

Introduction

Many scams begin with an unsolicited phone call where a scammer claims to be from a well-known organisation. This may include government departments, police, financial institutions or service providers. These calls can also take the form of an automated 'robo' call.

Prevention checklist

- ☐ Be vigilant when receiving unsolicited calls.
- ☐ Be suspicious of any sense of urgency being placed upon you to act.
- ☐ While the number may appear to be legitimate – hang up and contact the organisation on their verified number.

Detection checklist

These are some of the common themes of cold calls

- ☐ Someone is trying to access your bank account, and you need to move your money into a "safe" account.
- ☐ A payment has been processed on your bank card; was this you making the purchase?
- ☐ Someone is trying to access your cryptocurrency, and you need to move your funds into a "safe" wallet.
- ☐ An issue has been detected with your Wi-Fi, modem, computer or mobile device which needs immediate attention.
- ☐ A mobile phone has been registered in your name and is being used for fraudulent activity.
- ☐ The AFP has detained a person at an airport in possession of identity documents and/or bank cards in your name.
- ☐ Themes of being involved in illegal activity you know nothing about.

If you have received any of these calls recently – you have likely been targeted by a cold call scam.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response checklist

If you or someone you know has been involved in a cold call scam, the below checklist outlines some measures you can take to prevent further harm.

- ☐ Cease all communication with the scammer.
- ☐ Tell a trusted person what has happened if you need support as you work through the financial, emotional and practical recovery.
- ☐ Advise your bank(s) of the scam (if this information was provided).
- ☐ Notify the relevant document issuing organisations for any of the credentials that the scammer may have accessed. Common credentials include:
 - Driver licence
 - Passport (Australian passports contact [DFAT](#) on 131 232, for NZ passports contact [DIA](#) on 0800 22 50 50)
 - ATO details (Australian residents call 1800 467 033) or IRD details (NZ residents call 0800 257 777)
 - RealMe details (NZ residents call 0800 664 774 or online at [RealMe](#))
- ☐ If you have provided government issued identity documents, contact both credit reporting agencies for your [credit reports](#) and to request a [credit ban](#).
- ☐ If you have sent or received money or goods online, provided remote access to your computer, or shared credentials online that would enable identity theft and fraud, you can alert police through:
 - [ReportCyber](#) (in Australia)
 - Call 105 or [online](#) and choose "Report a Police non-emergency" (in New Zealand)
- ☐ Contact your GP if you feel you need additional support and strategies to deal with the stress of your situation.
- ☐ Be aware that you may see an increase in scam attempts.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.