



Australian Government
Australian Signals Directorate

cyber.gov.au

Personal cyber security handbook

A practical guide to staying secure online



Personal cyber security handbook

Cyber security is an important part of everyday life. This handbook is a practical guide for individuals on how to improve your personal cyber security. It provides advice and steps you can use to help protect you, and your family, friends and colleagues against common cyber threats. By following good cyber security practices, you're doing your part to help secure Australia.

How to use this handbook

This handbook provides advice on how to protect your devices, accounts and personal information. It also has advice for spotting scams and staying digitally secure while travelling.

Use this handbook to:

- **learn about and build good cyber security habits**
- **protect yourself against common cyber threats**
- **share cyber security tips with your family, friends and colleagues.**

Regularly check our website for the latest tips and advice on [cyber.gov.au](https://www.cyber.gov.au).



Core cyber security tips

Set up multi-factor authentication	6
Use passkeys	7
Use unique and strong passwords (where the use of passkeys is unavailable)	8
Keep your devices and software up to date	9
Learn how to spot scams	10

Detailed advice to improve your cyber security

Secure your devices	14
Secure your online activity	21
Travelling overseas	32
Getting help	34



Core cyber security **tips**

Set up multi-factor authentication

- Multi-factor authentication (MFA) is when you need to prove who you are in two or more ways before you can log in to your account. For example, after entering your password you might get a code on an authenticator app or need to use your fingerprint.
- It's an extra check so only you can access your account, even if someone steals your password.

Passkeys

- Use passkeys wherever possible.
- Passkeys are a more secure way to log in to your online accounts than using passwords.

Use unique and strong passwords

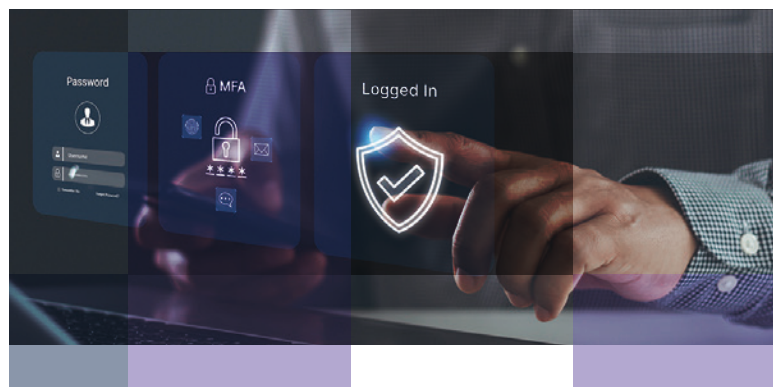
- Where you are unable to use a passkey, use unique passwords for each of your online accounts and never reuse passwords on other websites, apps or devices. This helps keep everything else safe even if one account is compromised.
- Make your password strong by making it long and hard to guess, especially if you're unable to use MFA.
- Make sure to keep your passwords private. Sharing them may put your data, devices and identity at risk.
- Use a password manager to help keep track of passwords. Password managers can automatically generate and store strong passwords, usually in the form of a random string of characters.
- If you think your passwords have been compromised, change them.

Keep your devices and software up to date

- Updates are new, improved or fixed versions of software.
- They can often include fixes to improve security.
- Update your device or applications (apps) as soon as they become available.
- Make sure your device has power, a secure internet connection and enough storage space to successfully install updates.

Learn how to spot scams

- Scams are one of the most common methods used by cybercriminals to compromise devices, online accounts, credit card details or other personal information.
- A scam will often convince people to pay money or hand over their personal information.
- Scammers often target people via email, text messages, phone calls and social media. They will often pretend to be a person or organisation you trust.
- Stop and check where a request is coming from for example by verifying an official phone number.



Set up multi-factor authentication

Multi-factor authentication (MFA) is one of the most effective ways to protect yourself from being hacked. MFA adds an extra verification step to check you are the true owner of the account. It prevents most password-related cyber attacks. For example, if a cybercriminal guesses or knows your password, they can't log in to your account without the MFA details.

Turn on MFA for accounts that have your personal or financial information. For example, your email, banking, online shopping and government services accounts.

Options for MFA

- Passkey – a more secure way to log in to your online accounts than using a password.
- Physical token – a physical token is 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 security key is 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 (OTP). 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.



Use passkeys

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.

Passkeys provide MFA and can help to:

- reduce the time it takes to log in to your account
- avoid the need to type in usernames, or one time codes provided via SMS, email or an authenticator app
- prevent cybercriminals from gaining access to your account by guessing your password
- stop cybercriminals from stealing your account password using scams or tricking you to log in to a fake website.



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

If your online account uses a password, make it unique, unpredictable and a suitable length, especially if you're unable to use MFA. Avoid using the same password for multiple accounts. If you reuse the same password anyone who knows, or guesses, your password can access all those accounts.

Keep your passwords private. Sharing them may put your data, accounts, devices and identity at risk.

Change your passwords if you think they have been compromised.

Steps to create a password

Make it a suitable length

A long password reduces the risk of it being guessed by cybercriminals. You should use a password that is at least 15 characters long.

Make sure your password meets the requirements of the account provider.

Make it unpredictable

The more unpredictable your password is, the stronger it is. Avoid words or phrases others may expect or easily guess, such as anything about you that's publicly available. Instead use a random mix of words, such as unrelated words from the page of a book.

Make it unique

Use a unique password for every account. If you reuse the same password, all those accounts are at risk. Cybercriminals could steal one password and use it to access other accounts that use the same password. Once someone has access to your account, they can change your password and lock you out.

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 that can be accessed by all of your devices
- save time and effort by auto filling your account logins
- reduce the risk of someone getting hold of your passwords.

Use a strong master password

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

Keep your devices and software up to date

Cybercriminals hack devices by exploiting weaknesses in their system or apps. Software providers release updates and patches to fix these weaknesses. Updates may also add new features and improve performance.

Installing updates when they are released is crucial for keeping your devices secure.

Turn on automatic updates

Cybercriminals never stop looking for vulnerabilities, so you need to download the latest version of software updates to your devices when they are released.

The easiest way to stay up to date is by turning on or confirming automatic updates where possible. An automatic update is a 'set and forget' feature that updates your software as soon as it becomes available. This way you can relax knowing you're always using the most secure version.

No matter what devices you're using, check you've got the latest software and make sure automatic updates are on.

Replace devices and software that are no longer supported

If your device or software is no longer supported by the manufacturer or developer, it will not receive updates or patches. It may still work, but it can be less reliable and at risk of cyber attacks. The best way to stay protected is to upgrade to a new device where possible.



Learn how to spot scams

Be aware of current cyber security threats by staying across official government advice, such as the Australian Signals Directorates' cyber.gov.au, and by talking with family, friends and colleagues.

Scams are one of the most common ways cybercriminals compromise devices, online accounts or personal information. Scammers will try to trick you into opening malicious links or attachments or providing them with information. This can put your devices and accounts at risk. Always stop and think before you open any links or attachments from email, text messages, websites and social media.

How scams work

Knowing how to spot common scams and how they work can help you avoid them. Most scams follow a similar pattern, typically including these phases:

Contact

You receive an unexpected message, call or offer.

Manipulation

The scammer pressures you to act quickly.

Payment or data theft

The scammer tries to get you to transfer money, share personal details, provide them with a verification code, install software, or click malicious links or QR codes.

Common scam tactics

Scammers might change their stories often, but their goal is the same: to steal money or information. Be aware of the following types of scam tactics.

Impersonation scams

A scammer pretends to be from a trusted organisation, such as a bank, government agency, delivery company or utility provider. They may spoof phone numbers or sender IDs to make the message look real.

Investment and cryptocurrency scams

You are offered high or guaranteed returns. The offer may involve cryptocurrency, trading platforms or “insider” opportunities. These scams often have real websites and testimonials behind them to appear authentic.

Romance and relationship scams

A scammer builds a relationship with you online, then asks for money, gifts or financial help. They may claim to work overseas or in remote locations.

Congratulations!

You won the amount of \$50,000.
You can get them with one click.
Access the
link: <http://banking.scam/fund20>

Remote access scams

Someone claims to be from technical support and asks you to install software or give them remote access to your device.

Jobs and employment scams

You are offered easy online work or paid tasks. You may be asked to pay fees upfront or use your own money before being “reimbursed”.

Deepfake scams

Scammers may use AI to copy a person’s voice or create convincing messages and videos. The term ‘deepfake’ is associated to this tactic. An example could be a phone call that sounds like a family member asking for urgent financial help.

AI chatbot scams

In online buying and selling, scammers may use chatbots to pose as fake buyers or sellers. They use quick, friendly messages to gain trust and push the deal forward. They might send fake payment links, claim they paid too much by mistake, or say you must pay extra fees before the item can be released.

SMS scams

Scammers often use familiar business or brand names to make their messages look real. Don’t trust a message just because it looks genuine. Avoid clicking links and contact the organisation directly if you’re unsure.

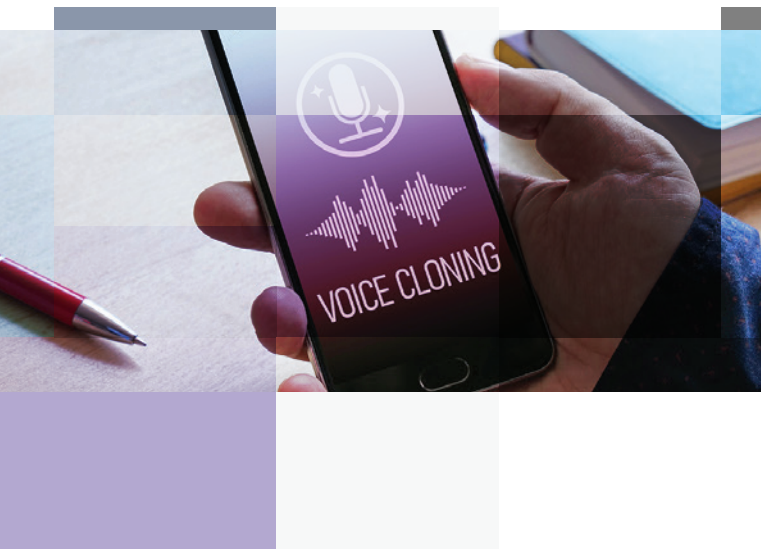
As part of the Australian Government’s efforts to reduce scams, businesses can register their branded sender IDs (the name shown at the top of an SMS, such as AusPost, StarTrack or myGov) with the Australian Communications and Media Authority (ACMA). Verified organisations can display their name when sending messages like delivery updates or security codes. Messages from senders that haven’t been verified may show as ‘unverified’, which can help you spot suspicious messages.

Phishing

Phishing is when cybercriminals pretend to be a trusted person or organisation to trick you into giving them information. They may send you fake emails or messages and pretend to be from a trusted organisation such as a bank or government service. They may try to steal your online banking logins, credit card details or passwords. They may try to gain access to your accounts by requesting you scan a QR code, share account registration PINs or account verification codes. This can lead to financial loss or identity theft.

Phishing messages can be sent through:

- email
- text message
- social media
- instant messaging platforms
- phone calls.



Warning signs of phishing

Phishing messages can be difficult to detect. Look out for these common warning signs:

- Unexpected emails, texts, messages or phone calls.
- Pressure to act quickly or urgently.
- Requests for passwords, authentication codes or personal information.
- Suspicious links, attachments or QR codes you weren't expecting.
- Caller IDs that look real but may be fake.
- Strange or misspelled email addresses.
- Generic greetings like 'Dear customer' and poor spelling, grammar or layout in messages.
- Callers asking you to skip normal security steps.
- Threats or warnings of serious consequences if you do not act.
- Messages that seem too good to be true.
- Voices that sound unusual or too perfect (possible voice cloning).

What you can do about phishing

Taking a moment to stop and check before you act can help keep your information and accounts secure.

- Be careful with messages and calls: Don't click links, scan QR codes, or download files you weren't expecting.
- Use trusted sources: Go directly to official websites or use known phone numbers instead of links in messages.
- Don't share personal details: Never give out passwords, authentication codes or banking details.
- Use strong security: Set strong passwords and turn on multi-factor authentication.
- Keep devices and software updated: Install updates and security patches regularly.
- Check before you act: If something feels urgent or unusual, stop and verify it.
- Protect your accounts: Contact your bank or service provider if you think your details are at risk.



Detailed advice

to improve your
cyber security



Secure your devices

Many devices in your home connect to each other and to the internet, including your:

- smartphone
- laptop or computer
- smart TV
- speakers
- cameras
- smart appliances
- internet router.



Being more connected also brings more exposure to online threats. If cybercriminals hack your device, they can access your personal data and accounts. Follow these tips to keep your devices and personal information secure.

Lock your device when not in use

If you can lock your devices, you should do so when you're not using them even if it's only for a short time. Make sure they are set to automatically lock (less than 5 minutes – the shorter the better).

Consider using biometrics such as a fingerprint or face scan. Pair this with a strong password to help protect your device from unwanted access.

Avoid unknown devices and cables

Only use external devices and cables, such as a USB drive or memory card, from trusted sources. If you have obtained an external device or removable media that is second-hand or was given to you for free, it could potentially contain malware.

Prepare for a lost or stolen device

Keep your devices in a safe place and know where they are. Do not leave them unattended, especially when you're travelling.

Turn on 'find my device' and device encryption features. This helps protect your data if your device is lost or stolen.

Secure your smart devices

Smart devices, also known as The Internet of Things (IoT), refers to a network of devices, vehicles, appliances, and other objects. These objects are embedded with sensors, software and network connectivity. This allows them to collect and share data.

Secure your smart devices to help prevent hackers gaining access to them. Imagine someone being able to control your smart speaker or camera.

Protect your smart devices by:

- using strong passwords
- keeping software updated
- using secure connections. The level of protection also depends on the security built into the device itself. Research devices before making a purchase, as manufacturers provide different levels of security. Choose products from trusted manufacturers. Compare similar devices made by different manufacturers.

To improve the security of the digital products used by Australians every day, the Cyber Security (Security Standards for Smart Devices) Rules 2025 commenced on 4 March 2026. These rules introduce mandatory cyber security standards for most smart devices.

Things to consider when buying smart devices:

- Is the device made by a trusted company and sold by a well-known, reputable store?
- Is it possible to change the password?
- Does the manufacturer provide security updates?
- What data will the device collect and who will the data be shared with?
- Does the device do only what you want it to do?
- If you bought the device on or after 4 March 2026, does it meet the Cyber Security (Security Standards for Smart Devices) Rules 2025? These rules require no default passwords, a clear way to report security issues and a defined period for security updates.

Smart devices use the internet to provide features such as remote access, apps and automation. Being a smart device means they can collect, store and share personal data. When choosing a smart device, select established manufacturers and service providers that have a clear approach to security, privacy and ongoing software support.

> Consider what data is collected and where your data is stored

Smart devices can collect information such as location data, usage patterns and details from linked accounts or devices. This data may be stored by manufacturers or third-party service providers, sometimes overseas. Check your device privacy settings and disable data sharing or features you don't need.

> Keep devices secure over time

Security is ongoing for all smart devices.

Manufacturers release updates to fix security issues and reduce cyber risks. To help reduce the risks:

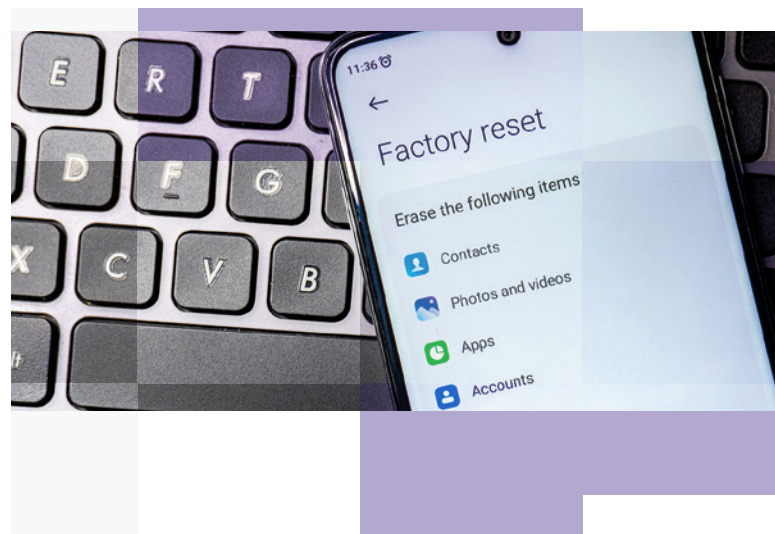
- install software and firmware updates as soon as they're available
- keep linked apps and your device's operating system up to date
- regularly review and remove apps, services or users that no longer need access.

> Dispose of smart devices safely

When selling, trading in or disposing of a smart device, take steps to protect your personal information.

- Restore it to factory settings.
- Unlink accounts and connected services.
- Remove saved devices, profiles and personal data.

When buying a second-hand smart device, perform a factory reset before use to ensure previous owners no longer have access to your data or your device.



Ransomware

Ransomware is a type of malicious software that can lock you out of your device or make your files inaccessible. Cybercriminals then demand payment, often in cryptocurrency, to restore access or prevent stolen information from being shared online. A ransomware attack can have a serious impact, including the loss of important documents, financial records or personal photos. Following good cyber security practices can greatly reduce the likelihood and impact of an attack.

To help protect yourself from ransomware:

- Keep your devices, applications and operating systems up to date.
- Regularly back up important files to an external drive or trusted cloud service.
- Ensure your backups can be successfully restored if needed.
- Use reputable antivirus software and keep it updated.
- Enable ransomware protection features where available.
- Turn on MFA for important accounts such as email.
- Use a standard user account for everyday activities instead of an administrator account.
- Create a strong, unique password for each account and never reuse them.
- Be cautious when opening email attachments, downloading files or clicking links from unknown sources.

What to do if you are affected

- Disconnect the affected device from the internet and other devices.
- Do not pay the ransom, as there is no guarantee your files will be recovered.
- Run a security scan using trusted antivirus software.
- Restore your files from a clean backup if available.
- Seek professional IT or cyber security assistance.

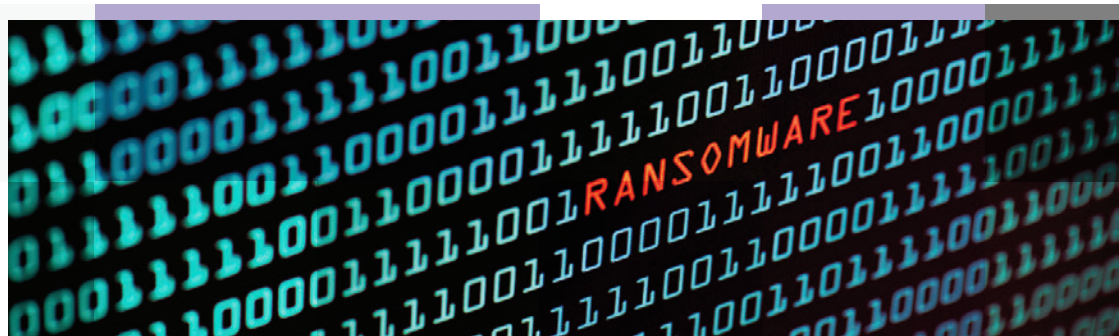
Use antivirus software

Antivirus software helps protect your devices as well as your personal information from malicious software or 'malware'.

Malware can stop your device from working and steal, delete or corrupt your files. It can also allow someone to access your device and the data on it. Malware can infect your device if you open, download or interact with infected content, such as:

- links
- attachments in emails
- websites
- apps or files you download from the internet.

A malware infection can cause serious harm, such as damage to important files, identity theft and financial loss.



How to get antivirus software

Your device may have built-in antivirus software. Most modern Microsoft and Apple computers include it for free. There are also third-party companies that sell antivirus software. They tend to come with more features than the free software.

Some new computers come with a free trial of third-party antivirus software. If you have this option, find out how the software works, what it costs and whether the company has a good reputation.

Third-party antivirus software may also include unrelated services such as a Virtual Private Network (VPN) or password manager. Consider the quality and reputation of these separate features before you buy.

Be aware that antivirus software doesn't protect against all threats. It works best when you also have good security habits and practices.

Get the most from your antivirus software

Follow these steps to help keep your device secure, whether you use built-in antivirus or a third-party product.

Depending on your device and antivirus software, some steps may happen automatically.

> Turn on automatic updates

For antivirus software to work well, it needs regular updates along with your device.

Check both your device and software are set to install updates automatically. Also check this setting is still on when you make system updates or changes.

Check your antivirus software is also getting 'signature updates', which help detect new threats. If you use third-party antivirus software and your subscription has expired, you may need to renew it or switch to a free option to keep getting the latest signature updates.

> Make sure your antivirus software is on

Built-in antivirus software should be on by default. Check your device settings for more information. If you're using a third-party product, check it's installed and working properly by opening it on your device.

> Run a full scan

If you've just set up a new device or turned on antivirus software for the first time, run a full scan to check for malware.

> Schedule automatic scans

After your first scan, set your antivirus software to scan automatically at regular intervals.

Depending on the type of device, it may do this in the background or at set times, such as once per week.

> Turn on ransomware protection

Ransomware is a type of malware. Cybercriminals use it to block access to your device or data until you pay a ransom. Some antivirus products include ransomware protection. Make sure you use it if you have the option.

Be aware of fake antivirus products

When searching for antivirus software online, be aware that malware may pose as a real antivirus product. Some forms of malware try to trick you into clicking on fake alerts by making them look like alerts from your antivirus software.

If buying antivirus software, make sure you get it from the provider's official website or an authorised app marketplace, such as Apple App Store, Google Play Store or Microsoft Store. Avoid following links in ads, pop-ups or emails, as they can lead to fake sites.

Make regular backups

- Your devices hold your important personal information and data. If your device is lost, damaged or stolen, your data may be lost too. Getting your data back can be costly or even impossible. That's why it's important to back up your data regularly.
- Making regular backups means you'll have a safe and recent copy of your files and settings. You might back up every hour, every day, once a week, or even once a month. How often you back up depends on how often your files change and how important they are to you. If available, turn on automatic backups so they run without you needing to do anything.

Decide what to back up

Choose what data to back up based on how important it is to you. For example, your back up may include:

- financial, medical and legal records
- photos and videos
- text messages.

Decide how to back up

There are several ways to back up your data. You can use a secure cloud service, an external storage device, or both.

> Back up to the cloud

When you back up to the cloud, a copy of your data is sent over the internet and saved on remote storage servers. Common cloud services include Apple iCloud, Google Drive, and Microsoft OneDrive.

> Back up to an external storage device

Another way to back up your data is to use an external storage device, such as a USB drive or external hard drive. This means storing your backup somewhere other than your main device. Keep your backup device in a safe and secure place so you can find it when you need it.

> Hybrid backup

You could combine cloud and external storage to get the benefits of both. For example, use cloud backup for important files you need often, and use an external hard drive to back up your entire system (known as a system image).

> Secure your backups

Your backup may contain sensitive information, so protect it like you would any important files. Follow these tips to keep your backups secure.

- Disconnect your backup when not in use.
- Keep an offline backup and ensure your backup device is updated.
- Store your backup in a different location to your device.



Review your apps and permissions

Checking app permissions helps protect your information and keep your device safe. Follow these key steps to manage app permissions:

- Check app permissions often: See which apps can use your location, contacts, camera, microphone, and other features that could impact your privacy.
- Manage location permissions: Stop apps from using your location if they don't need it.
- Limit app data access: Only let apps use the data they need, like contacts or photos, to reduce risks.
- Be careful when installing apps: Only download apps you need. Check reviews to see what they do and what permissions they ask for.
- Remove unused apps: Uninstall and delete apps you no longer use to free space and stop them from accessing your information.

Encrypt your data

Encryption is a way of scrambling information so only people with the right key can read it. When data is encrypted, it looks like unreadable text to anyone who doesn't have permission.

Encryption is used in many places to keep information safe, including:

- sending messages in secure apps
- shopping or banking online
- storing files on computers and phones.

Encryption helps protect your privacy. It also reduces the risk of criminals stealing or changing your data.

Check for encryption

Without encryption, criminals could steal your passwords, money or private messages. Encryption makes it much harder for anyone else to read or change your data.

Here's a simple checklist for spotting encryption in everyday internet use:

- Look for https:// in the website address.
- Use messaging apps that say they have end-to-end encryption.
- Make sure online banking and shopping pages show secure connections.
- Check your Wi-Fi is locked with a password and set to WPA2 or WPA3.



Dispose, trade or sell your device securely

Take the following steps to protect your information before selling, trading or throwing your device away.

Before disposing of your device:

- make a backup copy of your data
- take out any removable media, such as a SIM or SD card
- remove any identifying marks
- erase your data by doing a factory reset.

If you don't dispose of your device securely, someone could access the information on it. This includes your:

- account logins
- credit card details
- files, photos and videos
- personal messages.

End of support

If your device no longer supports the latest operating system or software upgrade and there are no issues with power, internet or storage, it may have reached 'end of support'. This means your device, software or system no longer gets updates or technical support. Your device might still work, but it will be less reliable and more at risk of cyber attack.

The best way to stay protected is to upgrade to a newer device. If that's not an option, follow these tips:

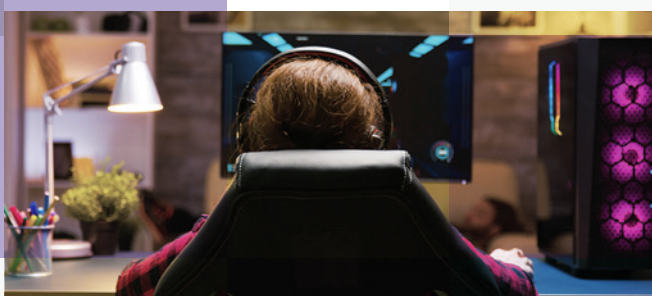
- Disconnect it from internet, Wi-Fi, Bluetooth.
- Don't use it to store important data or log into accounts.
- Don't open unknown links or attachments.
- Remove apps you don't use and avoid installing new ones.
- Keep it secure so others can't access it.



Secure your online activity

Staying secure online means protecting yourself in different ways. Build good habits such as:

- browsing securely
- using safe home and private networks
- managing what you share on public profiles
- staying alert when using social media and online games.



These habits help protect your money, privacy and identity from cybercriminals.

Use secure, and trusted websites

Always use secure and trusted websites, especially when entering personal or financial information. Avoid sites with pirated or illegal content, as they may carry malware.

Fake websites can look real, but their web address is often slightly different. For example, auspost.live instead of auspost.com.au. If you know the correct website address, type it carefully into your browser's address bar to avoid landing on a fake site.

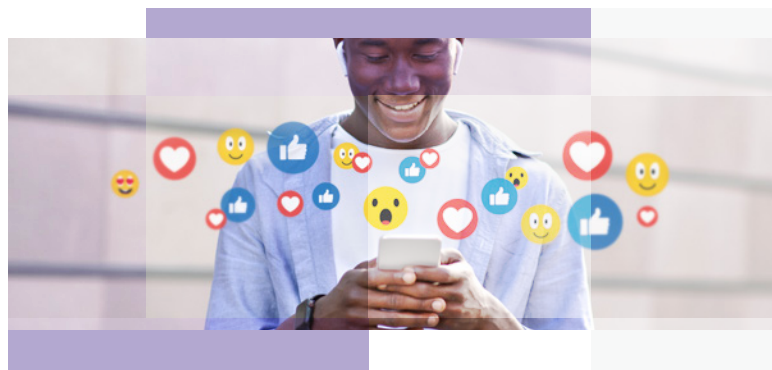
Manage your online identity

Review the privacy settings on your social media and messaging apps so you control who can see your information. Anything you post can be used by others, including cybercriminals who may try to scam you or steal your identity. Check your settings often, especially after updates.

Consider keeping your profiles private and only talking with people you know and trust. If you get an unusual message from someone you know, contact them directly to make sure it's really them.

To help protect your privacy online, consider these tips:

- Say 'no' to optional cookies.
- Use a reputable ad blocker to stop websites from tracking you.
- Use a reputable web browser and search engine that enforces privacy.
- Turn off automatic image downloads in your emails.
- Avoid using in-built social media web browsers.



Limit what you post online

Once you post something online, it's out there for anyone to see and can be very difficult to remove. Be careful of sharing information such as your:

- phone number
- email address
- home address
- date of birth
- bank and credit card details
- employment details
- school or university (including where your children go to school or childcare).

Also, be aware of what your photos and videos can reveal about you. Avoid including location details such as check-ins, street signs and metadata. You can go one-step further by changing your settings so your friends and family can't tag you in their photos.

Delete your unused accounts

Consider deleting any social media and messaging accounts you no longer use. Leaving them active can expose your information if you're not checking them.

Remember that uninstalling an app doesn't delete or deactivate your account. You will need to do this first through the official app or website before uninstalling the app.

Protect your accounts

Protect your accounts to keep your personal information, money and identity safe from cybercriminals.

Follow these simple tips to protect your accounts:

- Use strong and unique passwords.
- Turn on multi-factor authentication.
- Delete suspicious messages or links.

By adding simple layers of protection, it can be much harder for anyone to misuse your accounts.

Protect your social media and gaming accounts

Social media and online gaming are common targets for scammers. These accounts can be valuable because they may include game licenses or linked payment details.

Protect these accounts the same way you protect your bank or email accounts. Cybercriminals may try to scam you, steal your information, or install malware through social media or games.

Many of the same tips apply across social media, messaging apps and online games:

- Turn on MFA, use passkeys, and when passkeys are not available use strong, unique passwords for each account.
- Lock your devices when not in use and never save logins on shared or public devices.
- Be cautious with third-party apps, mods and plug-ins. Only install from official stores or trusted developers.



- Use trusted networks. Avoid logging in or making purchases on public Wi-Fi and use mobile data if possible.
- Don't click links sent in direct messages (DMs) or chats - even from friends.
- Limit what you post and share. Review privacy settings, disable location sharing, and avoid oversharing personal details.
- Be wary of giveaways, trades and offers that seem too good to be true. Keep transactions inside official marketplaces.
- Watch for warning signs of compromise (unexpected password resets, new logins or messages you didn't send).

> Extra tips for gaming

- Use legitimate game clients and keep games, launchers and consoles up to date.
- Back up your game saves and important files.
- If a gaming device is compromised (crashes, popups, unknown apps), reset it and change your passwords.

> Extra tips for social media & messaging

- Review who can find, tag or message you.
- Review privacy and messaging settings, including limiting direct messages, friend requests and other contact from unknown accounts on platforms where this is not enabled by default.
- Regularly remove unused accounts and revoke third-party app permissions.

Secure your email account

There are several ways to make your email account more secure.

- Start by using a passkey, or a strong password where passkeys are not available.
- Use multi-factor authentication
- Set up account recovery options
- Keep your devices and software up to date.

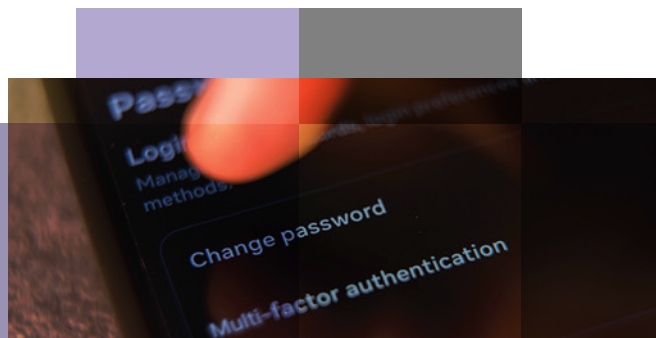
Improving your email account security is only the first step. You also need to be aware of what to do and what not to do when using your email at home and in public. This includes:

- checking your recent login activity
- using public Wi-Fi securely by ensuring you are connecting to the right hotspot; checking you are visiting secure webpages; disabling fire sharing and thinking twice about what you access.
- consider deleting unused accounts that are no longer required.

> Know the warning signs of email compromise:

- Your login details don't work.
- Your password recovery details have changed.
- You notice multiple login attempts at unusual locations or times.
- You get an unexpected email to reset your password.
- Your contacts are receiving emails from you that you didn't send.

If you notice any of these signs or suspect your email is compromised, reset your password and sign out of all sessions.



Use your own personal and work accounts

> Create different user accounts

On your personal computer you should have different user accounts for work and personal use. Avoid using an admin account for everyday tasks such as emailing or web browsing. A standard user account limits access to files, programs and settings on your device.

> Change your user account type

Check your account type in your computer's settings. On Microsoft Windows, use Control Panel or Settings to switch from an administrator account to a standard one. On a Mac, you can manage standard accounts in System Settings.

Keep a separate administrator account for tasks that need extra access, like creating new users. Protect it with a strong password and don't share it.

Make sure everyone who uses your computer has their own standard user account. This limits how much access a cybercriminal could get if one account is compromised.

Set up accounts for children with limited permissions and use parental controls. These tools help you manage what they can see and do online, reducing the risk of cyberattacks.

> Change default admin logins

A user account is the login you use on your computer at home, school, or work. Cybercriminals often target accounts with weak or default settings to gain access and steal information.

Changing default admin logins and using stronger security habits can help protect your accounts and reduce the risk of a cyberattack.

> Use administrator accounts only when needed

If cybercriminals access an administrator account, they can control your whole computer, which is why these accounts are a major target. Giving everyone admin access increases the risk of lost files, accidental changes, or malware from clicking fake links.

Think of an admin account like a master key. If someone uses it for everyday tasks and it falls into the wrong hands, everything becomes exposed. The same is true when you use an administrator account for daily computer use.

Secure your login

- Adjust your settings to automatically lock your account when you're not using it. A shorter lock time keeps your account more secure.
- Consider alternative login features such as Windows Hello or Apple's Touch ID. They provide a more secure way to login using fingerprint or facial recognition. You can also use physical security keys with a fingerprint or PIN instead of a username or password. Learn more about alternative login features from Windows and Apple.



Use networks safely

Staying safe online also means protecting the networks you use. Learn how to secure your connection and use public Wi-Fi securely to keep your information and devices safe.

Secure your Wi-Fi and router

A Wi-Fi router is a small box that lets your devices connect to the internet. It acts like a doorway between the internet and your private digital space. Securing your Wi-Fi and router stops threats from getting into your network and stealing your data.

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, connect smart home devices to a separate network from your main network to reduce the risk if they are compromised.

Turn on your firewall

Check if the firewall on your router is on. It is a built-in feature with most routers. Firewalls help to prevent suspicious traffic from entering your network. It will allow or deny traffic based on security rules.

Use public Wi-Fi networks securely

Public Wi-Fi is convenient when travelling or dealing with poor reception, but it does come with risks. These networks are often insecure or poorly configured, making it easier for cybercriminals to access your data. Where possible, use your mobile hotspot for internet connectivity.

You can use public Wi-Fi if you're careful. Avoid sensitive tasks, like online banking or other financial activity, while connected to public networks.

Tips to protect yourself when using public Wi-Fi

> Connect to the right Wi-Fi network

- Confirm correct network name on signage or with staff at the venue or location.

> Disable file sharing

- Turn off file sharing over Wi-Fi before you connect to a public network.

> Think twice about what you access

- Avoid accessing sensitive information, such as online banking, on public Wi-Fi networks. Use your mobile hotspot where possible.



Secure your online shopping and banking

Be cautious when shopping online. Do your research before you buy and stick to trusted companies and websites. If you're not confident about how the website will use your information, shop elsewhere.

Stick to well-known businesses and cross-check information on their website. You can research online shops by checking their:

- customer reviews
- fine print such as privacy, warranty, refund and complaints policies
- Australian Business Number (ABN) through [ABN Lookup](#), if they're a local business.

Spotting a safe site for online shopping

You should also do some research on online shopping websites before buying from them. You can find website domains by carefully typing them into your web browser. You can also use your favourite, trusted search engine to search for them. Avoid any search results that are advertisements or sponsored links.

> Online auctions

Online auctions can be fun and help you find good deals, but they also attract scammers. A common scam happens when someone claims the auction winner backed out and offers the item to you if you pay outside the auction site. Once you pay, the scammer disappears and the auction site cannot help you.



Here are some tips to help protect yourself:

- Always make your transaction within the auction website. Don't contact buyers or sellers in private.
- Keep printed and electronic records of all bids. Make sure you have noted down the item's description. Save emails to and from the seller, and transaction records or receipts.
- Consider using a reputable third-party escrow service if you're buying something expensive. These services hold the funds until you receive your goods.
- Check reviews and rating scores if the website uses a feedback rating system.
- Read the terms and conditions before using an online auction site. Marketplaces like eBay have dispute resolution processes if something goes wrong.

Online shopping scams

The best way to avoid being a victim of cybercrime is to stay informed. Learn how to secure your device and recognise a fake website or scammer.

> Warning signs when shopping online

If something looks too good to be true, it probably is. Watch for these warning signs before you buy:

- The website looks unprofessional or poorly designed.
- The prices seem unrealistically low or claims impossible benefits.
- The seller asks for payment by wire transfer, gift cards, digital currency or other unsafe methods.

- There is no clear contact information (phone, email, or address).
- The privacy details, terms and conditions, return policies, or dispute processes are missing or unclear.
- The seller won't let you use secure payment options.
- Your credit card details are requested for reasons unrelated to your purchase.
- The shipping costs or extra fees look unusual.
- The website link or the back button does not work.

> More warning signs on social media, classifieds and marketplaces

- New pages with low engagement are a red flag. Look at the page's age, followers, and posting history.
- A one-way conversation with little community interaction can indicate a fake store.
- New seller accounts with multiple very cheap listings may be scams.
- Private pages can be suspicious. True sellers keep their pages public.
- Scammers often copy real pages. Watch for small spelling changes or added symbols in business names.
- Don't use PayPal 'friends and family' for purchases, as it offers no buyer protection.

> Security tips for online shopping

Consider the following tips when shopping online:

- Use secure payment methods like Apple Pay, Google Pay, PayPal, BPay or your credit card. You can dispute a payment through these methods if something goes wrong.
- Avoid sending your bank or credit card details by email.
- Avoid clicking on payment links or sending payment details in an SMS.
- Check your bank statements for unusual transactions and report them to your bank.
- Limit how much personal information you share when making an online purchase (only fill in mandatory fields).

Also make sure you know how to pay securely when paying online. Scammers might ask you to use payment methods such as:

- direct bank deposits
- money transfers
- digital currencies (like Bitcoin).

Those payment methods are an easy way for them to steal from you. It's unlikely you will get your money back if you pay a scammer through one of these methods.



Choosing secure online payment methods

Apple Pay/Google Pay

Apple pay and Google pay are digital wallets that let you pay online safely without sharing your real card information with stores. Using a digital wallet reduces the risk of data theft.

PayPal

There are two payment types to choose from if you're sending funds to someone using PayPal. Use the 'goods and services' payment option if you're paying for an item you've agreed to buy online. This option has purchase protection.

If a seller insists on the 'friends and family payment' option, this could signal a potential scam. You won't be able to recover any money sent this way.

BPay

Use a legitimate biller code and customer reference number if you use BPay. Don't pay by direct transfer to a bank account.

Credit cards

You may want to set up a second card with a low credit limit and use it only for online purchases. This will minimise your financial losses if these card details are ever compromised after shopping online.

If you need to cancel your card, you'll still be able to use your primary credit or debit card.

Protect your information after an online purchase

Once you've made an online purchase, you still need to remain vigilant. Cybercriminals can target you even after you've made a purchase on a legitimate website.

Follow our tips to learn what to be aware of after you've bought something online.

Don't click on suspicious links

Genuine websites won't ask you to click on links in emails to verify your order.

If you're asked to do this, contact the buyer directly using details from their website. Don't reply to the email or click on any links.

Check the sender's address on emails about online orders

Scammers try to impersonate brands or sellers by copying their email branding. The best way to identify if it's a genuine email is to check their email address. Check if the email address matches with the contact details on the online store's official website.



Ignore and report suspicious contact

Scammers may contact you about an online purchase to try to steal your personal or financial details. Stay alert to strange calls, messages or emails about your orders.

Be cautious if an order confirmation looks wrong, doesn't use your name, or asks you to click a link to fix or verify your order. Fake messages may also mention orders you didn't make or show the wrong currency.

If someone contacts you about a problem with your order, stop the conversation and reach out to the organisation using the contact details on their official website. Ignore and report any SMS or instant message you receive that seem suspicious.

If you need more help, you can call our cyber security hotline on 1300 CYBER1 (1300 292 371), or follow our advice on how to [report](#) and [recover](#).

Be careful saving your payment details

Avoid saving your payment details to your online shopping accounts or browser.

This includes:

- credit or debit cards
- bank account details
- payment services such as PayPal.

Storing your payment details online increases the risk of someone stealing them if your account is hacked.

If you do save your payment details, protect your accounts where possible with:

- [a strong and unique password](#)
- a strong multi-factor authentication such as [passkeys](#).

Be on the lookout for fake delivery scams

Don't let your guard down while you're waiting for your goods to arrive.

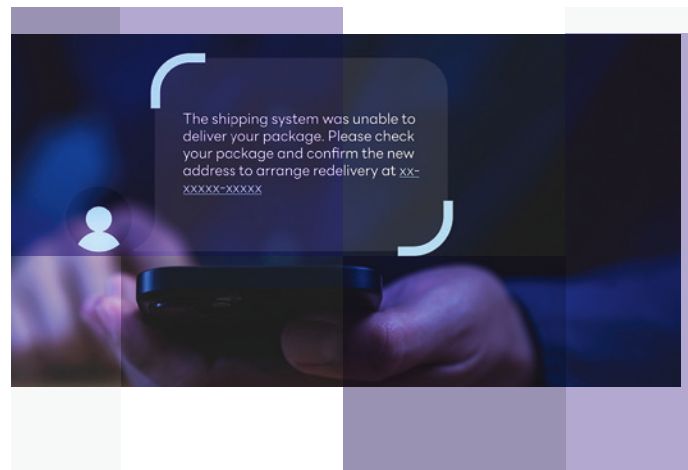
Cybercriminals can send fake parcel delivery notifications asking you to click on links to verify your delivery details. They might trick you into downloading malware or giving away your personal details.

You might get an email or text message pretending to be a parcel delivery service. It could say you have an 'undelivered package' waiting for pick up. You should be cautious if the message:

- doesn't use your name
- doesn't have many details about your order
- threatens to charge you more than you've already paid.

Australia Post will never ask you to click a link to fix parcel collection issues. They also won't ask you to update or verify your information.

Call the organisation if you're unsure. Remember to use contact details from an official website or other trusted source.



Use artificial intelligence responsibly

Artificial intelligence is a way of making computers perform tasks that usually require human thinking. It allows computers to learn, solve problems, understand language, and make decisions. AI works by using data and simple rules called algorithms. In short, it's like teaching a computer to be smart so it can help make life easier.

You'll see AI in many everyday tools and apps, such as:

- chatbots and virtual assistants
- translation tools
- apps that recommend music, videos or products
- tools that help write, plan or summarise information.

When you use AI, there are some important things to think about. You should not share personal information, like passwords or bank account numbers. Most AI systems are not designed to handle confidential information, and that information could be used by AI systems in ways you did not intend - such as for system improvements. When using AI it is recommended you review the policy on how your personal information will be handled.

There are steps you can take to engage with AI securely. Use the questions below to find AI risks and manage them:

- Does this AI system have a good reputation?
- Do I need to share this information with the AI system?
- How will the AI system use my information?
- What does its privacy policy say?
- What can I do to ensure the output of the AI system is accurate and appropriate for use?

Consider your privacy. AI can analyse large sets of data which can attract cybercriminals. Even when data is anonymised, there is a risk that cybercriminals may still be able to identify who the data belongs to.

Try to limit oversharing, read the fine print, and treat AI like any online service, helpful, but not always private or unbiased.

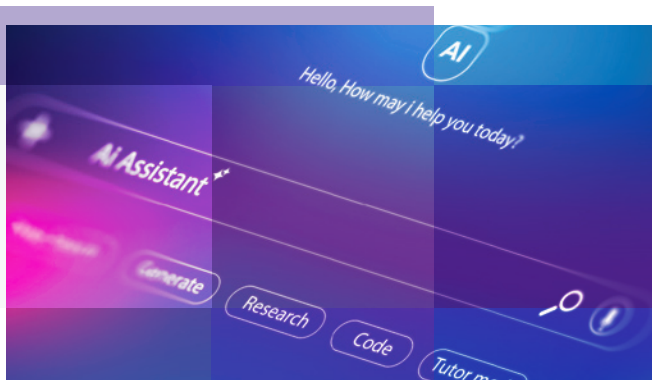
Be selective with what you share

Avoid entering sensitive information into AI tools unless you fully trust the provider. Assume it can store everything you share.

Check data policies

Review the privacy policy of the AI service you're using. Look for:

- what data is collected
- how it is used
- whether it's shared with third parties
- whether your data is used to train the AI tool/service.



Control your digital footprint

Where possible, use AI tools that allow you to delete your history or turn off data storage. You can also use separate accounts or email addresses to limit the link to your identity.

Watch for bias and accuracy

Be cautious if an AI tool gives advice or recommendations. AI outputs can be biased, inaccurate, incomplete or even made up (known as hallucinations). Always cross-check important decisions with trusted sources.

Security first

Be wary of entering personal information into free/public AI tools and follow your employer's advice on entering confidential work information and approved tools.

Check where your data is stored

Data processed overseas may not be protected under Australia's privacy laws. If possible, use AI providers that store data locally or comply with strong regulations.

Use AI agents securely

Some AI tools can act on your behalf by completing tasks automatically, such as organising information, sending messages or interacting with other apps. These tools are called AI agents. While they can be helpful, they may also increase security and privacy risks if they are given too much access. AI agents may find shortcuts or loopholes that technically achieve an objective but conflict with the user's intention or introduce security vulnerabilities.

If you use AI agents, only turn on features you understand and need. Check what accounts, apps or data the agent can access. Avoid giving it permission to make important changes without your approval. Where possible, start with limited access and review settings regularly.

Individuals should maintain a human-in-the-loop to review, approve and monitor agent actions, particularly where interactions with third-party services or other users may occur.



Travelling overseas

If you travel overseas, use safe online habits and watch for cyber threats. Follow this travel advice to stay secure at every stage of your trip.

Keeping your electronic devices secure when travelling overseas is just as important as keeping your passport safe. Cyber criminals targeting electronic devices is a real and growing risk.

Before you travel

Use these tips to secure your data, accounts and devices before travelling. This will reduce your likelihood of being a target for cybercriminals.

Protect your data

Make a backup of your important files and keep it safe at home. Leave behind any devices or information you don't need for your trip.

Bring only what you need

Think about using a separate device just for travel, like a burner phone (a separate cheaper phone). Don't store personal data, accounts or passwords on it. If someone gets access to it, there's less risk of your personal information being misused.

While you travel

Stay alert about your security during your trip by following these tips. This is when you're most at risk of cyber threats.

Lock your devices

Lock your devices whenever you are not using them. Where possible, always keep your devices with you.

Use trusted accessories, devices and networks

Only use chargers, cables, and other devices bought from reputable stores. USB drives can be lost, stolen or infected with viruses. Avoid using public computers, as they may contain malware and are not safe.

Use public Wi-Fi securely by ensuring you are connecting to the right hotspot; checking you are visiting secure webpages; disabling file sharing and thinking twice about what you access. You can also switch to mobile data or your personal hotspot when you can.

Think twice before sharing travel plans

Don't share your location or travel plans like your flight number or hotel details, on social media or other online platforms visible by others. Even photos in social media can give away personal information.



After you travel

Even after you return home, stay alert for signs that a device or account may have been compromised. To further secure your devices, consider:

- changing the passwords for your devices and accounts
- disposing of your burner phone if you used one, including any SIM cards, eSIMs or microSD cards
- wiping any removable storage used when travelling, such as USB drives or SD cards.

Get help with a suspected incident

It is important to act as soon as you believe someone has access to your accounts or devices. Log out of the compromised device and don't use it to change your passwords.

If you need more help, you can call our cyber security hotline on [1300 CYBER1 \(1300 292 371\)](tel:1300292371), or follow our advice on how to [report](#) and [recover](#).

Follow Smartraveller advice

Smartraveller is a government website provided by the Australian Department of Foreign Affairs and Trade, which provides timely advice for Australians travelling overseas.

For more tips when travelling, visit smartraveller.gov.au.



Getting help

Cybercrime can happen to anyone. If it happens to you, report it as soon as possible and follow our guidance to recover and reduce the chances of it happening again.

If there is an immediate threat to life or risk of harm, call triple zero (000).

Report a cybercrime

You can report a cybercrime, incident or vulnerability to us at cyber.gov.au/submit-a-report

Your report helps disrupt cybercrime operations and makes Australia more secure online. Your confidential report will be sent to the relevant state or territory law enforcement agency for review and action.¹

You can also contact the Police Assistance Line on **131 444** or Crimestoppers on **1800 333 000**.

For more recovery advice including where to get help, visit cyber.gov.au/recover-from-a-cyber-incident

Contact us

We're here to help all Australians affected by cyber incidents – we provide free advice and assistance:

- Call our hotline 24 hours a day, 7 days a week on **1300 CYBER1** (1300 292 371) or visit cyber.gov.au/contact-us
- Sign up for alerts at cyber.gov.au/sign-up-for-alerts

Connect with us on social media:

- [Facebook](https://www.facebook.com/cybergovau) @cybergovau
- [Instagram](https://www.instagram.com/asdgovau) @asdgovau
- [LinkedIn](https://www.linkedin.com/company/australiansignalsdirectorate) @australiansignalsdirectorate
- [X](https://twitter.com/asdgovau) @asdgovau



¹ Annual Cyber Threat Report 2023-2024

**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, the entity's logo, third party content, 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 <https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>

cyber.gov.au

