How to stay safe online

- **Don't click on any links or attachments** in text messages or emails pretending to be from myGov or Services Australia.
- **Secure your personal information** by only sharing information that you need to.
- Use a **unique strong password or passphrase** for every account.
- **Turn on multifactor authentication** if it's an option.
- **Check the website you're using is genuine.**
- **Use secure Wi-Fi networks** and always log off and close your browser tabs when you finish.
- Be careful what you **share about yourself online**.
- **Do your own search** for websites and phone numbers.

Secure your myGov account

Increase the security of your myGov account by using a passkey or your Digital ID as your sign in option.

Passkey	Digital ID
Uses the security features on your device to sign in, including: • fingerprint or facial recognition • a PIN or swipe pattern • security key.	Verify your identity documents to create your Digital ID. Then, enter a verification code in your Digital ID app to sign in. This is protected by the security features on your device, including: • fingerprint • facial recognition.

These sign in options offer a **higher level of protection** against scammers when you turn off your password.

For more information about myGov sign in options, go to **my.gov.au/sign-in**

Help us stop scams

If you see a **myGov**, **Medicare**, **Centrelink** or **Child Support** scam, email us at **reportascam@servicesaustralia.gov.au**

This helps us protect others from scams.

You can also help others by reporting scams at **scamwatch.gov.au**

Help if you've been scammed

If you've given your myGov sign in details or other personal information to someone you don't know, we can help you.

Call our **Scams and Identity Theft Helpdesk** on **1800 941 126**. The Helpdesk is open from **Monday to Friday**, **8 am to 5 pm**.

If you need help in your language, ask us for an interpreter. If you're deaf or have a speech impairment, call the **National Relay Service** on **1800 555 660**.

Help in your language

We have information about scams and identity theft in different languages.

You can find our Beware of scams factsheet and our What is a phishing scams? video by going to **servicesaustralia.gov.au/yourlanguage**

Help for your community

We have resources to help you educate and support people in your community about scams and identity theft.

Go to **servicesaustralia.gov.au/scamresources** and download our resource kit.

14484.2505

Australian Government

Services Australia

Scam?

Stop. Check. Protect.

If you think it's suspicious:

Don't click Don't reply Report it

What is a scam?

A scam is when someone tries to trick you into giving them your money or personal information by pretending to be someone else.

There are signs that can tell you if something is a scam:

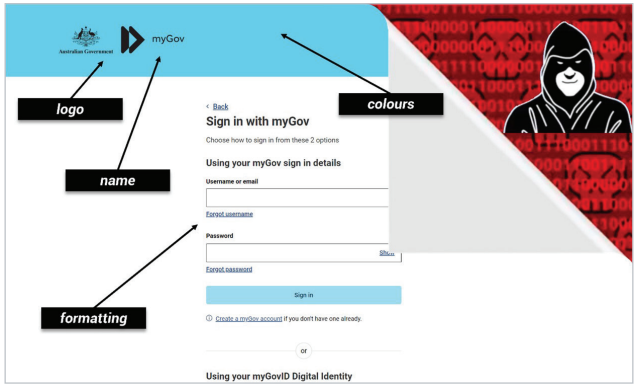
- an unexpected message, email or phone call
- includes a link or attachment
- asks you to act quickly
- offers money or makes a threat.

What is a phishing scam?

A phishing scam is a fake message designed to steal your personal information and money.

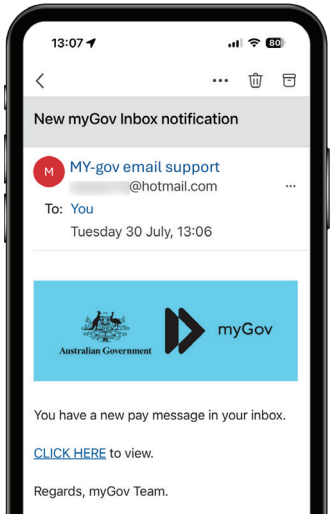
Scammers send texts, emails and social media messages pretending to be from the government and well known brands to trick you into giving them your information.

They include links that go to fake websites so they can steal your personal information. Scammers make these websites look real so you don't suspect anything is wrong.



Examples of common scams

Our website has information and real examples about **active scams** that target our customers. These scams pretend to be from myGov, Services Australia, Medicare and Centrelink.



We won't send you links in text messages or emails asking you to sign in or share your personal information.

What we won't do

- send links in text messages or emails asking you to sign in or share your personal information
- ask for your personal information through text messages, emails or social media
- contact you and ask for your myGov details
- ask you to private chat on social media
- ask you to pay for our services or to fix an issue
- ask for remote access to your device.

What we will do

- ask you to go to **my.gov.au** or the **official myGov app** to check for messages about your payments
- send you a message to **confirm updates to your personal details**
- remind you about obligations, such as **upcoming appointments** or **changes to your reporting date**
- call from a **private phone number**
- recommend you **call or visit us in person** if you're having difficulty online
- **ask you not to share personal details** on our social media accounts.