Factor
Accountants & Advisers

How to identify an ATO Scam

This document is intended to help you avoid ATO scams.
More information can be found on ATO's website:
ato.gov.au/scams

WHAT IS A SCAM?

A scam is a trick to get you to:

- pay money, or
- disclose information about yourself that helps scammers pretend to be you.

A scammer is someone who lies and tries to scam people. They might say they work at the ATO or other institutions in order to carry out their scam.

You should only give your personal information about yourself, like your tax file number and bank details, to people you can trust.

WHAT DO SCAMMERS DO?

A scammer can contact you by

- phone
- email
- text message

A scammer might ask for

- information about you
- your bank account or credit card number
- money

A scammer might say you will get a payment from the ATO, like a

- refund or bonus on your tax return
- JobKeeper payment
- Super payment

Be careful, it might be a scam.

THINGS THAT ATO WILL NEVER DO

- send you an email or text message asking you to send us your information by email or text message

- send you an email or text message with a link to log into online services

- send a pre-recorded message saying the police are coming to arrest you or demanding urgent payment of money

- ask for payment by
  - bank transfers to a bank that is not the Reserve Bank of Australia
  - overseas wire transfers
  - iTunes or Google Play cards
  - cardless cash transfers
  - cryptocurrency like Bitcoin.

WHAT A SCAMMER MIGHT DO

A scammer might:

- tell you to send information about yourself by email or text message
- ask you to click on a link in an email or text message to log on to online services
- say the police are coming to arrest you.

WHAT YOU SHOULD DO

If you get a phone call:

- hang up on any one who says they are from the ATO and threatens to arrest you
- delete all pre-recorded messages saying they are from the ATO. Do not phone them back.

If you get an email or text message:

- think carefully before responding to any email or text message from the ATO
- ask someone you trust if it looks real or phone us on 1800 008 540 to check
- don't click on any links asking you to log on to an online service with your user name and password
- check **ato.gov.au/scams**

USING ATO'S ONLINE SERVICES

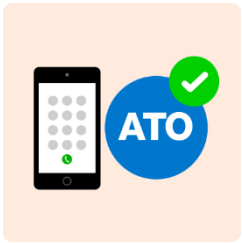
If you need to log into ATO's online services you should always go to my.gov.au

You can keep your myGov account safe by setting up myGov security codes.

This means when you try to log into myGov you will get a text message with a security code.

To set up myGov security codes, sign in to your myGov account and turn them on in Account settings.

HOW TO GET HELP



To report a scam, call the ATO on

1800 008 540

You can forward a scam email to

ReportEmailFraud@ato.gov.au