device. For example, set up smart home devices on a separate network from your main one to reduce the risk if they are compromised.

Avoid public Wi-Fi for work

Public WiFi networks are convenient but can be insecure and are often targeted by cybercriminals seeking to access sensitive information. Using these networks can increase the risk of data being intercepted or accounts being compromised.

Where possible, use trusted networks such as your home WiFi or a personal hotspot. If you must use public WiFi, limit what you access and avoid activities involving sensitive information, such as logging into accounts or making payments.

Secure your information

Protecting your information requires consistent and practical security measures. Regularly back up your data to ensure it can be recovered if lost, damaged or compromised during a cyber incident.

Use a dedicated work account to separate business and personal activities, reducing the risk of accidental exposure or compromise.

Take care when using online meetings or communication platforms. Meetings should be secured with appropriate settings, such as passwords or waiting rooms, to prevent unauthorised access and protect sensitive information.

Be aware of your surroundings

Avoid accessing sensitive information when in public locations. You could expose confidential work and customer details to anyone passing by. You should access this type of information when in a private or trusted location.

Check your workplace requirements for information security and privacy.

Transfer files securely

Avoid using removable media to transfer files between devices. Portable storage devices such as USB drives are easy to lose, steal or infect with malware.

Use secure methods of file transfer such as cloud storage from a reputable provider. Your workplace may already use this for online file management. If you don't have this option, you should encrypt your storage device with a strong password.

Use secure web conferencing systems

Web conferencing tools can expose your business to security risks if not configured properly. Taking simple precautions can prevent unauthorised access and protect sensitive information during meetings.

When hosting or joining online meetings, check for unknown participants, remain aware of your surroundings, and any information shared on screen. Only use trusted conferencing platforms with strong security features and follow your organisation's approved providers where applicable.



Using AI securely in your business

Artificial intelligence (AI) refers to tools that allow computers to perform tasks that normally require human thinking, such as problem-solving, understanding language and making decisions. AI can help you save time, improve efficiency for your staff, and support decision-making by analysing data and generating insights for your business.

You are likely already using AI in everyday business tools, including:

- chatbots and virtual assistants for customer service
- translation tools for communication
- platforms that recommend products or content
- tools that help you write emails, create plans or summarise information.

While these tools can be useful, you should use them carefully and understand the risks involved. You should avoid sharing sensitive business or customer information, such as passwords, financial details or confidential data. Many AI tools may store or use your data to improve their systems, so it's important to know how your information is handled.

Before using an AI tool in your business, you should consider:

- whether the provider is reputable and trustworthy
- whether you really need to share the information requested
- how and where your data will be stored, used or shared
- what the provider's privacy policy says
- whether you can verify and trust the outputs provided.



You should also be aware of privacy risks. AI systems often rely on large amounts of data, which can make them attractive targets for cybercriminals. Even if data is anonymised, there is still a risk it could be re-identified. This means you should treat AI tools like any other online service, helpful, but not always private or secure. To use AI safely in your business, you should:

> Control your digital footprint

- Use tools that allow you to delete history or limit data storage and consider separate accounts for testing new AI tools.

> Watch for accuracy and bias

- Do not rely on AI outputs alone. Always check important information, as results can be incorrect, incomplete or biased.

> Prioritise security

- Be cautious when using free or public AI tools and follow any internal policies about sharing business information.

> Be aware of data location

- Understand where your data is stored and processed, especially if it is outside Australia, as different privacy laws may apply.

By taking a cautious and informed approach, you can benefit from AI while protecting your business, your customers and your data.

Be aware of AI-enabled scams

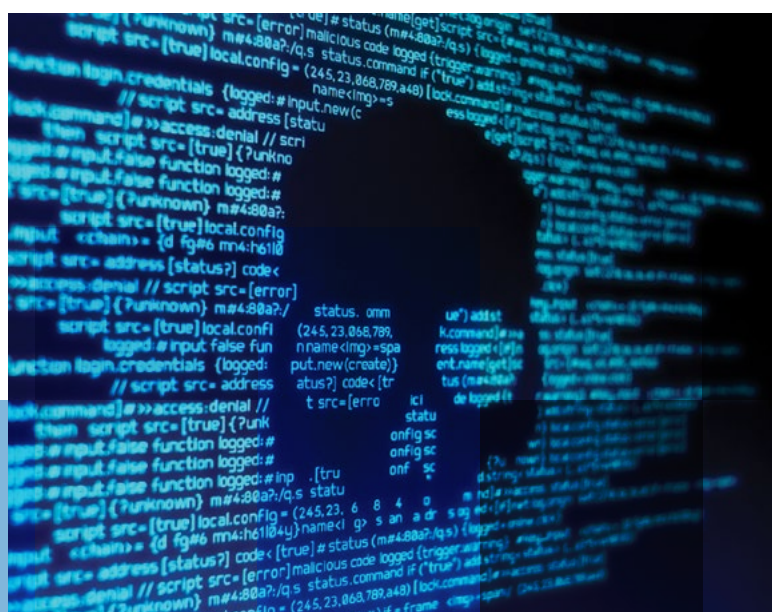
AI can be used by cybercriminals to create convincing phishing emails, fake invoices, impersonation messages, fake images and cloned voices. These techniques can make scams appear more legitimate and more difficult to identify.

Getting started

AI-generated content can be convincing and may be used to support scams, impersonation attempts or social engineering attacks. Train staff to recognise emerging AI-enabled threats and encourage them to question unexpected requests, even when messages appear professional, familiar or trustworthy.

Staff should also be aware of what information can and cannot be entered into AI systems, particularly business-sensitive, customer, personal or confidential information.

When assessing the legitimacy of a request, do not rely solely on the appearance, tone or quality of the message, and always confirm important actions through trusted communication channels.



Using AI agents securely in your business

Some AI tools can act on your behalf by completing tasks automatically, such as organising information, sending messages or interacting with other business applications. These are known as AI agents. While they can improve efficiency and save time, they can also increase security and privacy risks if they are given too much access or control.

As a small business owner, you should be mindful of how much authority you give these tools. AI agents can sometimes act quickly and independently, so it's important that you stay in control of key decisions and sensitive actions.

You should only enable features that you understand and genuinely need for your business. Before setting up an AI agent, you should carefully review what systems, accounts or data it can access. Avoid giving it permission to make significant changes, such as approving transactions, sending communications or modifying business data, without your oversight.

To use AI agents safely, you should:

- > **Use trusted tools and providers**
 - Choose reputable platforms with clear security and privacy practices.
- > **Limit access from the start**
 - Only give the agent the minimum access required to perform its task.
- > **Understand permissions**
 - Check what apps, systems and data the agent can access before enabling it.
- > **Maintain control over important actions**
 - Avoid allowing AI agents to make critical decisions or changes without your review.
- > **Review and adjust settings regularly**
 - Periodically check permissions and disable anything that is no longer needed.





Advanced cyber security advice for small business



Event logging

Event logging keeps a record of important system and user activities to help identify problems and investigate security incidents. Logging helps small businesses detect cyber threats, respond quickly and understand what has happened across their systems. Instead of collecting large volumes of data, businesses should focus on key security events and ensure logs are accurate, secure and reviewed regularly.

You should:

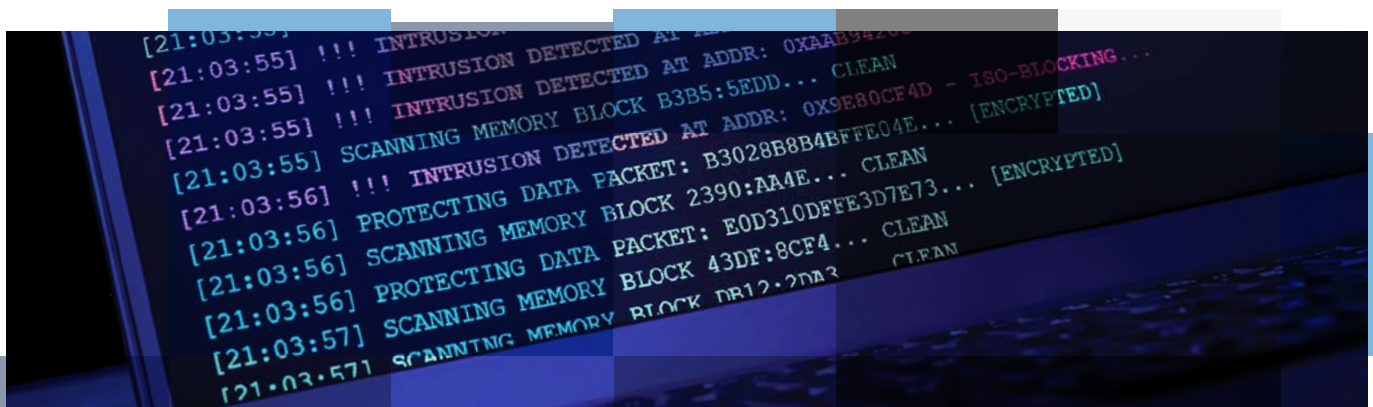
- create a simple logging policy covering systems, events, retention and responsibilities
- focus on high-value events such as logins, administration changes, remote access and security alerts
- ensure logs include useful details (time, user, system, action, outcome)
- retain logs for several months or longer where possible
- centralise logs to improve visibility and prevent data loss
- restrict access to logs and protect them from modification or deletion.

If cloud services are used, logging should also be enabled for user activity and administrative changes.

Indicators to watch for

Logs should be monitored regularly or supported by automated alerts. Businesses should focus on unusual activity, such as repeated failed logins or unexpected access patterns. Understanding what normal activity looks like makes it easier to identify potential threats. Watch out for:

- multiple failed login attempts or unusual login behaviour
- access from unexpected locations or outside normal hours
- creation or modification of administrator accounts
- large or unusual data transfers
- unexpected system or configuration changes.



Post-quantum cryptography

For most small businesses, implementing multi-factor authentication, software updates, backups and access controls are the first priority. However, post-quantum cryptography (PQC) is an emerging area of cyber security that businesses should be aware of as technology evolves.

Most of your business data, including emails and banking, are protected by complex encryption that normal computers can't crack easily. But a Cryptographically Relevant Quantum Computer (CRQC) is a powerful future computer that could break today's encryptions quickly. PQC focuses on developing and using encryption methods that can resist attacks from future quantum computers. These methods provide a practical way to protect data even as new computing technologies emerge.

Reasons to act now

Organisations should start to plan their transition to post-quantum cryptography now because:

- deploying protections may take longer than expected
- the timeline is uncertain as quantum computing is an active area of research
- sensitive data encrypted using classical encryption methods may be vulnerable to 'harvest now, decrypt later' attacks.

Getting started

Some service providers and vendors have begun their transition to PQC, with some offering PQC-only solutions and products. The shift to PQC will happen at different speeds and will depend on factors such as cost, dependent technology updates and legacy interoperability. This further highlights the need for organisations to start planning their PQC transition right away.

Learn more about [planning for post-quantum cryptography](#).



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

cyber.gov.au

1300 CYBER1 (1300 292 371)

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

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license
<https://creativecommons.org/licenses/by/4.0/>

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license <https://creativecommons.org/licenses/by/4.0/legalcode.en>

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 [Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au](https://www.pmc.gov.au/commonwealth-coat-of-arms-information-and-guidelines).

A decorative graphic at the bottom of the page consisting of a grid of colored squares. The colors include blue, dark blue, black, white, and purple. The squares are arranged in a pattern that is roughly rectangular, with some squares missing, creating a fragmented look.

cyber.gov.au