

Hank Jongen's May column – Scams

Hello everyone.

Scams are common and can affect anyone. Australians lost over \$2.18 billion to scams in 2025, according to the National Anti-Scam Centre.

Scammers may pretend to be from Services Australia (including myGov, Medicare, Centrelink or Child Support). They may try to get your personal or financial information, including your myGov sign in details. This can lead to identity theft.

Scammers keep changing their tactics. They can use new technology, including artificial intelligence, to create messages and websites that look real. This can make scams harder to spot.

What we're doing

Keeping your myGov account secure is our top priority. We use strong security controls to protect your information and we regularly improve security on the website and app. When you sign in, you can use the security review to check your settings and see steps you can take to help keep your account safe.

We also monitor scams that target customers and use controls to help protect your personal information.

You can also take simple steps to protect yourself:

- **Stop – don't share your myGov sign in details.** Treat them like your banking PIN.
- **Check – use the official myGov app or website.** If we need to contact you, we'll usually send a message to your myGov Inbox. Open the myGov app, or type my.gov.au into your browser, then sign in and check your Inbox. If you use the myGov app, you can opt to have push notifications instead of text message alerts.
- **Protect – use a more secure way to sign in,** such as a passkey or Digital ID. Passkeys use your device's security features, like a fingerprint, face recognition or PIN.

Signs of a scam

There are some signs you can look out for to help you spot a possible scam. These include:

- Unexpected messages or calls
- Urgency or pressure to act quickly
- Promises of money or threats, like fines or jail.

Remember: **we will not ask you to:**

- click a link to sign in to your myGov account
- pay us money to get a payment or benefit, or help from our staff
- give us remote access to your computer or device
- reply by email or text message to any electronic message we send you.

If you're not sure if information you've seen online about government payments or services is real, visit our genuine websites, **servicesaustralia.gov.au** and **my.gov.au** to learn more.

What to do if you think you've been scammed

If you think you've been scammed, call our Scams and Identity Theft Helpdesk on **1800 941 126**. Also call if you've shared your myGov sign-in details or other personal information. If you haven't been scammed but you've seen a Services Australia or myGov scam, report it to us.

Email details of the scam (and a screenshot, if you can) to reportascam@servicesaustralia.gov.au.

Until next time.

Hank Jongen
General Manager
Services Australia