Print whole section

Cyber security advice

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 and tax professionals

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

QC 40958

Top cyber security tips for individuals

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

Last updated 23 March 2026

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 you know (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.

Check whether your passphrases have been compromised and change them immediately if they have. One way to check your credentials is by going to Have I Been Pwned. Learn more about creating and protecting your passphrases.

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.

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.

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

Make sure all devices have the latest available security updates

Cybercriminals can take advantage of known weaknesses in systems or applications. Software updates include security improvements that make it harder for attackers to use those vulnerabilities. Regular updates are critical in maintaining a secure system. It's important to either:

- check for any updates regularly
- 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 by typing ato.gov.au or my.gov.au into your browser, or by using the ATO app. Do not follow link from texts or emails or social media.

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, including ransomware that locks your files until you pay a criminal. It can also be used to harvest your sensitive 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 accounts by searching for the organisation's website in a web browser
- phone the organisation using a number you've looked up.

Be vigilant about what you share on social media

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

People are accustomed to sharing personal information on social media. However, before sharing, ask yourself if it's 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 and tax professionals

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

Last updated 23 March 2026

Increase your online security

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:

Protect your Digital ID

Your Digital ID, such as myID, is a simple and secure way to prove who you are when accessing government online services including Online services for business and Online services for agents.

myID uses encryption and cryptographic technology and the security features in your device, such as face or fingerprint recognition, to protect your identity.

Your myID belongs to you. Protect your myID and don't share it with others. Sharing your myID could enable others to access your personal data across online services.

If you're aware or suspect that your myID has been inappropriately accessed, report it immediately to the myID support line.

Use multifactor authentication

Multi-factor authentication requires a combination of:

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

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

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.

Check whether your passphrases have been compromised and change them immediately if they have. One way to check your credentials is by going to Have I Been Pwned. Learn more about creating and protecting your passphrases.

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.

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.

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

Make sure all devices have the latest available security updates

Cybercriminals can take advantage of known weaknesses in systems or applications. Software updates include security improvements that make it harder for attackers to use those vulnerabilities. Regular updates are critical in maintaining a secure system. It's important to either:

- check for any updates regularly
- 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.

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.

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 by typing ato.gov.au or my.gov.au into your browser, or by using the ATO app. Do not follow link from texts or emails or social media.

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, including ransomware that locks your files until you pay a criminal. It can also be used to harvest your sensitive personal and business information.

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.

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. If you need to give your customers internet access, consider setting up separate private and public wi-fi networks.

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?

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

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

Be vigilant about what you share on social media

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

People are accustomed to sharing personal information on social media. However, before sharing, ask yourself if it's 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 or your business to access money, apply for credit cards and bank loans, or commit crimes.

Impersonators may send emails to trick your staff into providing valuable information or releasing funds.

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 reduce the risk and potential impact caused by a cyber incident.

Where your business or practice uses our online services, set a reminder to do a regular check-up in both Relationship Authorisation Manager (RAM) and Access Manager. By regularly reviewing and updating authorisations and permissions, you help keep your business secure and compliant.

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 ensuring the right people have the right access at all times. This includes:

- removing system access for people who no longer work for your business
- updating or removing system access for people who have changed positions and no longer require the same permissions
- updating or removing access to our online services on behalf of your business or practice in RAM.

It's also important to change the login details for any shared accounts or devices when staff leave or responsibilities change.

Keep up to date with security issues

Constantly educate yourself about existing and emerging threats.

You can:

- report cybercrime
- learn how to protect yourself against the latest scams at ScamWatch
- learn how to protect yourself

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

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

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

Tax professionals

As a tax professional, you are vital in ensuring the integrity of the tax and superannuation systems. When you represent your clients, it's important you take reasonable steps to avoid enabling tax fraud.

Your business holds sensitive data that is appealing to identity thieves and cybercriminals. It's important you protect this data.

Identifying and protecting your clients

To help protect your practice and client information we recommend you:

- apply or consider each of the above cyber safety tips
- follow the agent verification methods guidelines and check the proof of identity for all new clients
- question any discrepancies in proof of identity
- avoid retaining copies of any documents used to verify clients
- only lodge for clients whose identity you have confirmed
- check existing client records for unusual updates or lodgments

Reporting fraud

Fraud can be the result of many things, including criminals:

- stealing someone's identity to lodge incorrect returns and steal refunds

- obtaining access to your client records to gain information
- impersonating your business to gain a benefit.

Tax professionals may be targeted to steal client information. Criminals may also use tax professionals' businesses to lodge fraudulent claims.

To report suspected fraud or criminal activity, make a tip-off by phoning us on **1800 060 062** (between 8.00 am and 6.00 pm AEST, Monday to Friday).

You can also report a cybercrime.

QC 50563

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