

Introduction

Telephone scammers often claim to be from a legitimate organisation, most commonly government agencies, banks, telcos or internet service providers, utility providers, online retailers or streaming services. Most often the scammer will call you, but sometimes you may accidentally call them if you have found the wrong number online or are responding to fake “pop-up” warnings on your screen.

Telephone scammers:

1. Deceive individuals into providing personal information and payment details over the phone; and
2. May deceive individuals into providing remote access to their device(s), enabling them to harvest more information, make transactions, and/or install malicious software.

Prevention checklist

How can I avoid a telephone scam?

- ☐ Scammers may know some of your personal information, such as your name and address, and use this to ‘verify’ your identity. Remember that this information is often publicly available or may have been previously exposed in a data breach.
- ☐ Being on the Do Not Call register **will not** stop scammers – it will only stop legitimate telemarketers calling you.
- ☐ Organisations won’t call you and then ask you to prove your identity.
- ☐ Don’t feel pressured to act. You will never be called to “prevent being arrested” or to “assist police to catch a hacker.”
- ☐ If you think a call may be legitimate, take down the person’s name and number, end the call, and do your own research regarding the organisation and its contact details.
- ☐ **Do not** download apps or software (such as AnyDesk or TeamViewer) or allow remote access to your device to someone who has called you.
- ☐ Consider changing your phone settings to only allow calls from numbers listed in your “Contacts”. Some phones will silence calls from “unknown” numbers and send them straight to voicemail, while others will block these calls completely. Be aware that these changes will also prevent legitimate callers from numbers that are not in your Contact list or Recent call log.

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.

Detection checklist

If you are concerned that you or someone you know may be involved in a telephone scam, you may find this checklist helpful.

- ☐ A cold call from an individual claiming to be from a government agency or well-known private sector organisation.
- ☐ The caller requests that you prove your identity.
- ☐ The caller claims to be from the police and is threatening your arrest if you do not respond.
- ☐ The caller claims to be from law enforcement, the government, a bank or an internet provider. They need your assistance to catch a scammer or hacker. They may claim to require access to your device and/or bank accounts.
- ☐ The caller claims to be from your bank regarding problems with your account(s), such as fraudulent activity.
- ☐ The caller claims your account has been overcharged, and they need to reverse these charges.
- ☐ The caller claims that your computer has a virus and you must pay money to have it removed. They may also request remote access to your device.
- ☐ The caller directs you to purchase gift cards or cryptocurrency or make transactions from your bank account.
- ☐ The caller coaches you in what to say to the customer service operators at your bank or shops when transacting or making a purchase.
- ☐ The caller tells you not to hang up and/or not to disconnect your device from the internet for a period of time.
- ☐ The caller becomes aggressive when you do not act quickly or provide them with the information they request, or you ask too many questions.

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 telephone scam, the below checklist outlines some measures you can take to prevent further financial harm.

- ☐ If the scammer gained remote access to your device, disconnect it from the Internet immediately.
- ☐ Contact and advise your banks and any other financial institutions of the telephone scam, and request increased security on your accounts.
- ☐ Contact the legitimate organisation that the scammer claimed to be calling from, and request additional security on your account.

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.