Phone Scams target everyone

Scams target people of all backgrounds, ages and income levels across Australia. There's no one group of people who are more likely to become a victim of a scam, all of us may be vulnerable to a scam at some time.

Scams succeed because they look like the real thing and catch you off guard when you're not expecting it. Scammers are getting smarter and taking advantage of new technology, new products or services and major events to create believable stories that will convince you to give them your money, or personal details.

Be alert to the fact that scams exist. 30% of scams involve a phone call. When dealing with uninvited contacts from people or businesses over the phone, always consider the possibility that the approach may be a scam. The person on the other end of the call may sound very believable, and sound like they have your interests at heart, but they don't. They may imply that your current supplier is being sold, or they are taking it over, or they may imply that your current services will be detrimentally affected if you don't immediately transfer your services to them. Do not make any commitment on the basis of a single phone call, ask for information about their organisation, how they got your personal information, check out who they say they are, check the TIO members List, and call us if in doubt.

Its probably a scam if:

- someone you don't know has your personal details
- your bank (or another institution that you trust) calls or texts you to ask for personal information or money
- you're threatened or made to feel afraid
- someone asks to access your computer
- a call or text sounds too good to be true

Don't respond to phone calls about your computer asking for remote access – hang up – even if they mention a well-known company such as Telstra. Scammers will often ask you to turn on your computer to fix a problem or install a free upgrade, which is actually a virus which will give them your passwords and personal details. The only time we would ask for remote access is when we are resolving a service difficulty that you have reported to us.

Keep your personal details secure. Put a lock on your mailbox and shred your bills and other important documents before throwing them out. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam. Ask us to set up a password on your account, we would ask for this password before we discuss anything on your account.

Keep your mobile devices and computers secure. Always use password protection, don't share access with others (including remotely), update security software and back up content. Protect your WiFi network with a password and avoid using public computers or WiFi hotspots to access online banking or provide personal information.