Print whole section

Scams, cyber safety and identity protection

Learn about scams, cyber safety and how to protect your personal information.

Latest updates on scams, cyber safety and identity protection

Stay up to date with the latest news about scams, cyber safety, and identity protection.

Verify or report a scam

What to do if you get a phone call, text message or email that you're not sure is genuine.

Scam alerts

Find information and examples on the latest tax and super-related ATO impersonation scams.

Scam data

See the latest data on ATO impersonation scams.

Protect your information

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

Help for identity theft

If you know or suspect someone has stolen your tax file number or your tax-related information, contact us immediately.

Help with data breaches

What to do if you or your business has been affected by a data breach.

QC 49586

Latest updates on scams, cyber safety and identity protection

Stay up to date with the latest news about scams, cyber safety, and identity protection.

Last updated 13 October 2025

Temporary hold on bank accounts

13 October 2025

To help keep payments more secure we're updating our card payment systems.

Between 24 February and 30 November 2025, if you have a payment plan with us that’s linked to a credit or debit card, you may see a temporary hold in your bank statement named 'ATO payment'. The hold amount will be:

- $0 for Visa and Mastercard
- $0.10 for American Express.

If you do see this, you don’t need to do anything. It's not an additional charge and will be automatically removed after 5 days.

This is a legitimate transaction, but in future if you are unsure of any transactions view our tips on how to **verify or report suspected tax related scams**.

No more hyperlinks in our SMS

1 July 2024

We no longer use hyperlinks in outbound unsolicited SMS. This will help the community identify legitimate ATO messages and spot ATO impersonation scams, especially during tax time.

SMS continues to be one of our most reported channels for scams. These scam messages usually include hyperlinks to fake websites (such as a fake myGov sign in page). These hyperlinks are designed to steal your personal information.

To stay scam free:

- always access our online services by typing my.gov.au or ato.gov.au into an internet browser
- never share your sign in details for ATO services with anyone
- don’t give out your TFN, date of birth or bank details unless you trust the person you are dealing with, and they genuinely require these details.

If you receive a message claiming to be from us and you don’t think it’s genuine, don't open it or reply to it. You can **verify or report a scam** and check for **scam alerts** on our website.

If you have shared information or paid a scammer money as part of an ATO impersonation scam, phone us as soon as you can on **1800 008 540**.

For information and examples of ATO impersonation scams, visit our **Scam alerts** page.

ATO announces the removal of hyperlinks in SMS

11 January 2024

The ATO is in the process of removing hyperlinks from all outbound unsolicited SMS by Tax Time 2024. Removing hyperlinks is a scams preventative measure. It will help protect the community by making it easier to identify legitimate ATO SMS interactions and provide trust and confidence in the ATO and our tax, super and registry systems.

There has been significant growth in the use of SMS by cybercriminals. Throughout the 2022–23 financial year, SMS scams impersonating the ATO brand, products, services, and our people, increased by over 400%.

Cybercriminals often use hyperlinks in targeted SMS phishing scams. The hyperlinks take individuals to highly sophisticated fraudulent websites (such as a fake myGov sign in page) designed to steal their personal information or install malware.

We may use SMS to contact you, but we will never include links to log in pages. If you want to access our online services, always type my.gov.au or ato.gov.au into your internet browser yourself.

This change also serves as a timely reminder to protect your information. Do not give out your TFN, date of birth or bank details unless you trust the person you are dealing with, and they genuinely require these details.

If you think communication such as a phone call, SMS, voicemail, email or interaction on social media claiming to be from the ATO is not genuine, do not engage with it. You should either:

- go to Verify or report a scam to see how to spot and report a scam
- phone us on **1800 008 540,** if you have divulged information or paid a scammer money.

For information and examples of ATO impersonation scams, see Scam alerts.

2022–23 Scams by numbers

12 September 2023

The number of ATO impersonation scams are higher than ever, but our 2022–23 data indicates that Australians are becoming more aware and educated about how to identify and report scams.

Last financial year our data shows:

- There were 25,609 ATO impersonation scams reported to us, an increase of over 25%.
- The amount of money paid to scammers decreased by 75%.
- Only 28 people paid money to a scammer, a 66% decrease.
- 346 people divulged personal identifying information (PII), a decrease of 71%.
- There has been a significant shift in the way scammers are contacting people – email has increased by 179% and SMS contact has increased by 414%.
- The shift toward SMS and email scams has seen an increase in targeted phishing scams, leading clients to fraudulent websites. In response, we have initiated 4,836 take downs of websites with AusCERT.
- 35–44-year olds are now the most likely to pay money to a scammer. This has shifted from the younger demographic of 25–34 year olds in the previous year.
- 25–34-year olds have remained the age group that divulged the most PII to scammers.

Note: All data comparisons are with the 2021–22 financial year.

QC 73787

Verify or report a scam

What to do if you get a phone call, text message or email that you're not sure is genuine.

Last updated 1 May 2025

Verify a scam

Scams trick you into paying money or giving out your personal information.

Scammers often pretend to be from trusted organisations like the ATO.

We will sometimes contact you by phone, email, SMS and post. If you're not sure whether it's really us, **do not** reply. You should phone us on **1800 008 540** to check.

We're recommencing the use of an external debt collection agency, recoveriescorp. If you've been referred to them, recoveriescorp may contact you by phone, email, SMS or post. If you're not sure whether it's really them, **do not** reply. Phone recoveriescorp directly on **1300 323 495** to check**.**

Report a scam

If you've been affected by an ATO impersonation scam, you can report it to us.

This information contains instructions on how to report:

- Email and SMS scams
- Phone scams
- Social media scams

Information about scams and how to report a scam is also available in **Easy Read format** and **other languages**.

Email and SMS scams

If you've received a scam email or SMS, **do not** click on any links, open any attachments or download any files. We will never send an unsolicited SMS that contains a hyperlink.

If you **did** pay money or provide sensitive personal identifying information to the scammer, phone us on **1800 008 540** to report it.

You should **also**:

- make an official report to your local police
- contact your bank or financial institution if you provided your credit card or bank details to the scammer
- contact the bank you made the payment to and lodge a fraud report.

If you **did not** pay money or provide sensitive personal identifying information to the scammer, you should still report the scam to us. You can either:

- forward the **entire email** to ReportScams@ato.gov.au
- take a screenshot of the **SMS** and email it to ReportScams@ato.gov.au

Delete the email (from your inbox, sent, and deleted items) or SMS after reporting it to us.

You can report other types of scams to Scamwatch, myGov scams or contact the Australian Cyber Security Centre to report cybercrime.

Phone scams

If you received a scam phone call and you **did** pay money or provide sensitive personal identifying information to the scammer, phone us on **1800 008 540** to report it.

You should also:

- make an official report to your local police
- contact your bank or financial institution if you provided your credit card or bank details to the scammer
- contact the bank you made the payment to and lodge a fraud report.

If you received a scam phone call and **did not** pay money or provide sensitive personal identifying information to the scammer, you should still report the scam to us. You can use our online **Report a scam** form.

Social media scams

We've recently observed several social media accounts impersonating us.

If you're approached by a social media account that is impersonating us, do not engage with it. Take a screenshot of the account or post and email it to ReportScams@ato.gov.au.

You can read more on how to identify our legitimate social media accounts.

Warning signs of tax scams

Scammers are constantly looking for new ways to trick people.

There are some common warning signs to help you check if you have been contacted by a scammer or by us:

- Emails and SMS scams
- Phone scams
- Social media scams

You can also find out about **current scams** we're aware of.

Emails and SMS scams

Some of the common features of email and SMS scams are described in the table below. Use this information to help you identify and respond to scams.

How to identify and respond to email or SMS scams

What scammers may do	Our approach
Scammers may send text messages or emails advising of suspicious activity on your account. They may ask you to provide personal information through a return SMS or email.	Where the ATO has identified suspicious activity on your account, we may place protective measures on the account to protect you. We may SMS or email you to advise that suspicious activity has been identified on your account. However, we will **never** send an unsolicited message asking you to return personal identifying information through these channels. If you're not sure whether it's really us, **do not** reply. Phone us on **1800 008 540** to check. **Protect your personal information.** **Do not** give out your tax file number (TFN), date of birth, bank details, or other personal identifying information unless you trust the person you are dealing with, and they genuinely require these details.

	Never share your myGov sign in details with anyone, including your registered tax agent.
Scammers send text messages or emails that contain a link for you to click on or a QR code to scan to log on to online services. Scammers create fake log on or sign in pages that look real. They use these sites to steal your credentials (usernames and passwords).	We will **never** send you an email or unsolicited SMS with a link or a QR code to log in to online services.
Scammers send text messages or emails that contain a link to download files or attachments. Scammers may do this to install malicious software on your computer to gain access to your data. Or they may keep your personal identifying or financial information for future misuse.	**Do not** download attachments, or click links, even if the message appears to come from us. We will **never** send you an unsolicited SMS message that contains a hyperlink.

Phone scams

Some of the common features of phone scams are described in the following table. Use this information to help you identify if a phone call claiming to be from us is a scam.

How to identify phone scams

What scammers may do	Our approach
Scammers may threaten you with immediate arrest. They do this to make you afraid or panic and stop you thinking clearly.	We will **never** threaten you with immediate arrest.

Scammers may: • demand you pay right now and keep you on the phone line until you pay • say that if you hang up there will be a warrant for your arrest. They use these threats to make you pay by the end of the call.	We will **never** demand you stay on the line until a payment is made.
Scammers may: • send unsolicited pre-recorded messages (robocalls) to your phone • leave messages on your voicemail asking you to call back.	We will **never** send unsolicited pre-recorded messages to your phone. Only **phone us** on a number you have looked up yourself. Do not call the number given to you in the call or voicemail.
Scammers may use technology to show real ATO or Australian phone numbers in the caller ID or call log.	Calls from the ATO **do not** show a number. They will show as **No Caller ID**. Only **phone us** on a number you have looked up yourself. Do not call the number shown in caller ID or in your call log.
Scammers may request that you pay a fee to receive a tax refund. They will usually ask you to pay the fee using your credit card and then steal your credit card details.	We will **never** ask you to pay a fee to receive a refund. **Do not** provide your credit card details to anyone unless you trust the person you're dealing with, and they genuinely require these details.
Scammers may request that you pay money into a personal	We will **only ever** ask you to pay a tax debt into a bank

bank account. This could be an Australian-based account established by scammers. The money moves accounts until it is sent offshore.	account held by the Reserve Bank of Australia. Check online to see that the Bank-State-Branch (BSB) number is one for the Reserve Bank of Australia. You can find out about legitimate ways to **make payments to the ATO**.
Scammers may tell you that your TFN has been cancelled or suspended due to money laundering or other criminal activity. They will say you either need to: • pay money to avoid being arrested or sent to court • transfer your money to a safe bank account to protect your TFN from future misuse.	We do not cancel TFNs. Always check that you're dealing with a legitimate agency before providing any information. If you're not sure, hang up. You can **phone us** to check. Only call us on a number you have looked up yourself. Do not call the number given to you in the call or voicemail.
Scammers may refuse to allow you to speak with a trusted adviser or your regular tax agent. They do this to prevent anyone from telling you that it's a scam and stopping you from paying.	We will **never** prevent you from discussing your tax affairs with your trusted adviser or agent.
Scammers may request payment by retail gift cards or vouchers such as iTunes or Google Play. These vouchers can be easily purchased and sold globally. They are an untraceable form of currency (money).	We will **never** request payment of a debt through iTunes, Google Play, or other vouchers. You can find out about legitimate ways to **make payments to the ATO**.

Scammers may request you pay money through offshore wire transfer (where the scammers are located).	We will **not** request payment of a debt through offshore wire transfer. You can find out about legitimate ways to **make payments to the ATO**.
Scammers may offer payment arrangements if you can't pay the full amount. This is one to increase instances of payments and the total amount paid.	Before you enter a payment arrangement, **contact us** or your tax agent using a number you have looked up yourself.
Scammers may attempt to make a conference call with a fake tax professional, law enforcement officer or another official. They do this to make the call seem real and increase your fear, but the second person will be another scammer.	We will **never** make a conference call with a third party, such as your tax agent or law enforcement. **Know your tax affairs** – you can log into ATO online services through myGov to check your tax affairs at any time. You can also contact your tax agent or the ATO.
Scammers may request payment by Bitcoin or other cryptocurrencies, either directly or deposited into an ATM. This currency is difficult to trace and offers more anonymity.	We **do not** accept payment in cryptocurrency. You can find out about legitimate ways to **make payments to the ATO**.
Scammers may request that you pay money through a cash delivery either through a courier service or made in person at a pre-determined public location.	We will **never** ask you to pay through a cash delivery.

	You can find out about legitimate ways to **make payments to the ATO**.
Scammers may request that you pay through cardless cash ATM withdrawals.	We will **never** ask you to pay a tax debt through a cardless cash ATM withdrawal. You can find out about legitimate ways to **make payments to the ATO**.

Social media scams

Some of the common features of social media tax scams are described in the table below. Use this information to help you identify and respond to scams.

How to identify and respond to social media scams

What scammers may do	Our approach
Scammers may create fake social media accounts and send requests to you asking for personal identifying information or payments. We're actively working to combat these scams as they arise.	We are on Facebook, Instagram, X and LinkedIn, but we will **never** use these social media platforms to ask you to provide personal information or documentation, or ask you to make payments. You can tell it's genuinely our Facebook (Australian Taxation Office) or Instagram (@austaxoffice) account as our pages have a blue verification tick to the right of our name. Our X account has a grey tick next to our username (@ato_gov_au). You can verify us on LinkedIn by ensuring that the account you're engaging with: • has the official ATO logo and organisational name next to the message. Beware of

	slight variations of our name, like ‘Australia’ rather than ‘Australian’ Taxation Office • has been posting on LinkedIn actively, and has been doing so for a long time • only provides you with email addresses that end with ‘.gov.au’ • doesn’t have typos or grammatical errors in its messages • has a large number of account followers. We will **never** interact with you through Whatsapp. **Never share information** such as your TFN, myGov or bank account details on social media, even through private message.
If you comment on our social media posts, scammers may respond and offer to provide support, asking you to direct message them away from our official page.	We can’t access or discuss your personal ATO account on social media. We’ll never: • send you a private or direct message • engage with you outside our official social media pages • ask you for personal identifying information such as your TFN.

QC 40945

Scam alerts

Find information and examples on the latest tax and super-related ATO impersonation scams.

Last updated 20 June 2025

Scam advice

Be wary of emails, phone calls and text messages claiming to be from the ATO.

If you think a phone call, SMS, voicemail, email or interaction on social media claiming to be from the ATO isn't genuine, don't engage with it. You should either:

- phone us on **1800 008 540**
- go to **Verify or report a scam** to see how to spot and report a scam.

Stay up to date on the latest scam alerts by **subscribing to our general email updates**. You will also receive updates on all new general content on our website.

Misinformation

Misinformation is another online risk to watch out for. It can appear on websites, social media platforms, or in messages, and often contains false or misleading claims. While it may not be a scam, misinformation can still cause harm - especially if it leads you to make decisions based on incorrect or incomplete information.

It's important to stay alert and consider the source of the information you see online. If something doesn't seem right, check it against official government websites or speak to a trusted professional.

For more details, see **Protect yourself from misinformation and disinformation**.

Latest scam alerts

These are examples of ATO, myGov and myID scams, but don't cover all scams.

- November 2024 – ATO impersonation email scam
- November 2024 – myGovID and myID scams
- March 2024 – myGov email impersonation scams

- November 2023 – Multifactor Authentication (MFA) email scam
- August 2023 – taxtime SMS and email scams
- January 2023 – ATO social media impersonation accounts scam
- July 2022 – tax refund SMS scams
- June 2022 – 2022 tax lodgment email scam
- April 2022 – fake TFN/ABN application scams
- February 2022 SMS and email scams – cryptocurrency

November 2024 – ATO impersonation email scam

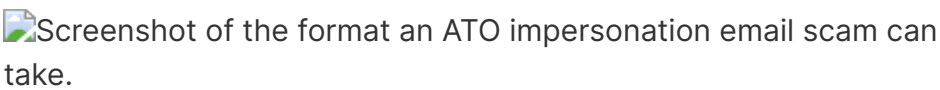
We're receiving reports of a new email scam attempting to steal **personal identifying information** by return email.

Scammers pretending to be from the 'Australian Taxation Office' or 'myGov' are emailing and falsely telling people their taxable income has been recalculated and they are due to receive compensation. To claim the amount, they are asked to reply to the email with personal identifying information such as payslips, TFN, driver's licence and Medicare details.

Scammers use this information in a variety of ways to:

- commit refund fraud in your name
- access your myGov account to steal your tax refund
- steal your superannuation
- sell your identity to organised crime groups on the dark web or via other means.

Be aware, the sender's email address looks legitimate. The following image is an example of the format this scam can take.


Screenshot of the format an ATO impersonation email scam can take.

If you receive an email like this, **do not** reply with any of your personal information.

To help protect yourself we remind you:

- We will never send an unsolicited message asking you to return personal identifying information through SMS or Email.

- Know your tax affairs – legitimate email communication from us can be located in ATO online services. You can check this by logging into your myGov account. You can also contact your tax agent or the ATO.
- 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, it is likely they are a scammer.
- Don’t click on links, open attachments or download any files from suspicious emails or SMS; we will never send an unsolicited SMS that contains a hyperlink.
- We are on Facebook, Instagram, X and LinkedIn, but we will never use these social media platforms to discuss your personal information or documentation, or ask you to make payments.

If you’re unsure if it’s really the ATO, don’t engage with them. Phone us on **1800 008 540** to check. You can report any suspicious contact claiming to be from the ATO to **ReportScams@ato.gov.au**.

November 2024 – myGovID and myID scams

We are seeing ATO impersonation scams relating to the recent name change of myGovID to myID, which occurred on 13 November.

myID is a new name and a new look – but it is used the same way as myGovID.

The community does not need to take any action, as the change has already been implemented. **You don't need to set up a new myID or reconfirm your details as part of this change. If you are asked to do this, it's a scam.**

We have communicated this change through activities (including email) to myID users.

Scammers are trying to trick the community into thinking they need to reconfirm their details via a link. The link directs users to a fraudulent myGov sign in page designed to steal personal information, including myGov sign in credentials.

These details can be used later in identity theft or other fraudulent activity such as refund fraud.

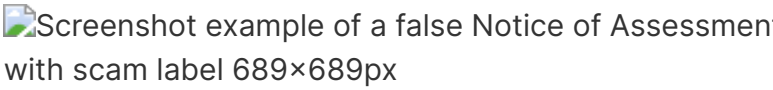
The following image is one example of the format this scam can take.

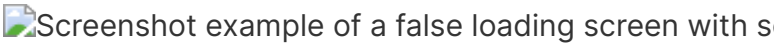

Email screenshot with red scam badge 689×400px

To protect yourself we remind you:

- We won't send you an SMS or email with a link or QR code to log on to online services. You should access them directly by typing ato.gov.au or my.gov.au into your browser.
- We will never send an unsolicited message asking you to return personal identifying information through SMS or email.
- Don’t click on links, open attachments or download any files from suspicious emails or SMS; we will never send an unsolicited SMS that contains a hyperlink.
- Only download the myID app from the official app stores (Google Play and the App Store).
- Never share your login code with anyone.

We are on Facebook, Instagram, X and LinkedIn, but we will never use these social media platforms to private message, discuss your personal information, documentation, or ask you to make payments.

The following images are examples of other myGovID scams

Screenshot example of a false Notice of Assessment QR code link with scam label 689×689px


Screenshot example of a false loading screen with scam label 689×485px


Screenshot example of scam account 689×529px

If you’re unsure whether it’s really the ATO, don’t reply. Phone us on **1800 008 540** to check.

Report any suspicious contact claiming to be from the ATO to **ReportScams@ato.gov.au**.

March 2024 – myGov email impersonation scams

The ATO and Services Australia are warning the community to stay vigilant as we continue to receive a high number of phishing scam reports that impersonate government agencies.

In February, ATO branded emails containing links to fake myGov websites were the most commonly reported scam by the community

and approximately 75% of all email scams reported to the ATO over the past 6 months have linked to a fake myGov sign in page.

Scammers use fake myGov websites to steal your sign in credentials and gain access to your myGov account. Once the scammer has access, they can make fraudulent lodgments in your name and also change bank details so that any payments are redirected to a scammers account.

Scammers use different phrases to trick people into opening these links. Some examples are:

'You are due to receive an ATO Direct refund'

‘You have a new message in your myGov inbox – click here to view”

'You need to update your details to allow your Tax return to be processed'

'We need to verify your incoming tax deposit'

'ATO Refund failed due to incorrect BSB/Account number'

‘Your income statement is ready, click on the link to view’

The following images are examples of the format this scam can take.

 Scam alert for MyGov.

 Scam alert for MyGov.

The ATO and myGov won't send you an SMS or email with a link to access online services. These should be accessed directly by typing ato.gov.au or my.gov.au into your browser.

Report any suspicious contact claiming to be from the ATO to **ReportScams@ato.gov.au**.

- You can find out more about scams impersonating myGov at my.gov.au/scams
- Scams that are not impersonating the ATO, myGov or a Services Australia brand can be reported to Scamwatch.

November 2023 – Multifactor Authentication (MFA) email scam

We’re seeing an increase in reports about an email scam impersonating the ATO.

Scammers are emailing clients advising them that due to ATO security updates, they are required to update the multifactor authentication (MFA) on their ATO account.

The scam email includes a QR code which takes you to a fake myGov sign in page, designed to steal your myGov sign in details.

The following images are examples of what the scam may look like.

The ATO will never send you an email with a QR code or a link to log in to our online services.

If you receive an email like this, don't scan the QR code, click on links, open attachments or download files. Forward the email to reportscams@ato.gov.au, and then delete it.

You can report other types of scams to Scamwatch or contact the Australian Cyber Security Centre to report cybercrime.


Scam email and myGov sign in web page.

August 2023 – taxtime SMS and email scams

This tax time, we're receiving an increased number of reports about several ATO impersonation SMS and email scams.

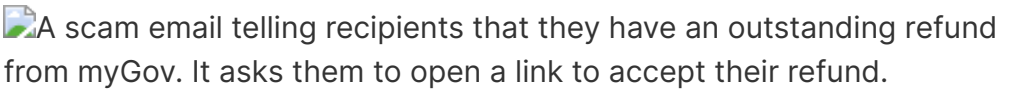
These scams encourage people to click on a link that directs them to fake myGov sign in pages designed to steal their username and password.

Scammers use many different phrases to try and trick recipients into opening these links. These include (but are not limited to):

- 'You are due to receive an ATO Direct refund'
- 'You have an ATO notification'
- 'You need to update your details to allow your Tax return to be processed'
- 'We need to verify your incoming tax deposit'
- 'ATO Refund failed due to incorrect BSB/Account number'
- 'Due to receive a refund, click here to receive a rebate'

The following images are examples of the format this scam can take.


A scam SMS asking recipients to open a link to view their processed tax return.


A scam email telling recipients that they have an outstanding refund from myGov. It asks them to open a link to accept their refund.

Don't open any links or provide the information requested.

We won't send you an SMS or email with a link to log on to online services. They should be accessed directly by typing ato.gov.au or my.gov.au into your browser.

While we may use SMS or email to ask you to contact us, we will never ask you to return personal information through these channels.

Report any suspicious contact claiming to be from the ATO to **ReportScams@ato.gov.au**.

January 2023 – ATO social media impersonation accounts scam

We're seeing an increase in fake social media accounts impersonating the ATO, our employees and senior executive staff across Facebook, Twitter, TikTok, Instagram and other platforms.

These fake accounts ask users that interact with the ATO to send them a direct message so they can help with their enquiry.

The people behind these fake accounts are trying to steal your personal information, including phone numbers, email addresses and bank account information.

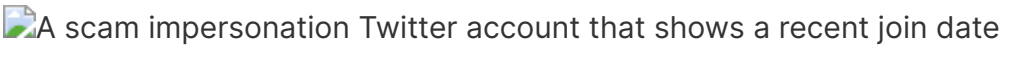
Our only official accounts are on Facebook, X, Instagram and LinkedIn.

The best way to verify that it's really the ATO is to:

- check how many people follow the account. Our verified Facebook and LinkedIn accounts have over 200,000 followers, and our Twitter account has over 65,000 followers
- check activity on the accounts. Our social media channels have been operating for around 10 years – if it's a newly created account, or only has a few posts, it's not us
- look for the grey tick next to our username (@ato_gov_au) on X (@ato_gov_au) and the blue tick next to our name (Australian Taxation Office) on Facebook (Australian Taxation Office) and Instagram (@austaxoffice)
- make sure any email addresses provided to you end with '.gov.au'.

The following images show examples of what impersonation accounts might look like.


A scam impersonation that shows a fake ATO Instagram account


A scam impersonation Twitter account that shows a recent join date and low number of followers.

If you're approached by an impersonation account, don't engage with them. Take a screenshot of the account, email the information to **reportscams@ato.gov.au** and block the account through the social media platform's reporting function.

July 2022 – tax refund SMS scams

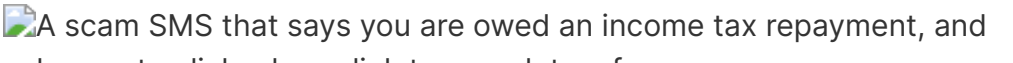
We're concerned about a high volume of SMS scams pretending to be from the ATO.

These scams tell you that you're owed an income tax repayment and ask you to click a hyperlink and complete a form.

Clicking the link takes you to a fake ATO webpage that asks for your personal identifying information, including your credit card details.

If you receive an SMS like this, don't click on any links. **Report the scam to us**.

The following image shows one example of what this scam can look like.


A scam SMS that says you are owed an income tax repayment, and asks you to click a hyperlink to complete a form

The real ATO won't send you an SMS with a link to sign in to our online services. We'll also never ask for your credit card details.

If you're ever unsure whether it's really the ATO, don't reply. Phone us on **1800 008 540** to check.

June 2022 – 2022 tax lodgment email scam

We're seeing an increase in email phishing scams claiming to be from the ATO.

These scams tell people their '2022 tax lodgment' has been received. The email asks them to open an attachment to sign a document and complete their 'to do list details'.

Opening the attachment takes you to a fake Microsoft login page designed to steal your login details. Entering your password could give the scammer access to your Microsoft account, allowing them to reset your passwords for other accounts like banking and online shopping.

If you get an email like this, don't click on any links or open any attachments. Forward the email to **reportscams@ato.gov.au**, and then delete it.

The following images are examples of the format this scam can take.

 A scam email telling recipients that their 2022 tax returns has been lodged and asking them to sign the document attached to the email.

 A fake Microsoft login screen that asks recipients to enter their account details and password.

The real ATO won't send you an email or SMS with a link to sign in to our online services.

While we may use email or SMS to ask you to contact us, we will never send an unsolicited message asking you to return personal identifying information through these channels.

Remember to **protect your passwords** and update them regularly.

April 2022 – fake TFN/ABN application scams

We're seeing an increase in scams involving fake tax file number (TFN) applications.

These scams tell people they can help them get a TFN for a fee. But instead of delivering this service, these fraudulent websites steal the person's money and personal information.

These scams are often advertised on social media platforms like Facebook, Twitter and Instagram.

Applying for a TFN is free. Find out how you can **apply for a TFN**.

If you're applying for a TFN through a tax agent, always check they are registered with the Tax Practitioners Board.

The same goes for Australian business number (ABN) applications – never give out your personal information, unless you're sure of who you're dealing with.

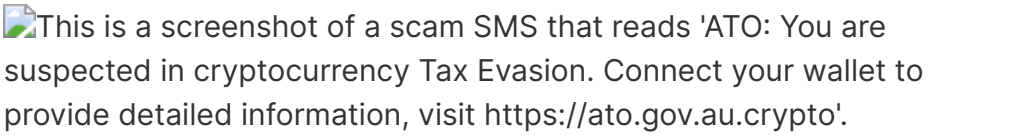
February 2022 SMS and email scams – cryptocurrency

We're receiving reports of cryptocurrency scams.

Scammers pretending to be from the ATO are telling people they are suspected of being involved in cryptocurrency tax evasion. They are then asking them to 'connect their wallet' and provide detailed information via a link.

If you receive an SMS or email like this, don't click on the link. It will take you to a fake myGov log on page, designed to steal your personal information.

The following image is one example of the format this scam can take.


This is a screenshot of a scam SMS that reads 'ATO: You are suspected in cryptocurrency Tax Evasion. Connect your wallet to provide detailed information, visit https://ato.gov.au.crypto'.

The real ATO won't send you an SMS or email with a link to sign in to our online services.

And while we may use SMS or email to ask you to contact us, we will never ask you to return personal information through these channels.

If you're ever unsure whether it's really the ATO, don't reply. Phone us on **1800 008 540** to check.

Previous scam alerts

- November 2021 phone and email scams – superannuation
- November 2021 phone scam – fake tax debt
- October 2021 email scam – update financial information
- August 2021 phone scam – new payment methods
- May 2021 email scam – update your myGovID details
- February 2021 phone scam – suspended TFN
- October 2020 email scam – JobKeeper and backing business investment claims

- September 2020 phone and SMS scams – fake tax debt
- July 2020 SMS and email scams – verify your myGov details

November 2021 phone and email scams – superannuation

We're concerned about an increase in scams involving fake superannuation investments.

Scammers are phoning and emailing people, pretending to be financial advisers or super experts. They are encouraging people to invest their super in a supposedly high performing self-managed super fund (SMSF).

These scammers will start by asking you for some information and may ask you to do a super comparison online. They are likely to be persistent and may contact you multiple times.

Sometimes, they will fraudulently use the name and Australian Financial Service Licence (AFSL) of a real business and set up a fake website to appear legitimate.

They will tell you there is no need for you to engage directly with the ATO, ASIC or any other tax or super professional.

If you agree to invest, they will transfer your super into bank accounts they control and disappear with it.

If you provide them with enough personal information (even if you don't agree to invest), they may use this to transfer your super from your existing account without you knowing. Ultimately, stealing your super savings.

Always check who you are dealing with before providing any personal or financial information.

Be cautious about anyone who contacts you with unsolicited financial advice:

1. Check ASIC's Professional registers to make sure they are licensed professionals.
2. Conduct an online search to independently verify their identity and to see if there are any reviews or indications of scam activity related to their website, email address or phone number.

3. If in doubt, check with another registered tax professional.

If you receive an SMS, email or letters from the ATO about an SMSF that you didn't establish contact us on **13 10 20** immediately.

ASIC has more information about how to recognise and report super scams.

November 2021 phone scam – fake tax debt

We're reminding people to look out for phone scams about fake tax debts.

Scammers pretending to be from the ATO are calling people and telling them they have a tax debt that they need to pay straight away.

We will use phone, email and SMS to contact you. But we will never:

- send a pre-recorded message to your phone
- threaten you with immediate arrest
- demand payment through unusual methods like gift cards or payments to personal bank accounts
- insist you stay on the line until a payment is made.

Phone calls from the real ATO will show up as 'No caller ID' on your phone.

If you're ever unsure whether it's really the ATO, don't reply. You should phone us on **1800 008 540** to check.

We have more information on how you can **identify and report tax and super scams**.

October 2021 email scam – update your financial information

We're receiving reports about a new email scam impersonating the ATO.

Scammers are sending emails telling people they will receive a tax refund. They ask them to update their financial information on an attached form to process the refund.

The following image is an example of the scam email.

 scam alert - coronavirus jobkeeper payments We are currently checking all claims made through the Coronavirus JobKeeper Payments / Backing Business Incentive Scheme. In order to complete all checks we kindly ask you to reply to this email with the following information: a clear, high-resolution photo (scane of your driver's licence (front & back); a clear, high-resolution photo (scan) of your Medicare Card (front & back).

If you receive an email like this, delete it. Don't open the attachment or click on any links.

If you receive a message from the ATO asking for your personal information, phone us on **1800 008 540** to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to **reportscams@ato.gov.au**.

You should never give out your personal information unless you are sure of who you are dealing with.

August 2021 phone scam – new payment methods

We're receiving reports of scammers demanding money by new methods.

This includes things like:

- ‘cardless cash’ ATM withdrawals
- retail gift cards, such as JB hi-fi, Myer and Woolworths
- courier services who collect the cash payments
- cash delivery made in person at a pre-determined public location.

Scammers are trying to trick people into making payments by pretending to be from the ATO and other agencies, such as the Australian Federal Police.

They might tell you that your TFN has been suspended or compromised due to money laundering or other illegal activity, or that you owe a debt.

The real ATO will never demand payment by these methods. You should always check legitimate ways to pay a tax debt on our website before making a payment.

If you have paid money to a scammer through one of these methods or are concerned about your personal safety, report it to your local police

straight away and specify all the details.

We also strongly encourage you to contact your financial institution immediately. In some cases, they may be able to stop a transaction or close your account if the scammer has your account details.

Remember, if you're ever unsure whether an ATO contact is genuine, hang up and phone us on **1800 008 540** to check.

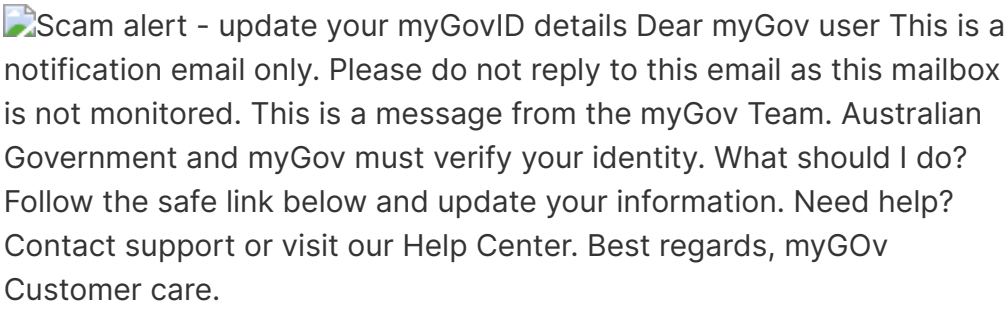
See **How to pay** for legitimate ways to pay a tax debt.

May 2021 email scam – update your myGovID details

We're receiving reports of a new email scam that asks people to update their myGov or myGovID details. As of November 2024, myGovID is now myID.

Scammers pretending to be from the 'myGov customer care team' are sending emails telling people they need to verify their identity by clicking on a link.

The following image is one example of the format this scam can take.



Don't click any links and don't provide the information requested.

The link goes to a fake myGov sign in page designed to steal your personal information, including your passport and driver's licence details.

You will get email or SMS notifications from myGov whenever there are new messages in your myGov Inbox. However, these messages won't include a link to sign in to your myGov account.

Always access our online services directly via one of the following:

- **my.gov.au**
- **ato.gov.au**

- the ATO app.

As of November 2024, myGovID is now myID. When downloading the myID app, make sure it's from either the Apple App Store or the Google Play Store.

If you receive an SMS or email that looks like it's from myGov but it contains a link or appears suspicious, you can report it to ScamWatch. If you have clicked on a link or provided your personal information, you can contact Services Australia's Scams and Identity Theft Helpdesk on **1800 941 126**.

February 2021 phone scam – suspended TFN

We are receiving increasing reports of people losing money to automated phone scams.

Scammers pretending to be from the ATO tell people their tax file number (TFN) has either been:

- suspended due to illegal activity
- compromised by a scammer.

They request the call recipient either pay a fine to release their TFN or transfer all bank funds into a holding account to protect it from future misuse.

We:

- **do not** suspend TFNs
- **will never** request you pay a fine or transfer money in order to protect your TFN pending legal action.

Phone calls from us don't show a number on caller ID. We will never send unsolicited pre-recorded messages to your phone.

If you receive a phone call like this, hang up and do not provide the information requested.

If you're unsure whether an ATO contact is genuine, phone us on **1800 008 540** to check.

An example of this type of scam is Audio recording of suspended TFN scam (MP3, 82KB)

October 2020 email scam – JobKeeper and backing business investment claims

We are receiving reports of email scams about claims for JobKeeper and Backing Business Investment.

The fake emails say we are investigating your claims. They ask you to provide valuable personal information, including copies of your driver's licence and Medicare card.

The following image is one example of an email scam currently circulating.

Don't provide the information requested, don't click on any links and delete the email straight away.

 scam alert - coronavirus jobkeeper payments We are currently checking all claims made through the Coronavirus JobKeeper Payments / Backing Business Incentive Scheme. In order to complete all checks we kindly ask you to reply to this email with the following information: a clear, high-resolution photo (scane of your driver's licence (front & back); a clear, high-resolution photo (scan) of your Medicare Card (front & back).

If you receive a message from the ATO asking for your personal information, phone us on **1800 008 540** to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to **reportscams@ato.gov.au**.

You should never give out your personal information unless you are sure of who you are dealing with.

September 2020 phone and SMS scams – fake tax debt

We are concerned about the increasing number of people paying fake tax debt scammers.

Scammers pretending to be from the ATO are contacting members of the community, telling them that they have a tax debt and that if they don't pay it straight away they will be arrested.

These scammers will often request payment through unusual methods, such as cryptocurrency, pre-paid credit cards or gift cards. They will try to keep people on the line until they have paid.

If you receive a phone call, text message or voicemail like this, don't send payment or provide any personal information. Hang up and delete the message.

We will **never**:

- threaten you with immediate arrest
- demand payment through unusual methods.

If you are not sure if it's the ATO contacting you, phone us on **1800 008 540** to check.

It's also a good idea to know your tax affairs. You can:

- log in to ATO online services through myGov to check your individual tax affairs
- log in to Online services for business to check your business tax affairs
- contact your tax or BAS agent
- contact us.

July 2020 SMS and email scams – verify your myGov details

We are receiving increasing reports of several myGov-related SMS and email scams. These scams look like they have come from a myGov or ATO email address. They also might appear in your legitimate ATO or myGov SMS message thread.

The following image is one example of an SMS scam currently circulating.

Don’t click any links and don’t provide the information requested.

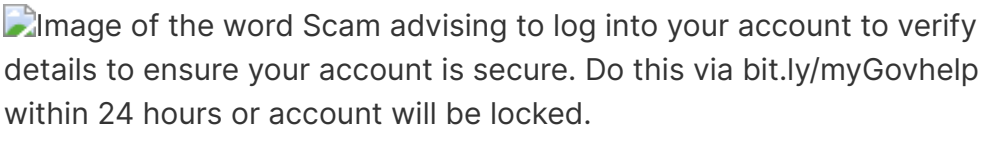


Image of the word Scam advising to log into your account to verify details to ensure your account is secure. Do this via bit.ly/myGovhelp within 24 hours or account will be locked.

You will get email or SMS notifications from myGov when there are new messages in your myGov Inbox. However, these messages won't ask you to click on a link to sign in to your myGov account.

Always access our online services directly via one of the following:

- **my.gov.au**

- **ato.gov.au**
- the ATO app.

All online management of your personal tax affairs should be done in ATO online services, accessed through your genuine myGov account.

Any communications containing your personal information, such as your tax file number (TFN), will be sent to your myGov Inbox and not your email account.

You can make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

If you receive an SMS or email from the ATO that you think is fraudulent, report it by sending an email to **reportscams@ato.gov.au**.

If you receive an SMS or email that looks like it's from myGov but it contains a link or appears suspicious, email **reportascam@servicesaustralia.gov.au**.

If you have clicked on a link or provided your personal information, phone Services Australia on **1800 941 126**.

QC 53447

Scam data

See the latest data on ATO impersonation scams.

Last updated 19 September 2025

Latest scam data

August update

In August 2025, we received **5,227** reports of ATO impersonation scams, which is a 30% decrease from July.

There were **no reports** of payments made to scammers.

Find out how to **protect your personal information** and **verify or report a scam**.

For legitimate ways to pay your tax debt, see **How to pay**.

Scam channel data

The following table provides a breakdown of scams reported to the ATO by channel used. The social media category includes scams that occur through platforms like Facebook, X, LinkedIn and WhatsApp.

The 'Other' category includes less common scam types such as physical letters and face-to-face approaches. Historically, this channel accounts for less than 0.1% of scam reports made to the ATO.

Table 1: Scam channel data – Rolling 12 months.

Month	Email	SMS	Phone	Social media	Other
August 2025	97.7%	1.5%	0.7%	0.1%	0.0%
July 2025	95.8%	3.4%	0.7%	0.1%	0.0%
June 2025	97.9%	1.1%	0.9%	0.1%	0.0%
May 2025	93.9%	5.1%	0.9%	0.1%	0.0%
April 2025	96.5%	2.8%	0.5%	0.2%	0.0%
March 2025	98.5%	1.0%	0.4%	0.1%	0.0%
February 2025	97.9%	1.7%	0.4%	0.0%	0.0%
January 2025	90.9%	8.1%	0.9%	0.1%	0.0%

December 2024	90.4%	8.9%	0.6%	0.1%	0.0%
November 2024	91.8%	7.2%	0.8%	0.2%	0.0%
October 2024	77.5%	20.8%	1.3%	0.4%	0.0%
September 2024	82.5%	15.6%	1.2%	0.7%	0.0%
August 2024	76.7%	21.7%	1.3%	0.3%	0.0%

Table 2: Scam channel data for 2025–26 financial year.

Email	SMS	Phone	Social media	Other
96.6%	2.6%	0.7%	0.1%	0.0%

QC 56423

Help for identity theft

If you know or suspect someone has stolen your tax file number or your tax-related information, contact us immediately.

Last updated 8 May 2025

If you know or suspect that someone has stolen your tax file number (TFN) or is using your tax-related information illegally, phone us on **1800 467 033** as soon as you can.

Depending on your situation, there are also other actions you can take if you suspect identity theft.

Identity theft – how to get help

Situation	What you should do
You think someone has stolen or misused your TFN, your Australian business number (ABN) or other tax-related information.	Phone us on **1800 467 033**, between 8.00 am and 6.00 pm AEST, Monday to Friday.
You think someone accessed your myGov account, including your linked ATO online services, without your permission.	Phone us on **1800 467 033**, between 8.00 am and 6.00 pm AEST, Monday to Friday.
You think someone has made fraudulent updates to your ATO record, including changing your bank account details.	Phone us on **1800 467 033**, between 8.00 am and 6.00 pm AEST, Monday to Friday.
You think someone has falsely used your personal information to set up a self-managed super fund (SMSF) under your name or made changes to your existing SMSF to gain access to your superannuation.	Phone us on **1800 467 033**, between 8.00 am and 6.00 pm AEST, Monday to Friday.

You must report all tax-related security issues to us.

You can also report:

- other cybercrime to the Australian Cyber Security Centre via the Cyber Issue Reporting System
- identity theft and fraud to your state or territory police.

Help to re-establish your tax identity

If you think someone has stolen or misused your identity, contact our Client Identity Support Centre on **1800 467 033** (between 8.00 am and 6.00 pm AEST, Monday to Friday).

We will help you establish your tax identity. When you phone us, we'll discuss the identification documents you'll need to provide.

If you think your other personal information was compromised, we recommend you contact IDCARE on **1800 595 160** (between 8.00 am and 5.00 pm AEST, Monday to Friday). IDCARE provides free advice and confidential support to victims of identity theft.

See also

- Data breach guidance for individuals

If you hold taxpayer information

If you hold tax or superannuation data (including TFNs) for clients or employees and you are aware (or suspect) the security of this information has been breached, phone our Client Identity Support Centre on **1800 467 033** between 8.00 am and 6.00 pm AEST, Monday to Friday.

See also

- Data breach guidance for businesses
- Data breach guidance for tax professionals

How we respond to identity theft

The way we respond to identity theft depends on the situation:

- Someone has your TFN
- Monitoring your tax and super account.

Someone has your TFN

If someone has your TFN, you need to tell us and we will check for any unusual or suspicious activity on your account.

If someone uses your TFN, we'll confirm and then correct the details in your account.

This may take longer for more complex tax affairs.

We will then discuss any further action taken with you.

Monitoring your tax and super account

If your ATO account has been compromised, we can help protect your tax and super account by monitoring your records before automatic processing of any lodgments or claims.

If an activity looks suspicious, we may contact you to confirm the details before processing commences.

The security measures we apply will remain on your file until we determine that there is no further risk.

Secure your sign in using myID

If you suspect someone may try and access ATO online services using your details, you can take additional steps to secure access to your personal information.

Using a Strong myID is the most secure way to access ATO online services through myGov, because:

- unlike multifactor authentication, to set up your Strong myID you need to verify your ID and complete a one-off face verification check in the app
- it sets your **online access strength** - meaning you must always use your Strong myID to access ATO online services.

This helps assure us of your identity and makes it harder for fraudsters to impersonate you.

See also

- Protect your information
- How to protect yourself
- Lost or stolen TFN
- Verify or report a scam
- Online security
- IDCARE
- Scamwatch

QC 49587

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