



Beware of scams

Scammers often pretend to be from trusted organisations, like Services Australia.

They may trick you into giving away money or information in return for payments, services and help.

If a scammer gets your information, they can:

- access your bank account and transfer money from it
- use your name to set up a phone plan and other contracts
- steal your superannuation
- access your email and social media accounts
- pretend to be you.

If you lose money because of a scam, you may not get it back.

Information scammers want

Scammers may try to get your:

- full name
- date of birth
- address
- Medicare card details
- Centrelink Customer Reference Number (CRN)
- identity documents
- myGov sign in details or linking codes
- bank details
- passwords.

How to protect yourself

To protect your information:

- know how to identify a scam
- be careful when someone unexpectedly contacts you, especially if they have an urgent deadline
- never tell anyone your linking codes, passwords or answers to your secret questions
- do not let others use or see your myGov, or other online accounts
- use a password that is easy for you to remember, but hard for others to guess
- protect your mobile device by locking it when you are not using it
- secure your mail by having a lock on your letterbox and redirecting your mail if you move.

How to tell if it is a scam

You can identify a scam by knowing what we do and what we do not do.

Things we do

We may send you an email or text message. Our messages will not include your name or contact details, but may:

- ask you to book, or remind you about, an appointment
- tell you about your payments
- confirm when you have changed your details
- tell you if you have a new message in your myGov Inbox.

If you owe us money, we will send you a letter.

We may call you, but be careful if you are not expecting a phone call from us. You should ask for the caller's name and contact details. If you do not think the caller is us, hang up and call back on one of our payment lines.

Things we do not do

We will **never** ask you to:

- tell us your password or Personal Identification Number (PIN)
- pay us to help you
- send or transfer money to us to get a payment
- buy gift cards or vouchers
- click on links or open attachments in emails or text messages
- give us your personal details on social media, like Facebook or Twitter
- give us access to your computer or personal devices.

We also do not work with other companies to give you special deals.

What to do if you have been scammed

If you have lost money or given away personal information, you should:

- keep a record of what happened
- call our Scams and Identity Theft Helpdesk straight away on **1800 941 126**. Let us know if you need an interpreter and we will arrange one for free.
- report the incident in English at [scamwatch.gov.au](https://www.scamwatch.gov.au)

Where to get more information

- call **131 202** to speak with us in your language about Centrelink payments and services
- call the Translating and Interpreting Service (TIS National) on **131 450** to speak with us in your language about Medicare and Child Support payments and services

- go to servicesaustralia.gov.au/yourlanguage where you can read, listen to or watch information in your language
- go to servicesaustralia.gov.au/scams for more information in English
- visit a service centre.

Note: calls from your home phone to '13' numbers from anywhere in Australia are charged at a fixed rate. That rate may vary from the price of a local call and may also vary between telephone service providers. Calls to '1800' numbers from your home phone are free. Calls from public and mobile phones may be timed and charged at a higher rate.

Disclaimer

The information contained in this publication is intended only as a guide to payments and services. It's your responsibility to decide if you wish to apply for a payment and to make an application with regard to your particular circumstances.