

Client eBrief



Scams are on the Rise

Protect Your Information

The ATO has seen an increase in scams targeting individuals' personally identifiable information (PII).

In 2022, a person's birthdate was the most common piece of PII divulged to scammers. Nowadays, scammers are getting their hands on far more valuable information.

Last year, the ATO saw an increase in reports of scams targeting people's PII, including myGov sign-in credentials – the doorway to their ATO accounts and financial information.

PII forms pieces of a scammer's puzzle that, when completed, gives them a detailed picture of a person's identity. Scammers can then use this information to steal the person's identity and commit crimes in their name, such as tax fraud.

The Role of Your Bookkeeper

Bookkeepers play a crucial role in helping clients safeguard their PII. They educate clients on the importance of protecting personal details, and encourage verification of requests for such information. Bookkeepers protect client data by implementing secure practices like encrypted storage and access controls.

Staying informed about security threats enables bookkeepers to provide timely updates and guidance. By promoting best practices and prompt reporting of suspicious activity, bookkeepers help maintain client identity integrity and build trust through proactive management of personal information.

It is important for your bookkeeper to have a conversation with you about protecting your PII – especially your myGov credentials.

ATO Lodgement Dates

These dates are from the ATO website and do not account for possible extensions.

You remain responsible for ensuring that the necessary information is with us in time.

See [ATO Due dates by month](#) to check monthly lodgment and payment dates.

BAS/IAS Monthly Lodgements

Final dates for lodgements and payments:

June Activity Statement
21 July 2024

July Activity Statement
21 August 2024

BAS Quarterly Lodgements

Final dates for lodgements and payments:

4th Quarter 2024 Financial Year:

June Quarter 2024 (incl. PAYGI)

28 July, 2024

1st Quarter 2025 Financial Year:

September Quarter 2024 (incl. PAYGI)

28 October, 2024

When a due date falls on a Saturday, Sunday or Public Holiday*, you can lodge or pay on the next business day.

*A day that is a public holiday for the whole of any state or territory in Australia.

Due date for super guarantee contributions:

4th Quarter 2024 Financial Year:

April to June 2024 – contributions must be **in the fund** by 28 July, 2024

1st Quarter 2025 Financial Year:

July to September 2024 – contributions must be **in the fund** by 28 October, 2024

Late payments of superannuation are **not** tax deductible. If your business has overdue superannuation guarantee payments and you are unsure of how to proceed, please contact us to discuss.

Here are some key points to remember:

- **Stop** – Don't share any PII unless you trust the person you're communicating with and they have a legitimate need for your details.
- **Think** – Always consider if a message or call could be fake. Never click on hyperlinks to an online login portal from an unexpected source.
- **Protect** – If you notice any suspicious activity on your ATO accounts, contact the ATO immediately.

Your security is our priority, so please stay vigilant and protect your information. These may seem like simple steps, but following them could prevent a scammer from putting your identity together.

If you do encounter a scammer, don't engage. Report it via ReportScams@ato.gov.au or use the online form at ato.gov.au/scams.

More information and practical steps to help your clients protect their information are available at ato.gov.au/protectyourself.

Source: ATO – *Scams are on the rise. Protect client information*

From the ATO

myGov Email Impersonation Scams

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

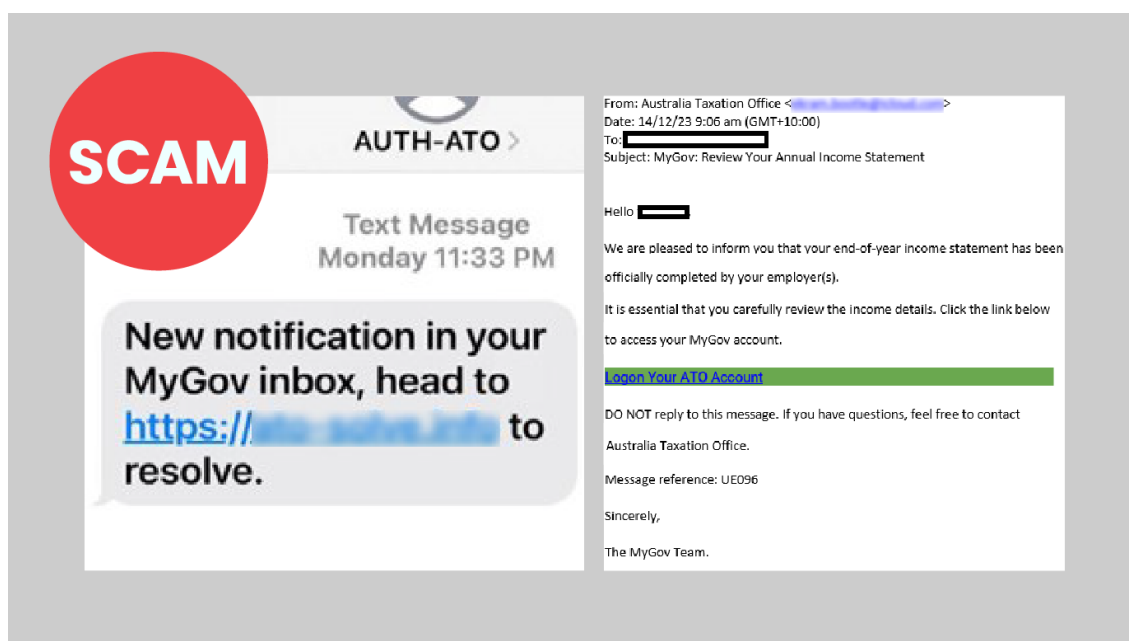
In February, ATO-branded emails containing links to fake myGov websites were the most commonly reported scam by the community, and approximately 75% of all email scams reported to the ATO over the past 6 months have linked to a fake myGov sign-in page.

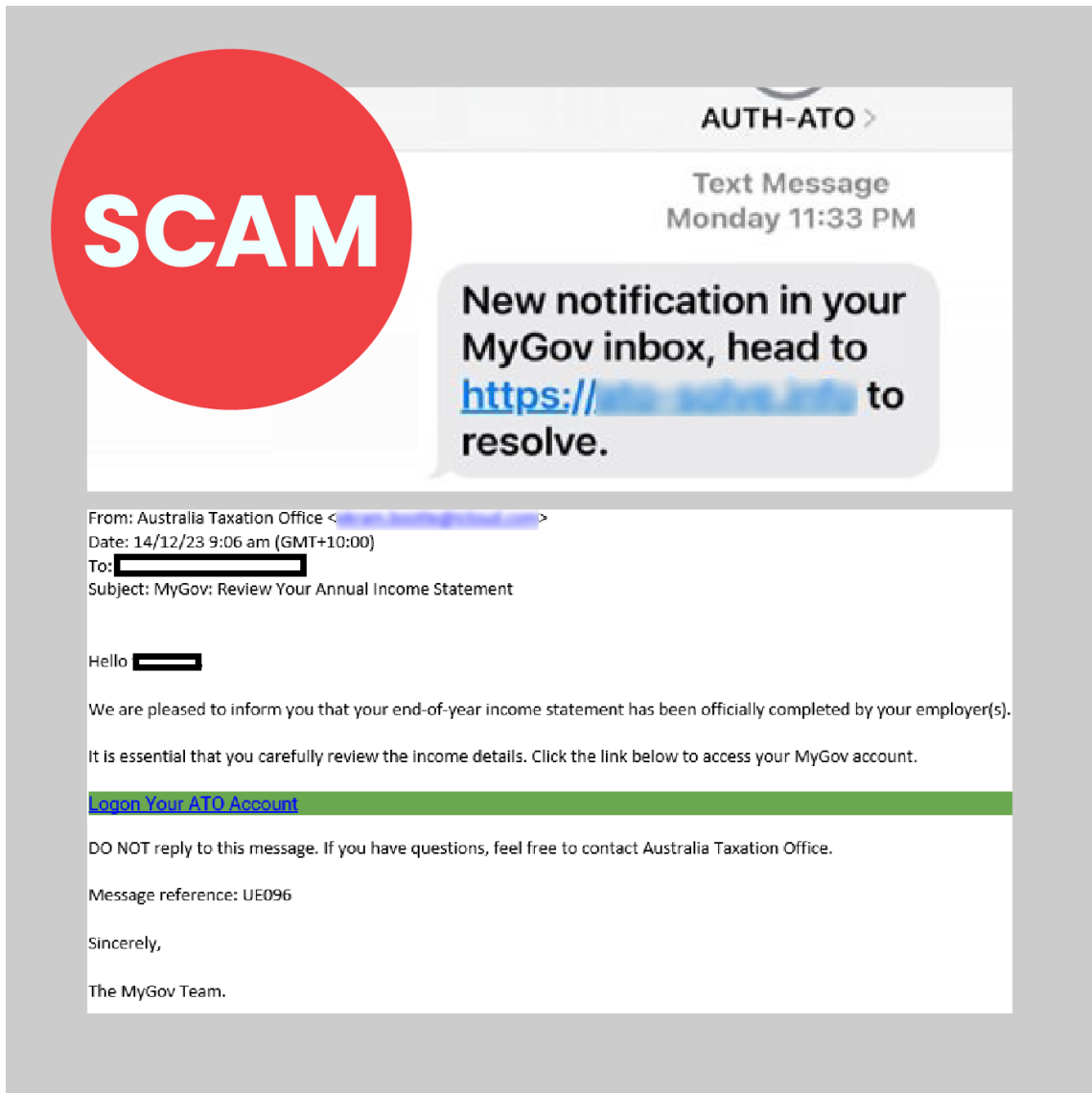
Scammers use fake myGov websites to steal your sign-in credentials and gain access to your myGov account. Once the scammer has access, they can make fraudulent lodgments in your name, and also change bank details so that any payments are redirected to a scammer's account.

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.





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 do not impersonate the ATO, myGov, or a Services Australia brand can be reported to Scamwatch.

Source: [ATO – Scam alerts](#)

Disclaimer: All or any advice contained in this newsletter is of a general nature only and may not apply to your individual business circumstances. For specific advice relating to your specific situation, please contact your accountant or contact me for further discussion.

JKM Management Services Pty Ltd

Tel: 1300 627 688

office@jkms.com.au | jkms.com.au | [Facebook](#)

This newsletter is produced by the Institute of Certified Bookkeepers and distributed by members.

