Scam alerts

This page provides examples of recent ATO impersonation scams.

If you think a phone call, SMS, voicemail or email claiming to be from us is not genuine, do not reply to it. Instead, you should either:

- phone us on **1800 008 540**
- go to Verify or report a scam (/General/Online-services/Identity-security-and-scams/Verify-or-report-a-scam/?=QC53447_Link1) – to see how to spot and report a scam.

Stay up to date on the latest scam alerts by subscribing to our general email updates (/Subscription.aspx). You will also receive updates on all new general content on our website.

On this page

Latest scam alerts

- November 2021 phone and email scams – superannuation
- November 2021 phone scam – fake tax debt
- October 2021 email scam – update your financial information
- August 2021 phone scam – new payment methods
- May 2021 email scam – update your myGovID details
- February 2021 phone scam – suspended TFN

November 2021 phone and email scams – superannuation

We're concerned about an increase in scams involving fake superannuation investments.

Scammers are phoning and emailing people, pretending to be financial advisers or super experts. They are encouraging people to invest their super in a supposedly high performing self-managed super fund (SMSF).

These scammers will start by asking you for some information and may ask you to do a super comparison online. They are likely to be persistent and may contact you multiple times.

Sometimes, they will fraudulently use the name and Australian Financial Service Licence (AFSL) of a real business and set up a fake website to appear legitimate.

They will tell you there is no need for you to engage directly with the ATO, ASIC or any other tax or super professional.

If you agree to invest, they will transfer your super into bank accounts they control and disappear with it.

Even if you don't agree to invest, if you provide them with enough personal information they may use this to transfer your super from your existing account without you knowing, ultimately stealing your super savings.

Always check who you are dealing with before providing any personal or financial information.

Be cautious about anyone who contacts you with unsolicited financial advice:

- Check ASIC's Professional registers (https://asic.gov.au/online-services/search-asic-s-registers/professional-registers/) to make sure they are licensed professionals.
- Conduct an online search to independently verify their identity and to see if there are any reviews or indications of scam activity related to their website, email address or phone number.
- If in doubt check with another registered tax professional.

If you receive an SMS, email or letters from the ATO about an SMSF that you did not establish contact us on **13 10 20** immediately.

ASIC has more information about how to recognise and report super scams (https://moneysmart.gov.au/how-super-works/superannuation-scams) .

November 2021 phone scam – fake tax debt

We're reminding people to look out for phone scams about fake tax debts.

Scammers pretending to be from the ATO are calling people and telling them they have a tax debt that they need to pay straight away.

We will use phone, email and SMS to contact you. But we will never:

- send a pre-recorded message to your phone
- threaten you with immediate arrest
- demand payment through unusual methods like gift cards or payments to personal bank accounts
- insist you stay on the line until a payment is made.

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

If you're ever unsure whether it's really the ATO, do not reply. You should phone us on **1800 008 540** to check.

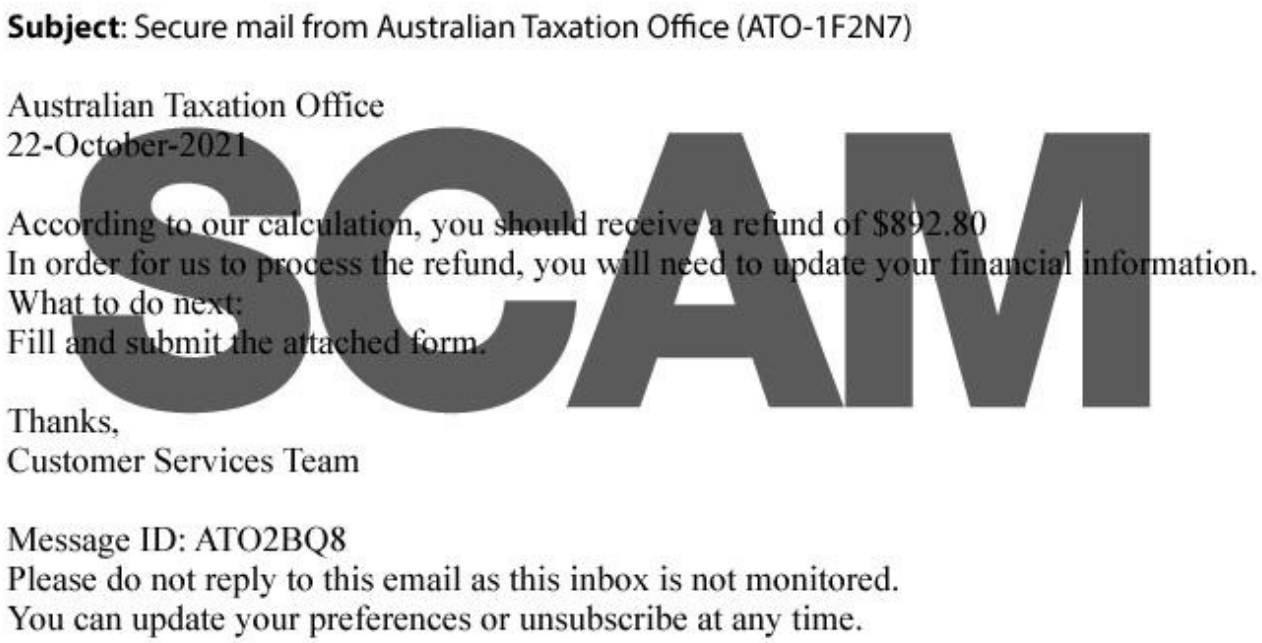
We have more information on how you can identify and report tax and super scams (/General/Online-services/Identity-security-and-scams/Verify-or-report-a-scam/).

October 2021 email scam – update your financial information

We're receiving reports about a new email scam impersonating the ATO.

Scammers are sending emails telling people they will receive a tax refund. They ask them to update their financial information on an attached form to process the refund.

The image below is an example of the scam email.



If you receive an email like this, delete it. Don't open the attachment or click on any links.

If you receive a message from the ATO asking for your personal information, phone us on **1800 008 540** to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to reportemailfraud@ato.gov.au (mailto:reportemailfraud@ato.gov.au).

You should never give out your personal information unless you are sure of who you are dealing with.

August 2021 phone scam – new payment methods

We're receiving reports of scammers demanding money by new methods.

This includes things like:

- ‘cardless cash’ ATM withdrawals
- retail gift cards, such as JB hi-fi, Myer and Woolworths
- courier services who collect the cash payments
- cash delivery made in person at a pre-determined public location.

Scammers are trying to trick people into making payments by pretending to be from the ATO and other agencies, such as the Australian Federal Police.

They might tell you that your TFN has been suspended or compromised due to money laundering or other illegal activity, or that you owe a debt.

The real ATO will never demand payment by these methods. You should always check legitimate ways to pay a tax debt on our website before making a payment.

If you have paid money to a scammer through one of the methods listed above or are concerned about your personal safety, report it to your local police straight away and specify all the details.

We also strongly encourage you to contact your financial institution immediately. In some cases, they may be able to stop a transaction or close your account if the scammer has your account details.

And remember, if you're ever unsure whether an ATO contact is genuine, hang up and phone us on **1800 008 540** to check.

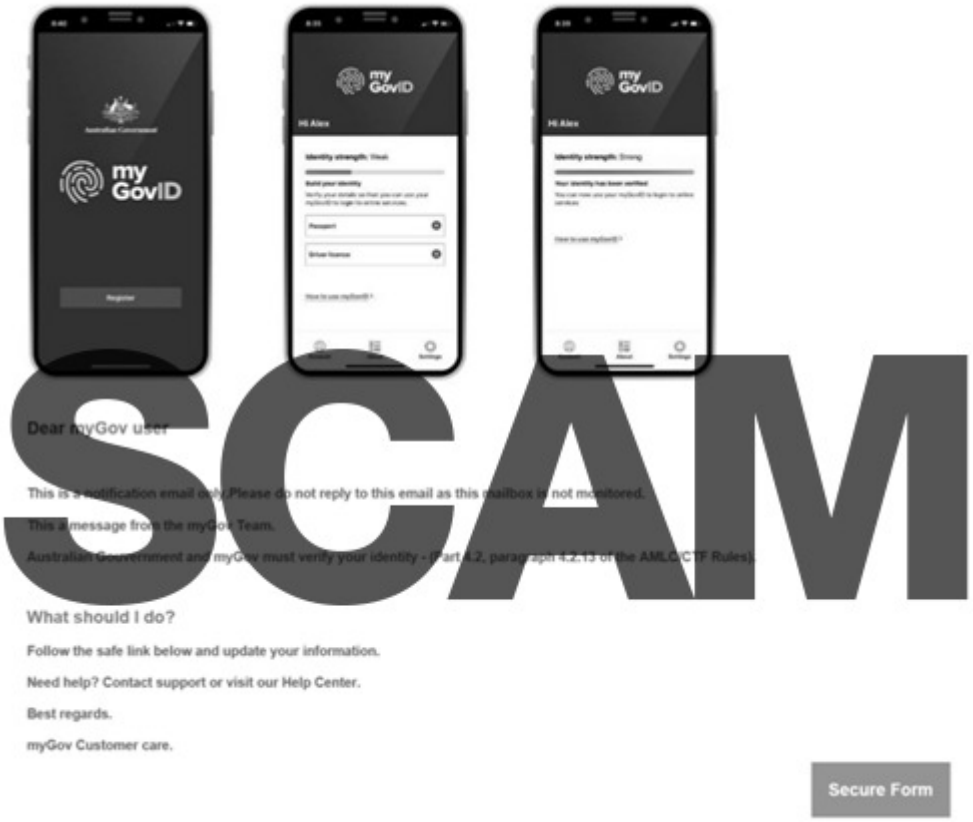
See How to pay (/General/Paying-the-ATO/How-to-pay/) for legitimate ways to pay a tax debt.

May 2021 email scam – update your myGovID details

We're receiving reports of a new email scam that asks people to update their myGov or myGovID details.

Scammers pretending to be from the 'myGov customer care team' are sending emails telling people they need to verify their identity by clicking on a link.

The image below is one example of the format this scam can take.



Don’t click any links and don’t provide the information requested.

The link goes to a fake myGov logon page designed to steal your personal information, including your passport and driver’s licence details.

You will get email or SMS notifications from myGov whenever there are new messages in your myGov Inbox. However, these messages will never include a link to log on to your myGov account. Always access our online services directly via one of the following:

- **my.gov.au**
- **ato.gov.au**
- the ATO app (/General/Online-services/ATO-app/).

When downloading the myGovID app, make sure it's from either the Apple App Store or the Google Play Store.

If you receive an SMS or email that looks like it’s from myGov, but it contains a link or appears suspicious, you can report it to ScamWatch. If you have clicked on a link or provided your personal information, you can contact Services Australia’s Scams and Identity Theft Helpdesk on **1800 941 126**.

February 2021 phone scam – suspended TFN

We are receiving increasing reports of people losing money to automated phone scams.

Scammers pretending to be from the ATO tell people their tax file number (TFN) has either been:

- suspended due to illegal activity
- compromised by a scammer.

They request the call recipient either pay a fine to release their TFN or transfer all bank funds into a holding account to protect it from future misuse.

We:

- **do not** suspend TFNs
- **will never** request you pay a fine or transfer money in order to protect your TFN pending legal action.

Phone calls from us do not show a number on caller ID. We will never send unsolicited pre-recorded messages to your phone.

If you receive a phone call like this, hang up and do not provide the information requested.

If you're unsure whether an ATO contact is genuine, phone us on **1800 008 540** to check.

An example of this type of scam is available below:

- Audio recording of suspended TFN scam (MP3, 82KB) (/uploadedFiles/Content/CR/downloads/Media_centre/30095054.MP3)

Previous scam alerts

- October 2020 email scam – JobKeeper and backing business investment claims
- September 2020 phone and SMS scams – fake tax debt
- July 2020 SMS and email scams– verify your myGov details
- June 2020 phone scam – threatening arrest and requesting personal details
- May 2020 phone scam – requesting bank account details for the JobKeeper payment

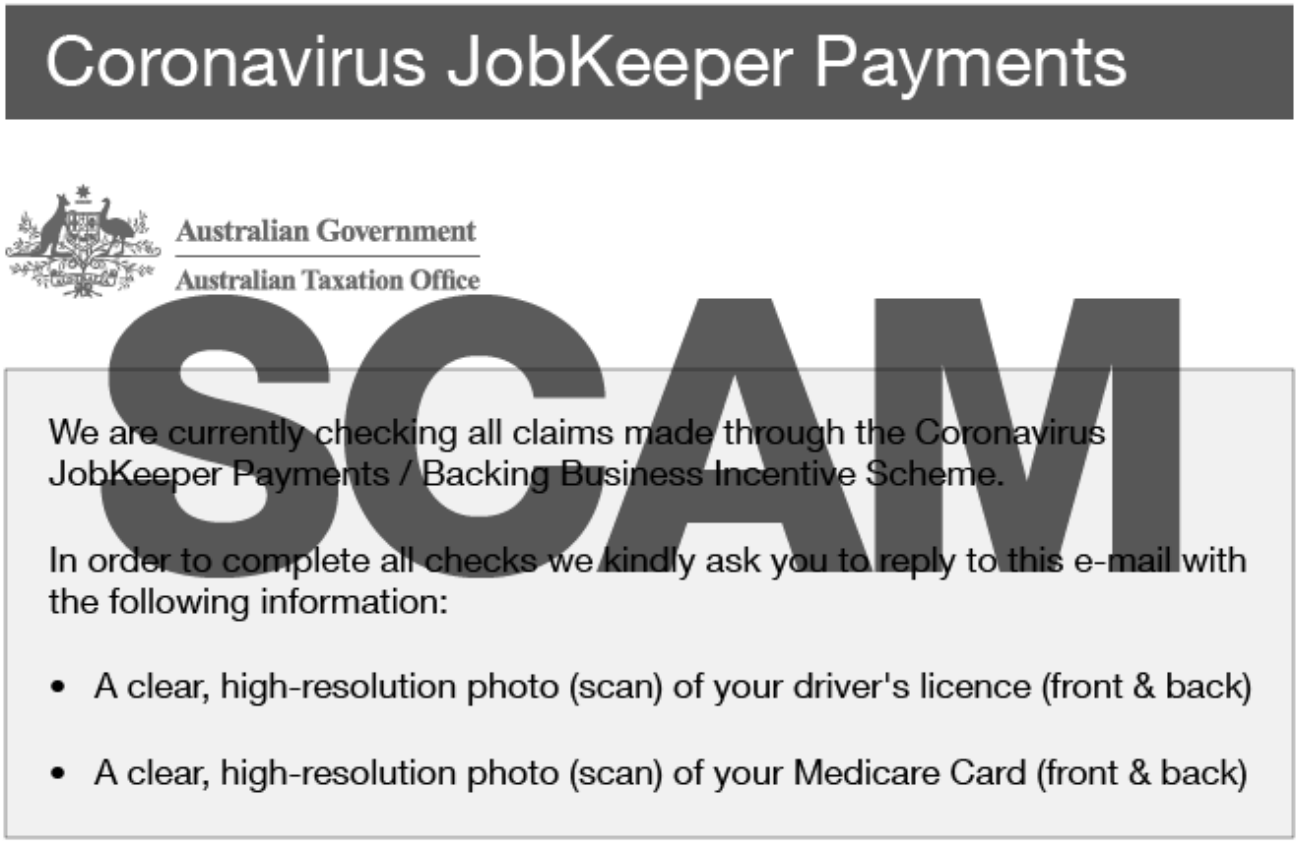
- March 2020 SMS scam – tax refund notification
- February 2020 SMS scam – 8% bonus for people affected by natural disasters
- January 2020 SMS scam – tax refund notification

October 2020 email scam – JobKeeper and backing business investment claims

We are receiving reports of email scams about claims for JobKeeper and Backing Business Investment. The fake emails say we are investigating your claims. They ask you to provide valuable personal information, including copies of your driver's licence and Medicare card.

The image below is one example of an email scam currently circulating.

Do not provide the information requested, do not click on any links and delete the email straight away.



If you receive a message from the ATO asking for your personal information, phone us on **1800 008 540** to make sure it's legitimate. If you think it's fraudulent, report it by sending an email to reportemailfraud@ato.gov.au (mailto:reportemailfraud@ato.gov.au).

You should never give out your personal information unless you are sure of who you are dealing with.

September 2020 phone and SMS scams – fake tax debt

We are concerned about the increasing number of people paying fake tax debt scammers.

Scammers pretending to be from the ATO are contacting members of the community, telling them that they have a tax debt and that if they do not pay it straight away they will be arrested.

These scammers will often request payment through unusual methods, such as cryptocurrency, pre-paid credit cards or gift cards. They will try to keep people on the line until they have paid.

If you receive a phone call, text message or voicemail like this, don't send payment or provide any personal information. Hang up and delete the message.

We will **never**:

- threaten you with immediate arrest
- demand payment through unusual methods.

If you are not sure if it's the ATO contacting you, phone us on **1800 008 540** to check.

It's also a good idea to know your tax affairs. You can:

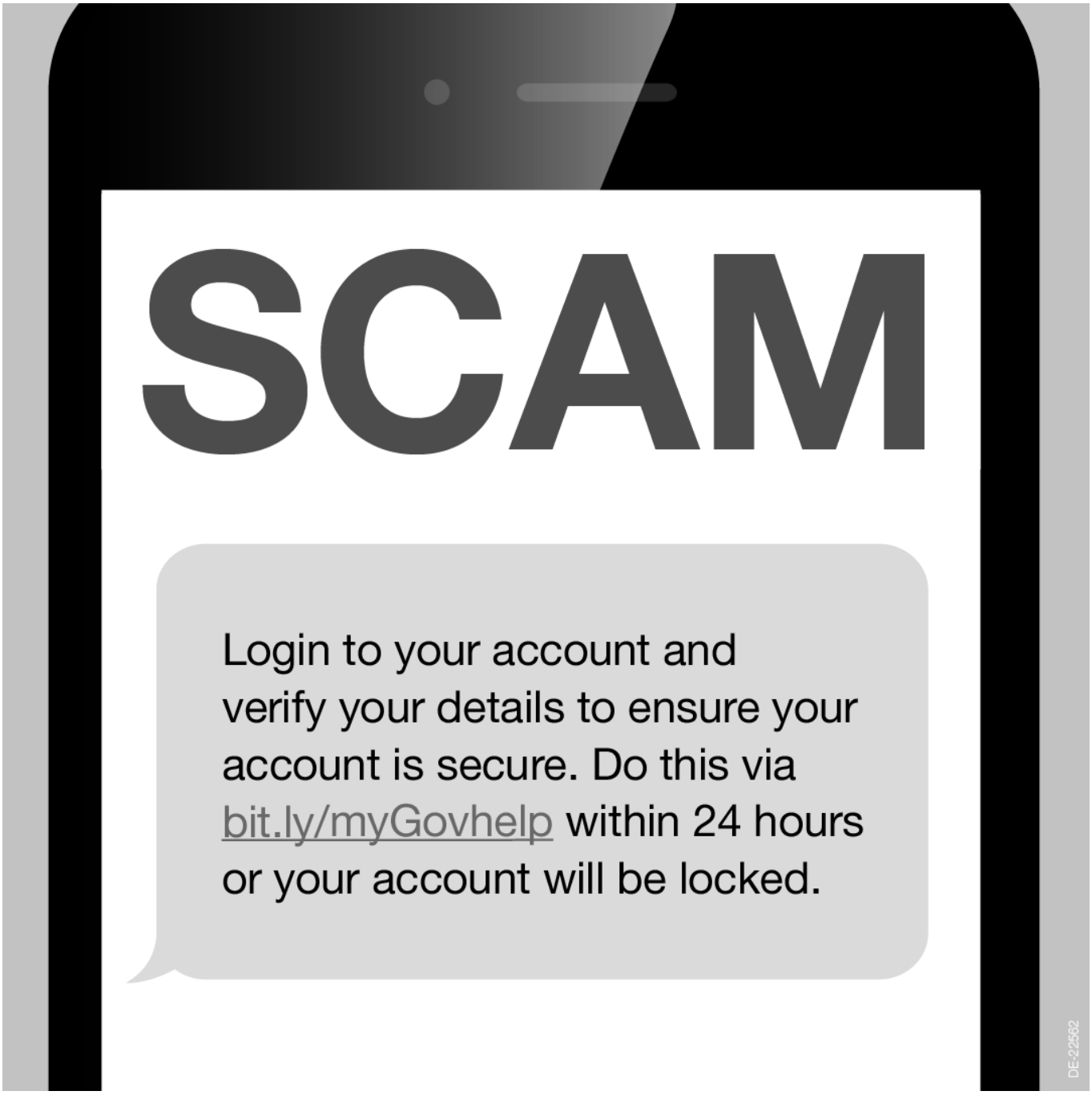
- log in to ATO online services through myGov to check your individual tax affairs
- log in to Online services for business to check your business tax affairs
- contact your tax or BAS agent
- contact us (/About-ATO/Contact-us/).

July 2020 SMS and email scams – verify your myGov details

We are receiving increasing reports of several myGov-related SMS and email scams. These scams look like they have come from a myGov or ATO email address. They also might appear in your legitimate ATO or myGov SMS message thread.

The image below is one example of an SMS scam currently circulating.

Don’t click any links and don’t provide the information requested.



You will get email or SMS notifications from myGov when there are new messages in your myGov Inbox. However, these messages will **never** include a link to log on to your myGov account. Always access our online services directly via one of the following:

- **my.gov.au**
- **ato.gov.au**
- the ATO app (/General/Online-services/ATO-app/).

All online management of your personal tax affairs should be done in ATO online services, accessed through your genuine myGov account. Any communications containing your personal information, such as your tax file number (TFN), will be sent to your myGov Inbox, not your email account.

You can make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

If you receive an SMS or email from the ATO that you think is fraudulent, report it by sending an email to reportemailfraud@ato.gov.au (mailto:reportemailfraud@ato.gov.au).

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 (mailto:reportascam@servicesaustralia.gov.au).

If you have clicked on a link or provided your personal information, contact Services Australia on **1800 941 126**.

June 2020 phone scam – threatening arrest and requesting personal details

We are receiving reports of scammers sending members of the public automated phone calls pretending to be from the ATO, as well as other government agencies including Services Australia and the Department of Legal Services.

These automated calls claim their TFN has been suspended and that there is a legal case against their name. The call tells people they must contact the caller by pressing '1' or they will be referred to the court and arrested.

If the person presses '1' and makes contact with the scammer they are typically told that their TFN had been suspended due to money laundering or other suspicious or fraudulent activity and that there are several allegations against them. They are then asked to provide:

- the last four digits of their TFN
- their address
- their date of birth
- the name of their bank account
- the approximate amount of money in the account/s.

Sometimes the scammer will 'transfer' the victim to the 'police' where they're told a case has been filed against them and they will be arrested unless they pay.

Sometimes they advise the victim will receive mail to their home or that their bank accounts will be closed.

If you receive this call, hang up and do not provide the information requested. We will **never**:

- send unsolicited pre-recorded messages to your phone
- threaten you with immediate arrest.

If you are not sure whether an ATO call is legitimate, hang up and phone us on **1800 008 540** to check.

May 2020 phone scam – requesting bank account details for the JobKeeper payment

We are receiving reports of scammers pretending to be from the ATO calling members of the public and asking them to provide their bank account details. They are telling them that:

- their employer has registered them for the JobKeeper Payment
- we need their bank account details to deposit the funds into their account.

Do not provide the information requested. Employees that are eligible for JobKeeper payments will be paid by their employer and the ATO will reimburse their employer for these payments. We **do not** need the bank account details of individual employees.

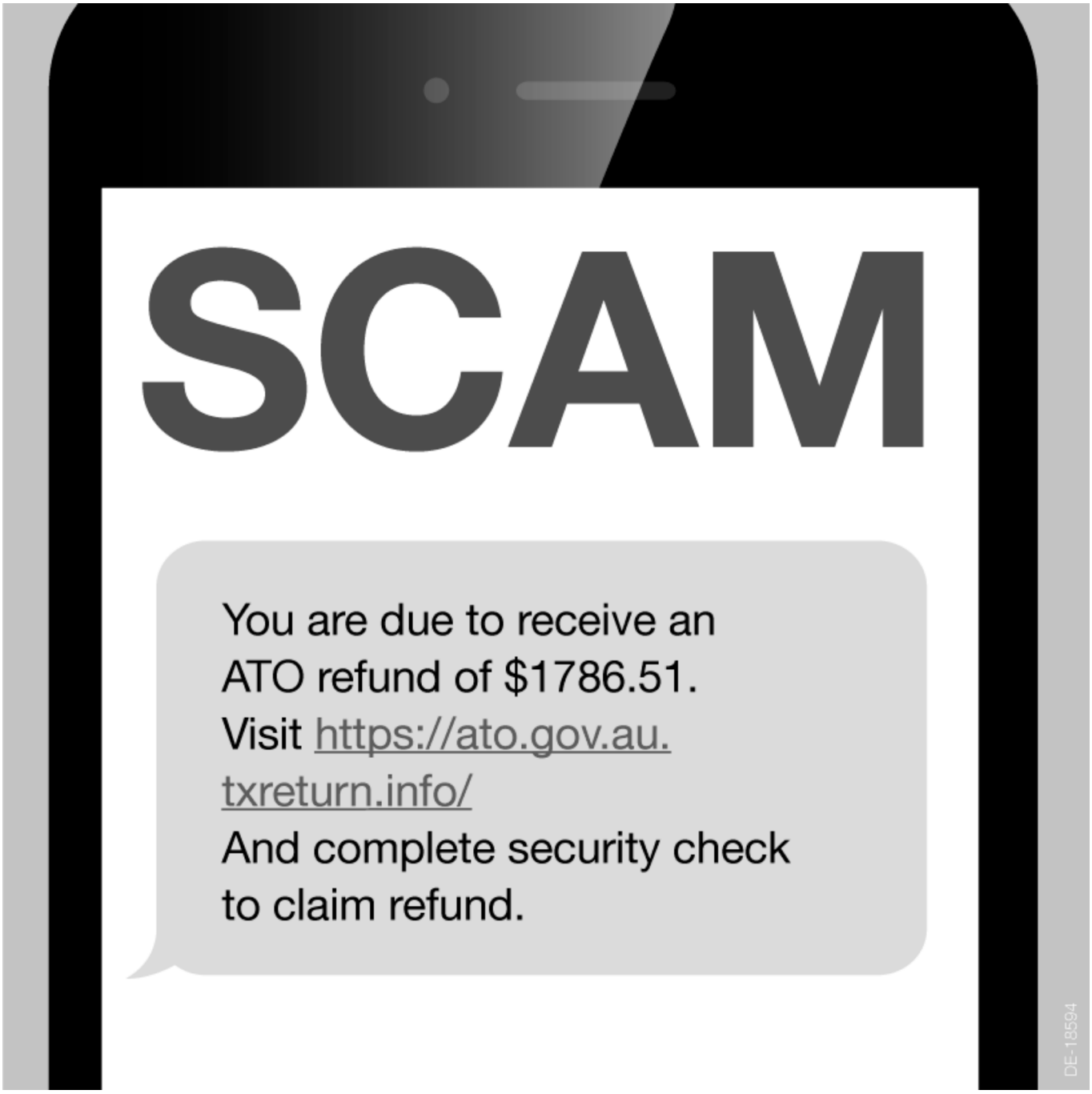
If you are not sure whether an ATO call is legitimate, hang up and phone us on **1800 008 540** to check.

March 2020 SMS scam – tax refund notification

Scammers are texting people, asking them to click on a link and provide personal identifying information to receive a refund.

The image below is one example of the format this scam can take. The link in this scam will take you to a fake myGov website.

The website is a phishing page and is being used to harvest user credentials. Do not click on any links and do not disclose the information requested.



We will **never** send an email or SMS asking you to access online services via a hyperlink.

If you use ATO online services for individuals and sole traders, all online management of your tax affairs should be carried out in ATO online services, accessed through your genuine myGov account. Sign in to your myGov account at my.gov.au.

Make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

February 2020 SMS scam – 8% bonus for people affected by natural disasters

Scammers are exploiting Australia's recent natural disasters in an SMS scam that is asking people to click on a link and provide personal information in order to receive an 8% bonus on their tax return.

The image below is one example of the format this scam can take.

The link will take you to a fake myGov website, designed to steal your personal information. Do not click on any links and do not disclose the information requested.

We will never send an email or SMS asking you to access online services via a hyperlink.

We will never ask you to provide any personal identifying information in order to receive a refund.

All online management of your tax affairs should be carried out in ATO online services, accessed through your genuine myGov account. Sign in to your myGov account at my.gov.au.

You can make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

When disasters like the recent bushfires strike, scammers will often try to take advantage of vulnerable Australians.

We do what we can to stop scammers in their tracks, but it's important to stay vigilant and warn your family and friends.

January 2020 SMS scam – tax refund notification

Similar to the alert we issued in August, scammers are texting people asking them to click on a link and provide personal identifying information to receive a refund.

To make the text messages seem more legitimate, scammers are using technology that causes them to appear in your genuine ATO message feed.

The image below is one example of the format this scam can take. The link in this scam will take you to a fake myGov website.

The website asks users to provide their bank details, along with other personal identifying information, for 'verification purposes'. Do not click on any links and do not disclose the information requested.

We will never send an email or SMS asking you to access online services via a hyperlink.

All online management of your tax affairs should be carried out in ATO online services, accessed through your genuine myGov account. Sign in to your myGov account at my.gov.au.

If you haven't already, make accessing your myGov account more secure by opting to receive a security code via SMS. It's a quick and secure way to sign in to access ATO online services.

We've initiated disruption activity to protect the community from this scam, but it's a good idea to encourage your friends and family to keep an eye out. This is particularly important in the current environment, as scams often spike when people are most

vulnerable.

Last modified: 30 Nov 2021 QC 53447

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice