

[Home](#) >

Scam Alert – Fake myGov email and SMS scam

13 January 2023



Be wary of emails and SMS claiming to be from myGov suggesting you are owed a refund. It may be a scam!

The ACMA is aware of increasing reports of myGov impersonation email and SMS scams. These scams try to get you to click on a malicious link or visit a fake website in order to receive a repayment or refund, such as a tax refund. Other examples may ask you to update your personal details via a link or attachment.

These messages will also often reference other government agencies or services, such as the Australian Taxation Office (ATO) or programs like Medicare. They may also use government logos to make the message look legitimate.

Do not click on any links or open any attachments in these messages. They are phishing scams

designed to steal your personal or financial details.

myGov will never send you an email or SMS with a link. If in doubt, type my.gov.au [↗](#) into your browser and sign into your myGov account or contact Services Australia directly. Do not rely on the contact information in the email or SMS if you think it's a scam.

You can find more [information](#) [↗](#) about how to identify and avoid these scams via the myGov website. Services Australia also provides [advice](#) [↗](#) to consumers on these and other similar scams on its website.

If you're concerned that you may have given your myGov and other personal information to a scammer, contact the Services Australia Scams and Identity Helpdesk on 1800 941 126.

Scammers target everyone. Learn more about how to protect yourself from phone scams on the [ACMA website](#) and make a report to [Scamwatch](#) [↗](#).