PROTECT YOURSELF
KNOW THE SCAM

AVOID BEING SCAMMED THIS TAX TIME

The End of Financial Year (EOFY) is a popular time for scam emails, SMS and phone calls from criminals claiming to be the Australian Taxation Office (ATO). Scammers often use software to 'spoof' the caller ID, changing the incoming phone number to mimic the number of a real organisation or person.

To learn how to PROTECT YOURSELF and KNOW THE SCAM visit www.police.sa.gov.au/scams

Report all scams to www.cyber.gov.au/report

SOUTH AUSTRALIA POLICE
SAFER COMMUNITIES

Government of South Australia

Supported by:
Neighbourhood Watch SA

PROTECT YOURSELF
KNOW THE SCAM

Scammers may use scare tactics to trick you into paying money with pre-paid gift cards or sending money to non-ATO bank accounts.

Warning signs:

- Password reset requests.
- Warnings that your account has been compromised.
- Tax refund emails/SMS.
- Reminders to pay taxes.

Protect yourself by:

- Checking legitimate payment methods on the ATO website.
- Checking the sender's email address to confirm email is authentic.
- Never trusting the caller ID.
- Hanging up the phone and calling the person back on a known, reputable number.

No official organisation would ever ask for your sensitive information via an email or SMS. Be aware of what you share – don't give out details such as your tax file number (TFN), date of birth, credit card or bank details unless you have confirmed the source and the need for the information.

Don't be pressured into making a decision. Scammers may create a sense of urgency to scare you into the scam.

Before you send money or bank details to anyone, discuss it with someone you trust.

To learn how to PROTECT YOURSELF and KNOW THE SCAM visit www.police.sa.gov.au/scams

These scams can be reported to www.cyber.gov.au/report