Phone scammers – don't fall for them

Customer guidance on scam phone calls and text messages

Phone scamming is big, bad business

Phone scammers cheat tens of thousands of Australians out of many millions of dollars every year, using fraudulent phone calls and text messages. They're cunning and calculating, but you can make yourself safer by taking some simple steps.

Types of scam call and text fraud risks

Scam callers and texters almost always seek *financial gain*.

- They might try to trick you into making an *immediate payment* to them or an associate, or they may be trying to get enough *information about you* to steal your identity.
- They may even try to fool you into giving them *remote control of your computer*, so they can read your emails or banking information or other confidential information.
- If they can successfully pretend to be you, or learn your account passwords, they might *steal from your bank account*, buy things with *your credit card*, or incur other *debts in your name*.
- In other cases, scammers ring your phone briefly and hang up from a premium rate number – with high call back charges – in the hope you'll see a missed call and dial back. Then the call back charges kick in – billed to your phone account. The scammer has arrangements to collect part of those charges at their end.
- Especially around tax time, scammers pretend to be calling from the Australian Taxation Office, seeking information or payment of money.
- Some scammers resort to threats e.g. they are from a government agency, and you have an overdue fine (that you didn't know about) – and that you'll be locked up if you don't make immediate payment to the account they nominate.
- Some scammers impersonate charities and seek donations, especially when a disaster or emergency is in the news.
- There are scammers who use 'spoofing' tools to send you a text that appears to have come from your own handset, hoping you'll open the message and click on a dangerous link.
- Some scammers pretend to be from a parcel delivery company, and recommend that you download certain software to track your parcel deliveries – but the software is really for giving the scammer access to your computer.
- Some scammers call to say you've won a prize, and may ask for your account details so they can 'pay' the prize into your account.
- Then there's a fraud know as 'smishing', where you receive a

message like: *Nice weekend coming up. Sophie and I are going to an outdoor art show, and she asked me to invite you along. Check out the event at (a dangerous web address)*.

- Other bogus texts might 'advise' you that your movie streaming account is about to be cancelled, and offer you the chance to keep it active by clicking on a dangerous link.
- A scam text might congratulate you on winning a prize, which you can 'claim' by clicking on an included – dangerous – link.

Frauds are always working on new ways to phone scam, so no list of scams is ever complete. But you can learn a lot more from official Australian Government resources like:

- www.cyber.gov.au
- www.scamwatch.gov.au
- www.communications.gov.au/what-we-do/phone/unwanted-communications-faqs

We especially recommend the Australian Competition and Consumer Commission's publication the *Little Black Book of Scams* at www.accc.gov.au/publications/the-little-black-book-of-scams – dealing with phone call scams, text message scams and other kinds of scam as well.

Blocking suspicious or unwanted calls and text messages

iPhones

Do you use an iPhone? Make sure you've installed the latest version of the iOS operating system and you can 'silence unknown callers' in your phone settings.

Any caller that's not in your contacts list will be diverted to voicemail. Listen to your voicemail, and if you decide the call is legitimate you can return the call, and perhaps add them to your contacts for future calls.

To block an individual number, go to the recent calls screen and press "i" for a number's "information". There's a block option at the bottom of that screen. That will block calls and text messages from that number.

To block someone who has texted, but not called you:

- Open their message … but don't click on any links.
- Tap on their circular 'headshot' at the top of the screen.
- On the next screen, tap on 'info'.
- On the 'info' screen, tap on 'Block'.

That will block texts and calls from that source.

In the Apple App Store, you'll find several apps that may assist in identifying and blocking scam calls. Use the search term 'call block' and 'text block' to find some options.

Android phones

Is your phone a Samsung, or another Android brand? Your recent calls list in

the phone app may offer an option to block each number. If you've had calls or a suspicious text from a number you don't trust, consider blocking them.

In the Google Play Store, you'll find several apps that may assist in identifying and blocking scam calls and texts. Use the search term "call blocker" to find some options.

If you're using the Google *Messages* app:

- Start Messages and open a message from a source that want to block … but don't click on any links.
- Tap the three-dot menu at the top right of the screen.
- In the drop-down menu, tap 'Details'.
- On the Details page, tap "Block & report spam'.
- On the pop-up that follows, choose whether you want to report the text messages as spam. If you do, check the box for 'Report spam.' You can clear the checkbox if you don't want to report the messages.
- Tap 'OK' to block all future messages from this sender.

Landlines – anti-scam handsets

Some phone companies offer handsets with built-in anti-scam features, like 'announce' mode, where anyone calling your number needs to announce who they are and then press the "hash key". This will filter out the autodiallers that many scam callers use.

Landlines – network blocking

Phone network operators may be able to block specific problem numbers if you notify their support team.

Reducing your risks

You can minimise the risks associated with scam calls and text messages.

Protect your personal information

It's a good rule these days that information about you should only be shared with people you trust, and for good reason. Online, on the phone, in opening and responding to text messages or in the 'real' world, be discriminating in what personal information you give to strangers.

Don't share personal information with unknown or unsolicited callers or texters

Has your bank or a government department ever asked your date of birth before talking about your affairs with you? If you tell a scam caller or text messager your date of birth, they could answer that security question as if they were you.

Keep all your personal details sensibly secret, especially from callers and text messagers you haven't reliably identified. That means name, address, date of birth, which bank you're with, etc, etc, etc. Unless you know who's asking, and why, treat all personal data secret.

Contact your financial institution immediately, if you think a scammer has taken your money, or may be able to

Your bank or credit card issuer may be able to stop a transaction or even reverse it, if you act fast. They may be able to temporarily lock a card or account to protect it.

Change default PINs and passwords as soon as you get a new phone or other communications device

Some equipment comes with a preset PIN or passcode (like "1111") or password (like "Admin"). Change these to personalised ones immediately, or a scammer might guess the PIN, passcode or password very easily.

Choose strong PINS, passcodes and password

Whether it's the PIN, passcode or password for your bank account, mobile phone handset, an online store or a health fund, make sure it's not a 'weak' one that's easily guessed, or worked out by a computer – like '1234' or '0000' or 'password', etc).

Use your favourite search engine to search for 'how to choose a strong password" or 'how to choose a secure password' for a lot of good advice on what makes a secure PIN, passcode or password.

Lock your mobile handset with a secure PIN

Set your mobile handset to auto-lock after a short period of non-use, and set it to require a strong PIN to unlock it. Even if your handset also offers face or fingerprint recognition, a weak PIN (like the current year) may let a fraud access it with ease.

Make sure your voicemail PIN is secure

Does your mobile phone service or landline offer a 'voice mailbox' where callers can leave messages? It's great to be able to check your home messages from another phone when you're out – but not so great if a scammer can dial in and listen to them as well.

Voicemail services almost always use a PIN to keep out unauthorised persons, but make sure your PIN is strong and secure.

Disable PABX ports and features that are not used

If your business uses a 'PABX', it's a powerful system – a 'mini phone company in your office'. But some of the powerful tools can be used for fraud.

For instance, some systems let you dial in from outside and divert your office number to wherever you are. But there's always a risk of a bug that lets a scammer take control of your PABX feature and divert your calls to themself. Even if the risk is small, why take it if you never actually use that feature?

If you have a PABX or another sophisticated business phone system, check your user manual or contact your product consultant for information about turning off unnecessary or unused features. A feature that isn't enabled normally can't be 'hacked'.

Change PINs, passcodes and passwords regularly

Using the same PINs, passcodes and passwords for a long time is a security risk. For instance, when online stores are hacked, lists of their customer passwords are often sold on the internet. If you changed your password regularly, the password being offered online would be stale before long – even before a scammer had a chance to use it.

Don't respond to text messages or missed calls from unknown international or Australian numbers, or unknown callers

The tricks that scammers play with missed calls are explained above. Text messages asking for a call back can be traps in the same way. Don't call back. If the caller is legitimate, they'll leave a message. If you think you know who it may have been, contact them by another means (e.g. email, another phone number on an official website, etc) and check if they called or texted.

Block suspicious or unknown international or Australian numbers on mobile handsets and use of blocking services or products, where available, on landlines

This is also explained above.

Let unknown calls to go to voicemail / listen to any message left / decide if this might be a genuine call

It's explained above how to automatically send calls to voicemail (in some cases). If you can't do that, you can choose to simply not answer unknown calls. Your own voicemail message might encourage callers to leave a detailed message, so you get enough information to make an informed choice whether or not to call back.

Talk to family or friends

If you're not sure about a call you have received, talk about it with someone close to you. Two heads can be wiser than one.

Don't take computer actions at the request or direction of a caller

If someone on the phone, or who texts you, whom you don't positively trust asks you to download or install software, visit a web page, click on a link, fill in a web form or open an email – **don't do it**. They could easily be trying to trick you into giving them control of your computer, or otherwise assisting them to scam you.

What to do if you receive scam calls or text messages

If you do receive a scam call or text message, you should consider taking action.

You can protect yourself

- by blocking the calling number, as explained above
- by contacting police immediately if you have been threatened or had your property stolen
- by contacting your financial institution immediately, if you believe your account/s have been compromised or you have made a

payment to the scammer

- by immediately changing PINs, passcodes or passwords that might be at risk

You can help protect the community

- by reporting the scam call to ScamWatch – an initiative of the Australian Consumer and Competition Commission (**ACCC**) at www.scamwatch.gov.au