Understanding Telephone Scams

Understanding telephone scams

The most prolific form of identity compromise currently impacting the Australian and New Zealand communities are telephone scams.

Most scams originate from offshore. There are two common varieties –

1. scams that deceive individuals to provide personal information and payment details over the phone;
2. scams that can lead to remote access of a device for the purposes of harvesting information, transacting and/or installing malware, such as ransomware.

Detecting telephone scams

- Cold calls from individuals that claim to be from well-known government and private sector organisations.
- Numbers may appear from Australia or New Zealand, but will likely be routed from offshore.
- Scammers will look to incentivise individuals to act on something, for example a prize, a grant, an unpaid tax, a virus.
- Some may even threaten legal action or money loss.
- Scammers will ask you to "prove" who you are or ask for access to your device.

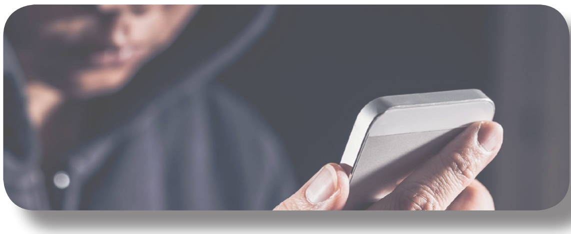
Preventative measures:

- Good organisations won't call you and then ask you to prove yourself.
- Scam calls can be received from landline or mobile numbers and the "Do Not Call" register will only keep honest telemarketers at bay.
- Don't feel pressured to act. If you think a call may be legitimate take down the person's name and number and do your own research. Make sure when you hang up you hear a dial tone – some scammers will pretend to hand up and catch you dialling the real organisation's number only to pretend to answer it (when they haven't disconnected from the first call).
- Don't think a message left is more legitimate, it's not.
- Hang up if you suspect it is a scam and talk to family or friends about it.

Understanding Telephone Scams

Responding to telephone scams:

- If you believe that you have experienced a telephone scam contact IDCARE for assistance 1300 432 273 (AUS) 0800 201 415 (NZ) or idcare.org.
- Disconnect your device immediately from the Internet if they have gained remote access.
- Immediately contact your financial institution(s) and inform them of what has happened.
- Engage service providers and ask what additional security can be put in place.
- Note down any identifiers of scammers, such as the telephone numbers they have called from.
- If you believe you have had your licence, passport or other high-risk credential compromised see our Fact Sheet about Credit Reporting Agencies.



More information

- In June 2018, 45% of individuals experienced a telephone (remote access) scam.
- One of the main reasons for believing a telephone scam was the scammer knowing details about an individual (eg. name and address.
- Another reason for believing a scam was if an individual was experiencing issues with their internet or device.

Other Fact Sheets

- Credit Reporting Agencies
- Scam Prevention and Education
- Engaging Organisations
- Social Media
- Devices and Technology
- Your Rights