

SAFEGUARDING AGAINST TEXT AND CALL SCAMS

Risks of text and call scams

Text and call scams pose significant risks, especially for our older community members. Scammers often target seniors, taking advantage of their trust and kindness. These scams can result in financial loss, identity theft and emotional distress. Common scams include fake lottery wins, urgent requests for money, and fraudulent calls claiming to be from government agencies. Understanding these risks is the first step in protecting yourself from falling victim to these schemes.

How to spot text and call scams

Recognising text and call scams is crucial for your safety. Be wary of unexpected messages or calls asking for personal information, money or access to your computer. Scammers often use urgency or fear tactics to manipulate victims. Watch out for unusual numbers, generic greetings and messages with spelling errors. Legitimate organisations won't ask for sensitive details via text or phone without prior arrangement. They will also never call you from a mobile or overseas number. If something feels off, trust your instincts and end the call. Prior to taking any action, check with friends or family. If you wish to contact the organisation the caller said they were calling from, ensure you use their phone number displayed on bills or letters. Do not call back the number they have called or texted you from.

What to do if you receive a text and call scams

If you receive a suspicious text or call, stay calm and never share personal information, such as your bank details or government-issued numbers, over the phone. Do not let them rush you – legitimate organisations do not rush us. Avoid clicking on any links or opening attachments in text messages from unknown sources. Hang up on unexpected calls that make alarming claims or requests. Report the incident to your phone carrier and relevant authorities, such as the Australian Cyber Security Centre www.cyber.gov.au. Do not hesitate to ask for help from friends or family. Keeping a record of the incident details, including the caller's number and the content of the message, can aid in investigations.

How to protect yourself from text and call scams

Protecting yourself from text and call scams involves adopting proactive measures. Start by registering your phone number on the "Do Not Call" register in Australia: go to www.donotcall.gov.au and click on "register your numbers". Be cautious about sharing personal information on the phone, via text or on website links they provide. Educate yourself about common scams and stay informed about the latest tactics: the ACCC manages the Scamwatch website, which provides detailed information about various scams, alerts about new scams, and tips on how to protect yourself from scams.



FAMILIES OF VETERANS GUILD

You can visit the Scamwatch website at: <https://www.scamwatch.gov.au/>

Regularly review your bank statements for any unusual activity, and if you have concerns, contact your bank immediately. Remember, staying informed and vigilant is your best defence against text and call scams.

By being aware of the risks, learning how to identify scams, knowing what to do when confronted, and implementing preventive measures, you can be empowered against text and call scams. To help you identify potential scams, we have some examples below.

Examples of common text scams:

Phishing texts:

Example: "Your bank account has been compromised. Click on the link to verify your details immediately."

Fake prize or lottery wins:

Example: "Congratulations! You've won \$1,000 in our prize draw. To claim your prize, reply with your credit card details."

Government impersonation:

Example: "URGENT: Your tax file number has been suspended. Call us immediately to avoid legal action."

Fake delivery notices:

Example: "Your package delivery is pending. Click the link to track and reschedule."

Support scams:

Example: "Virus detected on your phone! Call this number now for assistance."

Romance or family scams:

Example: "Hi, I'm overseas and in trouble. Can you send me money urgently? I'll pay you back."

Charity scams:

Example: "Help us support disaster victims. Donate now by clicking on the link."

Subscription renewal scams:

Example: "Your subscription will be automatically renewed today. Click to cancel if you don't want to be charged."

Remember, legitimate organisations usually do not request sensitive information or payments via text messages. If you receive a suspicious message, do not click on any links or provide personal information. Verify the message with the supposed sender through official channels: call them on their official phone number to make sure everything is in order or visit your accounts online. Report scams on www.cyber.gov.au to help protect others.