Australian Government
Australian Taxation Office

Protect your personal information at tax time

The Australian Taxation Office (ATO) is reminding people to protect their personal information at tax time.

Your personal information is valuable. Always be aware of what information you share.

If a scammer knows enough about your identity, they can pretend to be you and:

- lodge false tax returns
- gain access to your superannuation (super)
- commit fraud in your name
- access your bank account, or
- take out loans in your name.

How to spot a scam

Scams can be difficult to spot, here are some warning signs that it could be a scam:

- emails, text messages or social media interactions that ask you to click a link and provide personal information or provide copies of identity documents
- job ads that ask for your tax file number (TFN) as part of the application process
- online ads that ask for your personal information such as your bank account details or ATO online/myGov sign in details.

If someone claiming to be from the ATO contacts you via email or SMS and advises that you have a debt or are owed a refund or asks you to enter your myGov sign-in details or bank or personal details such as your TFN, do not click on links or provide any details.

We will never send an SMS or email that contains a link to log on to our online services.

How to stay safe from scams

Your personal details are very important, so only share them with people you trust. Be careful when sharing your:

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

Use the ATO app to safely and easily manage your tax and super on the go, and secure your sign in to ATO online services by using myID set up to the highest identity strength you can.

What to do if you suspect a scam

Here are some steps you can take if you think you have been contacted by a scammer:

- Don't respond. Always check the contact details first.
- Take a screenshot of the text or forward the **entire email** to ReportScams@ato.gov.au then delete the suspicious text message or email
- Use the verify call feature in the ATO app to check if a call from the ATO is genuine
- Hang up the phone if someone says they're from the ATO and the caller is threatening you
- Don't click on links, instead access online services by typing it directly into your internet browser.
- Ask someone you trust if you feel unsure about a communication that says it's from the ATO, or call the ATO on **1800 008 540** to check if it is real.

Where to get help

For more information about protecting yourself and your family from scams, visit the ATO website at ato.gov.au/ScamSafe or talk to a registered tax agent.

If you have paid money or given your personal information to a scammer, phone the ATO immediately on **1800 008 540** to report it.

See also:

- *Protecting your information* at ato.gov.au/ScamSafe
- *Is it a scam?* at ato.gov.au/EasyRead

Important: some people who charge money to help with your tax return may be trying to scam you. Registered tax agents are the only people allowed to charge a fee to lodge your tax return. You can check whether your tax agent is registered at tpb.gov.au

Disclaimer: This information is a general summary only and was current as at May 2026.

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).