Print whole section

Scams, cyber safety and identity protection

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

Verify or report a scam

What to do if you get an email, SMS or phone call from the ATO that you're not sure is real.

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.

Cyber security advice

What you can do to stay safe online.

How to stay scam safe

Learn how to protect your personal information and stay safe

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.

Report a system security vulnerability

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

QC 49586

Verify or report an ATO scam

What to do if you get an email, SMS or phone call from the ATO that you're not sure is real.

Last updated 23 March 2026

Verify a scam

Scammers aim to trick you into paying money or giving out your personal information, often by pretending to be from trusted organisations like the ATO.

While we may contact you by phone, email, SMS or post, if you are not sure whether it's really us, **do not** respond. Instead, call **1800 008 540** to check.

Learn more about:

- Email scams

- SMS scams
- Phone scams
- Social media scams

You can see examples of ATO impersonation scams on our scam alerts page.

Information about scams and how to verify and report an ATO scam is also available in Easy Read format and other languages.

Email scams

Scammers may send emails claiming there is suspicious activity on your account, urging you to respond with personal details such as your TFN, bank information or login credentials. These messages often include hyperlinks, QR codes or attachments designed to steal your information or install malicious software.

Although the ATO may notify you of suspicious activity, we will never:

- send unsolicited messages containing hyperlinks or QR codes
- ask for personal identifying information via email.

If you receive an email claiming to be from the ATO, carefully check for these signs it might be a scam:

- Suspicious sender addresses – Real ATO emails always come from addresses ending in "**ato.gov.au**".
- Requests for personal information – The ATO will never ask for your TFN, bank details or myGov login via email.
- Spelling and formatting – Look for poor grammar, unusual formatting or logos that don't match official ATO branding.

For more information, see Email scams on the ScamWatch website.

Text or SMS scams

Scammers may send text messages claiming to be from the ATO, often including hyperlinks that direct you to a fraudulent website.

Sometimes the scam messages can appear in the same message chain as authentic messages from the ATO, making them more difficult

to identify.

The ATO will never:

- send an unsolicited SMS that contains a hyperlink
- ask for personal identifying information via SMS.

If you receive an SMS claiming to be from the ATO, carefully check for these signs it might be a scam:

- Unexpected messages about refunds or debts you weren't aware of.
- Links in SMS asking you to log in or provide sensitive information.
- Threats or urgency, such as "your account will be locked" or "legal action will be taken."

For more information, see Text or SMS scams on the ScamWatch website.

Phone scams

Scammers may call pretending to be from the ATO, using fear and urgency to pressure you into paying money or sharing personal information.

They may threaten you with arrest, demand immediate payment, or insist you stay on the line to prevent you from speaking with a trusted advisor. Some may also:

- send unsolicited pre-recorded voicemails (robocalls)
- make fake conference calls with impersonated tax professionals or law enforcement
- impersonate legitimate-looking caller IDs, including real ATO or Australian numbers.

The ATO will never:

- threaten you with arrest or demand you stay on the line
- send unsolicited robocalls
- ask for payment via gift cards, crypto, cash delivery or personal/offshore accounts
- threaten to cancel your TFN

- prevent you from speaking with your tax agent
- ask you to pay a fee to receive your tax refund.

Phone calls from the ATO will show as No Caller ID.

Before calling the ATO, always verify you have the correct phone number.

To check your individual tax affairs you can also use ATO online services through myGov or a registered tax agent.

For more information, see:

- Phone scams from the ScamWatch website
- How to pay the ATO.

Social media scams

Scammers may create fake ATO accounts on social media platforms and send requests to you asking for personal information or payments. They may also reply to your comments, offering to provide support and ask you to message them privately.

The ATO does not engage with the community via private or direct message.

The ATO is active on Facebook (Australian Taxation Office), Instagram (@austaxoffice), X (@ato_gov_au) and LinkedIn. However, we will never ask for personal details, documents or payments through social media.

Always check for:

- a verified indicator on our profile
- the official ATO branding
- the follower count
- any typos or unusual language.

For more information, see Social media scams on the ScamWatch website.

How to protect yourself

To help protect yourself from scams:

- Never share personal details 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.
- Avoid clicking links or downloading attachments from unexpected messages.
- Delete suspicious messages after reporting them.
- Do not interact with the scammer's messages or social media accounts.
- Remember to protect your passwords and update them regularly.

For more tips, see:

- How to stay scam safe
- Top cyber security tips for individuals
- Top cyber security tips for businesses and tax professionals.

Report a scam

If you have come across an ATO impersonation scam, it's important to report it, even if you didn't respond or lose money.

If you paid money or shared sensitive information

If you paid money or provided sensitive personal identifying information to the scammer, call the ATO immediately 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 have been the victim of cybercrime, you can report it to the Australian Cyber Security Centre.

If you did not pay money or share sensitive information

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

- **For email scams:** Forward the **entire email** to ReportScams@ato.gov.au, then delete the email from your inbox, sent, and deleted items.
- **For social media scams:** Take a screenshot of the account or post and email it to ReportScams@ato.gov.au.
- **For SMS scams:** Take a screenshot of the **SMS** and email it to ReportScams@ato.gov.au or use our online Report a scam form.
- **For phone scams:** Use our online Report a scam form.

Report a scam form

You can also report other types of scams to ScamWatch or myGov scams.

QC 40945

Scam alerts

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

Last updated 23 March 2026

Be alert

Scammers impersonate the ATO via email, SMS, phone calls, social media, and fake websites. If you're unsure it's us, don't engage.

You should:

- call **1800 008 540**
- visit Verify or report a scam.

Stay up to date on the latest scam alerts by subscribing to our email or RSS updates (select the Online services category).

Learn how to protect yourself from scams. See:

- How to stay scam safe
- Top cyber security tips for individuals
- Top cyber security tips for businesses and tax professionals.

Misinformation

Misinformation is another online risk to watch out for. It can appear in AI overviews, search results, on websites and social media platforms, or in messages. It 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 tax or super 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.

Scam alerts

These alerts show some ATO, myGov and myID scams, but they don't represent every type of scam:

- February 2026 – Cryptocurrency email scam
- October 2025 – DocuSign email scam
- November 2024 – ATO impersonation email scam
- March 2024 – myGov email impersonation scams.

February 2026 – Cryptocurrency email scam

We have received reports of a new email impersonation scam claiming you are holding cryptocurrency in a 'non-KYC decentralised wallet'. The scammers are pretending to be from the ATO or myGov and are asking people to make an immediate declaration by calling the phone number on the email to avoid further action.

Some variations may also include small attachments that should not be opened.

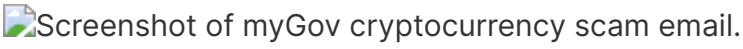
The ATO will never:

- Email you demanding immediate disclosure of cryptocurrency or other assets.
- Threaten arrest, prosecution or legal action via email or SMS.
- Request payment or personal details through unsolicited communication.

What to do if you receive this message:

- Do not respond.
- Do not call the number.
- Do not provide any information.
- Do not open attachments.
- Report the email by forwarding it to ReportScams@ato.gov.au.
- If you have shared information or engaged with the sender, phone us as soon as possible on **1800 008 540**.

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


Screenshot of myGov cryptocurrency scam email.

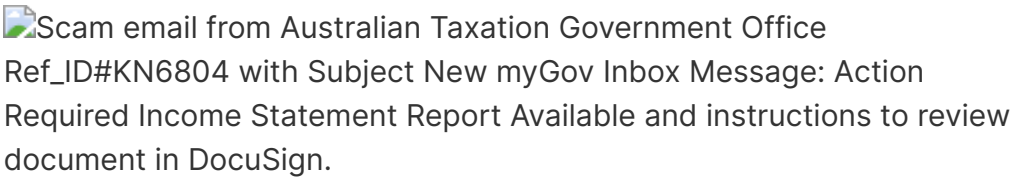
October 2025 – DocuSign email scam

We have received reports of a new ATO impersonation email scam circulating in the community. The scam advises people they have an outstanding tax-related ‘DocuSign’ that requires action.

The scam looks like a real ‘DocuSign’ email, making it appear familiar and trustworthy to recipients who have used the platform previously.

Scammers attempt to trick recipients into clicking on the Review Document button by naming the document 'Declaration and Final Release'. The email also details (often in the subject line) tax-related text such as ‘notice of assessment’. This approach falsely implies the DocuSign is from the ATO and that we are holding the recipient's tax refund until this action is completed.

The following image is an example of the scam email.


Scam email from Australian Taxation Government Office Ref_ID#KN6804 with Subject New myGov Inbox Message: Action Required Income Statement Report Available and instructions to review document in DocuSign.

If the recipient clicks on the **Review Document** button, an embedded link directs them to a fake **myGov sign in** page. This is designed to steal personal information, such as their myGov sign in credentials, name, date of birth and drivers licence details. Scammers then use this information to:

- commit refund fraud in their name
- access their myGov account to steal their tax refund
- steal their superannuation
- sell the personal identity to organised crime groups online.

The following image is an example of the fake myGov sign in page.

Sign in with myGov using your myGov sign in details screen.

The ATO will never use DocuSign to finalise a tax refund.

If you receive an email like this, report it to us by forwarding the email to ReportScams@ato.gov.au, then **delete it**.

Remember:

- We will **never** send an unsolicited message that directs you to a log in page or ask you to send 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.
- We will send legitimate email communication via ATO online services. You can check this by signing in to your myGov account. You can also contact your tax agent or us.

If someone claiming to be from the ATO contacts you and tells you are owed a refund, have a tax debt, or asks for your myGov sign in credentials, bank details or personal information such as your tax file number, it is likely a scam.

If you aren't sure if it's really the ATO contacting you, **do not engage**. Phone us on **1800 008 540** to check.

Learn more on how to protect yourself and stay scam safe.

November 2024 – ATO impersonation email scam

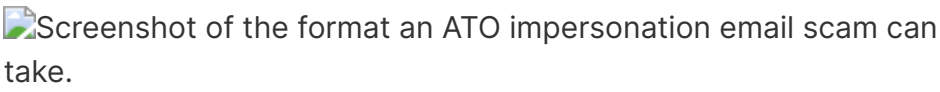
We received reports of a new email scam attempting to steal personal identifying information by return email.

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, people 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.
- 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 contact us.
- 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 details, or 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.

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. 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
- change bank details so that any payments are redirected to a scammer's 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 will **never** send you an SMS or email with a link to access online services. These services should be accessed directly by typing ato.gov.au or my.gov.au into your browser.

Report any suspicious email or SMS contact claiming to be from the ATO to ReportScams@ato.gov.au, then delete it.

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.

QC 53447

Scam data

See the latest data on ATO impersonation scams.

Last updated 24 April 2026

Latest scam data

March update

In March 2026, we received **1,461** reports of ATO impersonation scams, which is a 2% increase from February.

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

Find out how to protect your personal information and verify or report an ATO 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
March 2026	96.7%	2.3%	1.0%	0.0%	0.0%
February 2026	97.0%	0.6%	2.3%	0.1%	0.0%
January 2026	97.9%	0.7%	1.1%	0.2%	0.1%
December 2025	97.1%	1.2%	1.5%	0.2%	0.0%
November 2025	97.5%	1.4%	0.9%	0.2%	0.0%
October 2025	98.1%	1.1%	0.7%	0.1%	0.0%
September 2025	97.7%	1.0%	1.2%	0.1%	0.0%
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%

Table 2: Scam channel data for 2025–26 financial year (year-to-date)

Email	SMS	Phone	Social media	Other
97.2%	1.8%	0.9%	0.1%	0.0%

QC 56423

How to stay scam safe

Learn how to protect your personal information and stay safe from scammers.

Last updated 23 March 2026

Media: Protecting your personal information https://share.viostream.com/bi9or7ortxgn96 (**Duration:** 30 sec)

Take a sec to check

Scammers:

- aim to take advantage of weak security
- plan on you being distracted with everyday life.

To keep yourself safe:

- **Stop** – Don't share your personal information – such as your myGov sign in details, tax file number (TFN) or bank account details – with anyone unless you trust the person and they genuinely require your details.
- **Check** – Take a sec to check. Ask yourself could the message or call be fake? Is it really the ATO contacting you?
- **Protect** – Act quickly if something feels wrong or you've noticed suspicious activity on your ATO accounts.

Always be aware of what information you share. Scammers can use your personal information to access your bank account, sign into your myGov account, or steal money and commit fraud in your name.

If an interaction doesn’t feel right, don't engage. Instead:

- visit Verify or report a scam
- check our latest Scam alerts
- call us on **1800 008 540** to confirm.

If you are the victim of a data breach and your personal information has been accessed, go to Data breach guidance for individuals.

Your personal information

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

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

- passport details.

Scammers can misuse stolen personal information in many ways, such as to commit refund fraud in your name, access your myGov account, steal your superannuation or sell your identity to organised crime groups.

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 8:00 am and 6:00 pm AEST, Monday to Friday.

Consequences of identity theft

Identity theft can have long-lasting consequences that go well beyond immediate financial loss. For example, your super may be stolen or refund fraud committed in your name.

Identity theft can also lead to serious personal and professional challenges, including:

- damage to your credit rating, making it harder to get a loan or credit card
- difficulty proving your identity and replacing important identity documents
- harm to your reputation, including potential access to your social media accounts and misuse of your online presence.

Victims often spend years repairing the damage and restoring their identity.

The emotional toll is also significant. Many people experience stress, anxiety and a sense of vulnerability knowing someone else can exploit their personal information at any time.

Protect yourself

Our top tips to keep your personal information safe are:

1. Don't give out your personal information to anyone unless you trust the person and they genuinely require your details.
2. Always access online services by directly typing the URL into a browser, not by clicking on a link.

3. Protect your 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.
4. Never share your passwords – consider using passphrases instead of passwords, a password manager can help you generate or store passphrases. You should also consider updating them regularly.
5. Enable multifactor authentication – if scammers obtain your password, multi-factor authentication will make it significantly harder for them to access your account.
6. 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.
7. Use your Digital ID (such as myID), set to the strongest level you can achieve, to access ATO online services through myGov.
8. Set up Voice authentication to help us identify you and protect your tax account.

For more information about:

- myID, see How to set up myID.
- cyber security tips, visit Top cyber security tips for individuals.
- securing your devices, visit Australian Cyber Security Centre.

How we keep your information safe

We take the security and privacy of your personal information seriously. We use a range of measures to keep your data and online transactions with us safe and secure.

We protect your information by:

- confirming your details when you contact us
- using secure systems and controls
- logging access to your information so we can detect any unusual activity.

To help keep you safe online, we:

- never ask for your TFN or bank details via return email, SMS or social media
- only share your information with your consent, unless the law allows otherwise.

How we communicate with you

We may use SMS or email to ask you to contact us, but we will never send an unsolicited message with a link asking you to return personal information or log in to our online services.

We are on Facebook, Instagram and LinkedIn, but we will never use these platforms to ask you to provide personal information, documentation or ask you to make payments.

Authorised by the Australian Government, Canberra.

QC 50498

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 23 March 2026

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	Phone us on **1800 467 033**, between 8.00 am and

(ABN) or other tax-related information.	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

Authorised by the Australian Government, Canberra

QC 49587

Report a system security vulnerability

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

Last updated 1 May 2026

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 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 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.

Don't 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, email 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 **won't**:

- 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 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
- Rishaan Anand
- Quoc Bao Huynh
- Belal Eladawy
- Jamieson O'Reilly

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