



 [Print whole section](#)

Protect your information

Protect your personal information from identity thieves. Criminals can start using your identity with basic information.

Protect your personal identifying information



Learn how to protect your personal identifying information.

Security advice for tax professionals and businesses



Strong security practices to protect your business from identity thieves and cybercriminals.

QC 19354

Protect your personal identifying information

Learn how to protect your personal identifying information.

Last updated 27 September 2024

On this page

[Be aware of what you share](#)

[Your personal identifying information \(PII\)](#)

[Protect yourself](#)

[How we protect you](#)

[Spot the scam signs](#)

Be aware of what you share

Always be aware of what information you share. Your personally identifying information (PII) forms pieces of a scammers puzzle. Scammers can use this information to access your bank account, sign in to your myGov account, steal money and then commit fraud in your name.

To help protect yourself:

- **Stop** – Don't share your personal information such as your myGov, Tax File Number (TFN), or bank account details, with anyone unless you trust the person and they genuinely require your details
- **Think** – Ask yourself could the message or call be fake?
- **Protect** – Act quickly if something feels wrong. Phone us on 1800 008 540 if you have disclosed any personal information.

For more information on how to report scams, refer to [Verify or report a scam](#).

If you are the victim of a data breach and your personally identifying information has been accessed, go to [Data breach guidance for individuals](#).

Your personal identifying information (PII)

To commit identity crime or fraud, scammers only need some of your PII. This may include:

- full name
- date of birth
- current address
- myGov and ATO online login details
- tax file number (TFN)
- passwords
- bank account numbers
- credit card details
- driver's licence details
- passport details.

They can use this information in a variety of ways, such as to commit refund fraud in your name, access your myGov account to steal your tax refund, steal your superannuation or sell your identity to organised crime groups on the dark web or via other means.

If you suspect your personal information, such as your TFN, has been stolen, misused or compromised, phone us as soon as possible on **1800 467 033** between 8am and 6pm Monday to Friday. We will investigate and can place extra protection on your ATO account.

Protect yourself

Our top tips to keep your personal information safe are:

1. Don't give out your PII to anyone unless you've verified that the person you're speaking with is who they say they are and has a legitimate need to know your details.

2. Think before you click on a hyperlink or open an attachment. Scammers often use these methods to steal your PII or plant malware on your devices.
3. Always access online services by directly typing the URL into a browser, not by clicking on a link.
4. Use your Digital ID (such as myID), set to the strongest level you can achieve, to access ATO online services through myGov.
5. Protect your Tax File Number (TFN) - only give your TFN to organisations or people who have a legitimate need for it, such as your tax agent, current employer or bank. It's important to verify that the person you're giving your TFN to is who they say they are.
6. Never share your password/s. Consider using passphrases instead of passwords, a password manager can help you generate or store passphrases. You should also consider updating them regularly.
7. Enable multifactor authentication. If scammers obtain your password, it will be significantly harder for them to access your account.
8. Keep your devices up to date. Scammers can use viruses, malware and programs to access or steal your personal information on your devices including phones, computers and tablets.

For top cyber security tips for individuals, visit [Top cyber security tips for individuals](#). You can also set up [Voice authentication](#) to help protect your tax account and reduce the chance of scammers accessing it.

More information on securing your devices is available from the [Australian Cyber Security Centre](#) [↗](#).

How we protect you

We take the security and privacy of your personal information very seriously. We have steps in place to make sure your data and online transactions with us are secure and safe.

We keep your personal information safe by:

- confirming your details when you contact us

- having a range of systems and controls in place to make sure your data and transactions with us are secure
- logging access to your personal information (to help us identify any unusual behaviour).

To help you stay safe online, we:

- won't ask you for your TFN or bank details via return email, SMS, or on social media
- won't give your personal information to anyone without your consent, unless the law permits us to
- won't communicate with you on behalf of another government agency or ask another government agency to represent us.

Spot the scam signs

Scams can trick you into providing either personal information or paying money. Scammers use various methods of communication, they may send you an SMS, email, or call you.

If someone claiming to be from the ATO contacts you and advises that you have a debt or are owed a refund or asks for your myGov sign in credentials, bank or personal details such as your TFN, consider the possibility that it may be a scammer.

For more information about scams and how to verify a scam, see:

- [Verify or report a scam](#)
- [Scam alerts](#).

QC 50498

Security advice for tax professionals and businesses

Strong security practices to protect your business from identity thieves and cybercriminals.

On this page

[Tax professionals' role](#)

[Security advice for your business](#)

[Secure your physical premises](#)

[Secure your electronic information](#)

[Protect your Digital ID](#)

[Report fraud](#)

[Data breaches](#)

Tax professionals' role

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.

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

- 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
- train your staff in why and how to secure client information
- check existing client records for unusual updates or lodgments
- perform background checks on new employees
- educate your employees about what is appropriate to discuss on social media or by email.

Security advice for your business

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

Strong security practices can help mitigate the risks from identity thieves or cybercriminals infiltrating your systems. Criminals can try to access this information by:

- breaking into your business and stealing your records
- taking a photo of your business or employee details
- stealing your passwords, account logins or personally identifying information (PII)
- using legitimate access as an employee to steal information (also known as insider threat)
- using compromised emails with malicious links or programs
- sending emails to phish for information from your business
- exploiting security vulnerabilities in software.

Secure your physical premises

You can help keep your business, customer and employee information safe by:

- installing physical barriers such as locked doors and windows
- making sure you have appropriate alarm systems in place
- ensuring paper documents and devices are not left unattended
- filing paper documents in lockable storage units
- ensuring your mailbox is secure and cleared out daily to avoid mail theft
- securely storing portable storage devices (such as thumb and hard drives) when not in use.

Secure your electronic information

Secure your electronic devices and physical files wherever you are. Your information can be stolen in an instant. In some situations, you won't even know it's been stolen.

Stolen information could be used to commit crimes, often in your business' name.

Make sure you:


- don't leave your electronic information unattended
- ensure employees log out of systems and lock computers when not in use
- secure your electronic business files and employee information when they're not in use
- secure your electronic devices (such as phones or tablets) with passcodes.


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 fingerprint or face, 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](#) .

Report 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 8.00am and 6.00pm AEST, Monday to Friday).

You can also [report a cybercrime](#) .

Data breaches

If you have experienced a data breach, you will need to take steps to secure your business information and client records from potential fraud:

- [Data breach guidance for businesses](#)
- [Data breach guidance for tax professionals](#)
- [IDCARE](#)  provides help to organisations that experience data breach events. We also have information on [how to get help for identity theft](#).

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

© Australian Taxation Office for the Commonwealth of Australia

You are free to copy, adapt, modify, transmit and distribute this material as you wish (but not in any way that suggests the ATO or the Commonwealth endorses you or any of your services or products).