



**Australian Government**

**Australian Taxation Office**

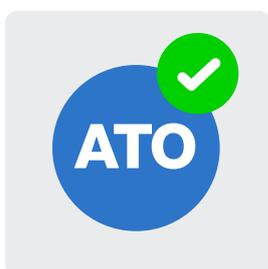
# Is it a scam?



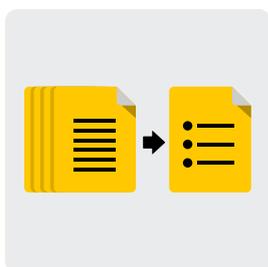
**Easy read**

# How to use this document

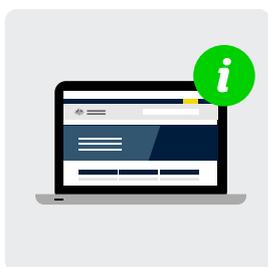
**This information is written in a way that is easy to read.  
We use pictures to explain some ideas.**



This document has been written by the Australian Tax Office or ATO. When you see the word 'we' it means the ATO.



This Easy Read document is a summary of another document.



You can find the longer document on our website at [ato.gov.au/scams](https://ato.gov.au/scams)

# What is a scam?

A scam is a trick to get you to



- pay money
- share information about yourself that helps someone pretend to be you.



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



People who scam are called scammers. Scammers lie. They might say they work at the ATO.

# What do scammers do?

A scammer can contact you by

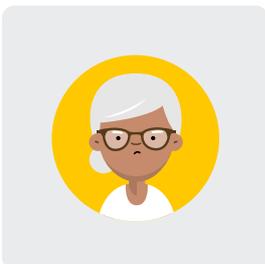


- phone
- email
- text message
- social media.

A scammer might ask for



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



A scammer might say things to make you anxious or afraid of getting in trouble.

# What do scammers do?



They might say you have to act quickly. This is so you don't have time to stop and think clearly.



A scammer on social media might ask you to private message their account so that they can help you with your tax or super.

# Things we will never do

We will never



- send you an email, text message or post on social media asking you to reply with your information



- send you an email, text message or post on social media 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

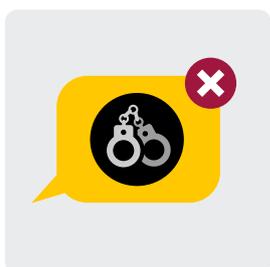
# Things we will never do



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

# A scammer might

A scammer might



- say the police are coming to arrest you

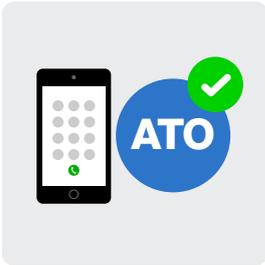


- tell you to send information about yourself by email, or text message or social media



- ask you to click on a link in an email, text message or social media post to log on to online services.

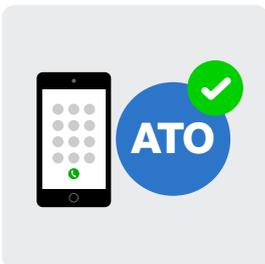
# What you should do



Phone calls from the real ATO will show as 'No caller ID' on your mobile phone.



Hang up on any one who says they are from the ATO and threatens to arrest you.



You can phone us on **1800 008 540** to check if we needed to speak to you.



Delete all pre-recorded messages saying they are from the ATO. Do not phone them back.

# What you should do

If you get an email or text message from the ATO



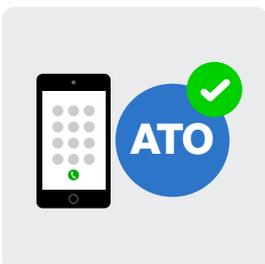
- think carefully before responding to it



- don't click on any links asking you to log on to an online service with your user name and password



- ask someone you trust if it looks real



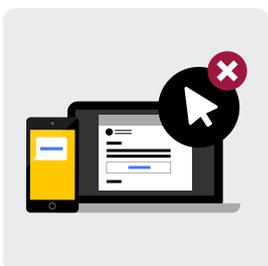
- phone us on **1800 008 540** to check

# What you should do



- check [ato.gov.au/scams](https://ato.gov.au/scams)

If you see a social media account or post from us or an ATO staff member that looks strange

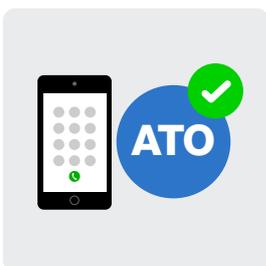


- do not respond to it with any of your personal information

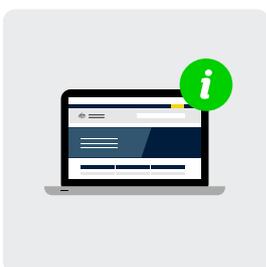


- do not click on any links

# What you should do



- phone us on **1800 008 540** to check if it is really us talking to you

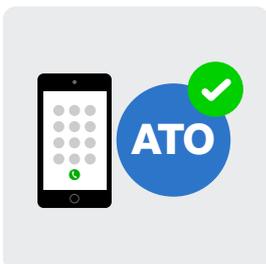


- check [ato.gov.au/scams](https://ato.gov.au/scams)



- If you think an ATO social media account is fake you should block it.

# How to get help



To tell us about a scam phone us on  
**1800 008 540.**



You can forward a scam email to  
[ReportScams@ato.gov.au](mailto:ReportScams@ato.gov.au)



You can take a screenshot of fake social  
media posts and email them to  
[ReportScams@ato.gov.au](mailto:ReportScams@ato.gov.au)