Print whole section

Cyber safety

What you can do to stay safe online.

Top cyber security tips for individuals

Tips for individuals to keep your personal information safe from cyber criminals.

Top cyber security tips for businesses

Tips to keep business and client data safe from cyber criminals.

Report a system security vulnerability

Find out about our security vulnerability disclosures policy and how to report potential vulnerabilities in ATO systems.

QC 40958

Top cyber security tips for individuals

Tips for individuals to keep your personal information safe from cyber criminals.

Last updated 8 May 2025

Increase your online security

Your personal information is an important part of your identity. There are many ways you can interact with us online, and the following tips can help you make sure your online transactions with us are safe.

Use myID to access online services

myID, is the most secure way to access ATO online services and helps protect against identity crime, including tax fraud.

If you can, we recommend you secure your sign in with a Strong myID and protect your valuable personal information. Follow our simple steps to **increase your online security with myID** and set your online access strength to Strong.

Use multi-factor authentication

Multi-factor authentication requires a combination of:

- something the user knows (PIN, secret question)
- something you have (card, token), or
- something you are (fingerprint or other biometric).

Enabling multi-factor authentication increases your online safety, but the most secure way to access online accounts and services is by using myID. Protect yourself against cyber criminals and set up your myID now.

Use strong and secure passphrases

Consider moving from a password to a passphrase. Using passphrases can:

- boost the security of your accounts
- make it harder for cyber criminals to access your information.

A passphrase:

- should be easy for you to remember

- can involve a set of 4 or more random words, numbers and/or symbols depending on the website's password requirements.

The longer your passphrases, the better.

A random mix of unrelated words:

- is less predictable than a password
- will produce a stronger passphrase – for example, 'crystal onion clay pretzel'.

A password manager can help you generate or store passphrases. Regularly change passphrases and do not share them.

Regularly back up your devices

Back up your files and devices regularly on a physical device (such as an external hard drive) or in the cloud. This is helpful if your data becomes damaged, lost, stolen or infected by ransomware.

Secure your backup devices by making sure they are not continuously connected to your main network.

Make sure all devices have the latest available security updates

Cyber criminals hack devices using known weaknesses in systems or apps. Updates have software security upgrades and make it harder to hack.

Regular updates are critical in maintaining a secure system. It's important to:

- check for any updates regularly, or
- turn on automatic updates.

Antivirus software can help prevent, detect, and remove malware from your device. Make sure you turn on your antivirus software and keep it up to date.

Be careful when clicking on links, downloading programs or opening

attachments

Be careful when downloading attachments or clicking on links, even if the message seems to come from someone you know.

Always access our online services directly via ato.gov.au, my.gov.au or the ATO app – not by following a link.

Be sure you are downloading authorised and legitimate programs. Unless you know the program is legitimate, do not open attachments or download it.

Some programs contain malware that can infect your computer or be used to harvest your personal information.

Use a spam filter on your email account

Always use a spam filter on your email account and do not open unsolicited messages.

Be wary of downloading attachments or opening email links you receive, even if they are from someone you know.

Spam emails can be:

- embedded with malware
- used to trick you into providing information or buying non-legitimate goods.

Do not respond to or click on these emails. This can help you reduce the risk of your personal information being used fraudulently, or your computer being infected with malware.

Learn more about how to secure your email.

Monitor your accounts for unusual activity or transactions

Check your myGov Inbox and your accounts (including banking and online services) regularly. If you know everything is in order, it will be harder for a scammer to convince you otherwise.

If an organisation you deal with sends you an email or SMS alerting you to unexpected changes on your account, **do not**:

- click on included hyperlinks
- open any attachments.

You should immediately:

- check your account
- contact the organisation by telephone.

Be vigilant about what you share on social media

Keep personal information private and be aware of who you are interacting with.

People are accustomed to sharing personal information on social media. However, before sharing ask yourself if it is information you want strangers to have access to.

It's very easy for information on social media sites to be shared outside of your network, even when your security settings are set to private.

Be sure you know who you are speaking to on social media, and only share information with people you know and trust.

Criminals can use certain combinations of your personal information to impersonate you to access money, apply for credit cards and bank loans, or commit crimes.

Keep your personal information secure

Keep your tax file number (TFN), passwords, superannuation and other sensitive information (such as your myGov or bank account details) secure. Don't share them with others, including in emails, to prospective employers or on social media.

Secure your electronic devices wherever you are. Your personal information can be taken in an instant. In some situations, you won’t even know it was stolen.

Make sure you:

- do not leave electronic devices unattended
- secure your electronic devices with passcodes

- securely store portable storage devices (such as thumb and hard drives) when not in use.

Learn more about how to protect yourself online.

QC 50562

Top cyber security tips for businesses

Tips to keep business and client data safe from cyber criminals.

Last updated 28 March 2025

Media:Use strong and secure passphrases
http://tv.ato.gov.au/ato-tv/media?v=bd1bdiunji3ij9

Media: Protect your business against identity crime https://tv.ato.gov.au/ato-tv/media?v=bd1bdiunji3ij9 (**Duration:** 1:18)

Secure your information and systems

It is important you keep your business, staff and client information secure. If data is lost or compromised, it can be very difficult, time consuming and costly to recover.

Using advice from the Australian Cyber Security Centre (ACSC), we have created this list of top cyber security tips to help keep you and your business information safe:

- Use strong and secure passphrases
- Use multifactor authentication
- Manage your employees' accesses
- Remove system access from past employees
- Check devices have security updates
- Back up your data
- Don't use USBs or external hard drives from unfamiliar sources
- Use a spam filter on your email account
- Don't download computer programs or open attachments
- Secure your wireless network and avoid public wireless networks
- Be aware about what you share on social media
- Monitor your accounts for unusual activity or transactions
- Ask questions when sourcing software
- Keep up to date with security issues

Use strong and secure passphrases

Consider moving from a password to a passphrase. A passphrase uses 4 or more random words as a password. Regularly change passphrases and don't share them. Check whether your passphrases have been compromised and change them immediately if they have. Learn more about creating and protecting your passphrases.

Use multifactor authentication

Use multi-factor authentication if possible. Multi-factor authentication requires users to use multiple pieces of information to authenticate themselves.

Multi-factor authentication puts an additional layer of security on your accounts, making it harder for others to gain access.

Manage your employees' accesses

Implementing access controls can limit your employees' access to certain accounts, systems or programs and files, particularly those of

sensitive nature. This can minimise the damage caused by a cyber incident.

Remove system access from past employees

Unauthorised access to systems by past employees is a common cause of identity security or fraud issues for businesses. You can mitigate this risk by removing access for people who:

- no longer work for your business
- have changed positions and no longer require access.

It's also important to change the login details for any shared accounts.

Check devices have security updates

Applying updates, also known as patches, to your devices as soon as possible reduces the risk of a cyber incident occurring.

You should:

- turn on automatic updates as having automatic updates ensures the patches are applied as soon as they're available
- consider using vulnerability scanning software as they constantly monitor your systems to identify security risks and vulnerabilities
- upgrade devices, apps, or software to a newer product if the current product no longer receives updates
- run weekly anti-virus software and malware scans and update your system as soon as a patch becomes available.

Back up your data

Back up your files and devices regularly on a physical device (such as an external hard drive) or in the cloud. This is helpful if your data becomes damaged, lost, stolen or infected by ransomware.

A ransomware attack can:

- lock your computer or encrypt your data until you pay a fee to the criminal
- steal your personal or business information and threaten to leak or sell the information unless a ransom is paid.

Don't use USBs or external hard drives from unfamiliar sources

USBs and external hard drives may contain malware that can infect your business computers without you noticing. Ensure you and any employees only plug in USBs or external hard drives that have come from a trusted source.

Use a spam filter on your email account

Always use a spam filter on your email account and don't open any unsolicited messages.

Be wary of downloading attachments or opening email links you receive, even if they are from a person or business you know. They can infect your computer with malware and lead to your business or client information being stolen and used to commit fraud.

Don't download computer programs or open attachments

Be sure you are downloading authorised and legitimate programs. Unless you know the program is legitimate, don't open attachments or download any files.

Some programs contain malware that can infect your computer (including ransomware that locks your files until you pay a criminal). It can also be used to harvest your sensitive personal and business information.

Secure your wireless network and avoid public wireless networks

Avoid using public wireless networks to complete tasks. Not all wi-fi access points are secure. By making online transactions (such as online banking) on an unsecure network, you can put your information and money at risk.

Ensure you use a strong password for your business wi-fi. Consider the use of a private and public wi-fi network if you need to give your customers internet access.

Be aware about what you share on social media

Keep your personal and business information private and be aware of who you are interacting with online.

Scammers can take the information you publicly display and impersonate you or your business. Impersonators may send emails to trick your staff into providing valuable information or releasing funds.

Monitor your accounts for unusual activity or transactions

Regularly check your business accounts (including bank accounts, digital portals and social media) for transactions or interactions you didn't make or content you didn't post.

If you receive an email alerting you to unexpected changes on your account, don't open any links or attachments. Instead:

- check your accounts by searching for the organisation's website in a web browser
- phone the organisation using a number you've looked up.

Ask questions when sourcing software

When sourcing software for your business, it's recommended to ask vendors about their cyber security practices. For example:

- Will your data be stored in Australia or overseas?
- What data breach support services do they provide?
- Do they follow the Australian Cyber Security Centre's essential 8 mitigation strategies?
- Do they have security certification (ISO27001, iRAP) and what were the outcomes of any assessments?

Keep up to date with security issues

Constantly educate yourself about existing and emerging threats.

You can:

- report cybercrime online
- learn how to protect yourself against the latest scams at Scamwatch
- learn **how to protect yourself**

- get help if you are affected by a data breach at IDCARE.

If you believe someone has gained unauthorised access to your data, call the ATO on **1800 467 033** to report it.

Stay informed with the Australian Cyber Security Centre

For comprehensive information and additional tips, see Australian Cyber Security Centre The ACSC provides essential resources and expert guidance to help businesses of all sizes secure their systems and data.

QC 50563

Report a system security vulnerability

Find out about our security vulnerability disclosures policy and how to report potential vulnerabilities in ATO systems.

Last updated 21 August 2025

About our security vulnerability disclosure policy

The **online security** of our systems is our top priority. We take every care to keep them secure. But despite our efforts, they may still be vulnerable.

We are keen to engage with the security community. Our security vulnerability disclosure policy allows you to responsibly share your findings with us.

If you think you have identified a vulnerability in one of our systems, services or products, report it to us as quickly as possible.

As an Australian Government agency, we can't compensate you for finding potential or confirmed vulnerabilities. However, we can

recognise you by publishing your name or alias on this page.

Our policy doesn't authorise you to conduct security testing against the ATO. If you think a vulnerability exists, report it to us. We can test and verify it.

What the policy covers

Our security vulnerability disclosure policy covers:

- any product or service wholly owned by us to which you have lawful access
- any product, service and infrastructure we provide to shared service partners to which you have lawful access
- any services that are owned by third parties but utilised as part of our services that you have lawful access to.

Under this policy, you must **not**:

- disclose vulnerability information publicly
- engage in physical testing of government facilities
- leverage deceptive techniques, such as social engineering, against ATO employees, contractors or any other party
- execute resource exhaustion attacks, such as DOS (denial of service) or DDOS (distributed denial of service)
- leverage automated vulnerability assessment tools
- introduce malicious software or similar harmful software that could impact our services, products or customers or any other party
- engage in unlawful or unethical behaviour
- reverse engineer ATO products or systems
- modify, destroy, exfiltrate, or retain data stored by the ATO
- submit false, misleading or dangerous information to ATO systems
- access or attempt to access accounts or data that does not belong to you.

Do **not** report security vulnerabilities relating to missing security controls or protections that are not directly exploitable. Examples include:

- weak, insecure or misconfigured SSL (secure sockets layer) or TLS (transport layer security) certificates
- misconfigured DNS (domain name system) records including, but not limited to, SPF (sender policy framework) and DMARC (domain-based message authentication reporting and conformance)
- missing security HTTP (hypertext transfer protocol) headers (for example, permissions policy)
- theoretical cross-site request forgery and cross-site framing attacks.

How to report a vulnerability

To report a potential security vulnerability, send details to **VulnerabilityDisclosure@ato.gov.au**.

Provide as much information as possible, including:

- an explanation of the potential security vulnerability
- listing the products and services that may be affected (where possible)
- steps to reproduce the vulnerability
- proof-of-concept code (where applicable)
- names of any test accounts you have created (where applicable)
- your contact details.

We may need to contact you for more information to resolve the concern. We will handle your report confidentially in line with our **ATO privacy policy**.

We ask that you also maintain confidentiality. Don't publicly disclose details of any potential security vulnerabilities without our written consent.

What happens next

When you report a vulnerability, we will:

- respond to you within 2 business days
- recognise your contribution to our program.

We will **not**:

- financially compensate you for reporting
- share your details with any other organisation without your permission.

If you have any questions, contact us at **VulnerabilityDisclosure@ato.gov.au**.

People who have disclosed vulnerabilities

The names or aliases of people who contribute to our security vulnerability disclosure program will be published with their permission and shown below:

- Harrison Mitchell
- Cyril Luk
- Tim McMahon
- Callum Macarthur
- Scott Sturrock
- Anthony Jones
- Sayan Chakraborty
- Arkadeep Roy
- Sandeep Giri (Sndp)
- Ian Mckay.

QC 66993

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into

account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice