16 July 2020

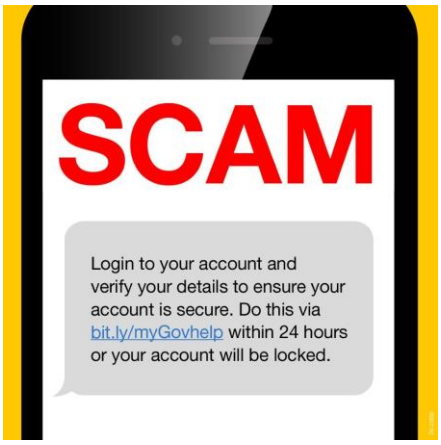
Dear ACSC Alert Service subscriber

What's happened?

The Australian Taxation Office (ATO) is receiving increased reports of several myGov-related SMS and email scams.

At this time of year, when people expect some form of interaction with the ATO during tax time, be aware that cybercriminals take advantage by pretending to be the ATO or myGov. These scams look like they've come from a myGov or ATO email address and they ask you to click on a link to verify your details.

To make them seem more legitimate, cybercriminals use technology that causes these messages to appear in the same conversation thread as genuine messages from myGov or ATO addresses. The image below is an example of this scam message.



If clicked on, the hyperlink takes you to a fake website that asks you to provide your details and other personal information for 'verification purposes'.

As always our advice is DON'T click any links and DON'T provide the information requested.

Does it affect me?

These SMS and email scams are widely circulating around Australia, so anyone can receive them.

Protect yourself and others from these scams

If you receive one of these scam texts or emails, do not click on the links and do not provide the information requested.

- Know that the ATO will never send an email or SMS asking you to access online services via a URL.
- Sign into your myGov account at my.gov.au to check the status of your online tax affairs at any time.
- For added security on your myGov account, turn on two-factor authentication (2FA). For example, opting to receive a security code via SMS when you log into your myGov account.
- To set up your security code, sign in to your myGov account and turn it on in 'Account settings'.
- If you receive an SMS or email that looks like it's from myGov but it contains a link or appears suspicious, email reportascam@servicesaustralia.gov.au.
- If you have clicked on a link or provided your personal information, contact Services Australia on 1800 941 126.

Where possible, hover over web links without clicking on them to check where the link will take you – if it looks like it will take you away from the platform's official website, don't click on it.

More information

The ACSC's Stay Smart Online program has more advice on how to protect yourself from tax related scams.

To stay up to date on the latest online threats and how to respond, sign up to the ACSC's Alert Service and follow us on Facebook.

Our Alert Service has a new look and is now called the 'ACSC alert service.'

You'll notice from now on you are receiving our alerts from our new email address alerts.staysmartonline@contact.cyber.gov.au (instead of alerts@staysmartonline.gov.au).

If you've been the victim of a cybercrime including financial loss, identity theft or compromised personal details, report it to ReportCyber at www.cyber.gov.au/report.

CONTACT US
Facebook: www.facebook.com/staysmartonline
Email: staysmart.online@defence.gov.au
Web: www.cyber.gov.au