Fact Sheet

CRIME STOPPERS .com.au 1800 333 000 NSW

NSW GOVERNMENT

NSW Police Force

# PHONE SCAMS


SHARE IF YOU CARE

Australians have lost on average $41 million per month in scams in the first six months of 2022 (ACCC data 2022). In the last year more than $2 billion in total combined losses reported to ScamWatch, ReportCyber, 12 financial institutions and govt agencies*.

Phone calls and text messages are the most common methods used by scammers. Scams via phone calls accounted for 50% of all scams. Scams via text messages accounted for 23% of scams*.

Scammers are finding new and smarter ways to steal people's hard-earned money, so it can be difficult to know if a call is a scam or not and its causing financial devastation and emotional harm to individuals, families, and businesses.

## Phone Calls

**Say bye bye or kiss your cash goodbye**

- Scammers will often pretend to be from trusted organisations.
- If you think something might be legitimate, call the organisation or government agency back using details you find in an independent search, rather than the details provided by the caller.
- Be suspicious of callers you don't know. Scammers find ways to get your personal information, credit card or account details. The best way to protect what's yours is to not share any information with them.
- If you are unsure who is calling and the caller leaves a message, check the number matches the one on the caller's website.
- Scammers use a sense of urgency to get you to act quickly and without thinking. This should be a red flag and you should just hang up.
- If you get a phone call that doesn't sound right, hang up. Check in with someone you trust, like a friend or family member, to talk about it.
- Don't ever send money or provide payment details over the phone to someone you don't know.

## Text Messages

**THINK before you CLICK**

- Scammers are using applications via text that, once opened, can add malware to your phone and/or extract your personal details. If you receive a text message from an unknown number or entity just delete it.
- Stop and think before you click the link. Be careful about clicking on links and attachments, even if a message seems to come from a legitimate source or someone you know.
  It's always safer to look something up or type in a web address yourself.
- If you suspect your phone has been infected with malware, back up your personal items only (such as photos, authenticators), and complete a factory reset on your device.

*(Targeting Scams Report of the ACC on scams activity 2021).

Fact Sheet

CRIME STOPPERS .com.au 1800 333 000 NSW

NSW GOVERNMENT

NSW Police Force

# PHONE SCAMS


SHARE IF YOU CARE

## Minimise Your Risk

- Don't give out your personal identifying information unless you trust the person you're speaking with.
- Create strong passwords, and do not share them with anyone. Passwords should be a minimum of 10 characters consisting of at least three of the following character sets:
  - lowercase alphabetic characters (a-z)
  - uppercase alphabetic characters (A-Z)
  - numeric characters (0-9)
  - special characters
- Secure your private Wi-Fi network with passwords and do not make financial transactions when using public Wi-Fi networks. These are unsecured networks so it's easier for cybercriminals to intercept your information.
- Be careful about the information you share about yourself
  on social media. It's easy for information on social media sites to be shared outside of your network, even when your security settings are set to private.

## Is it a Scam?

It is probably a scam if:

- A call or text that sounds too good to be true
- Someone you don't know has your personal details
- You are urged to 'act urgently'
- You are threatened, blackmailed, or made to feel afraid
- Someone asks you for access to your computer

## If you think you have been scammed:

- **Contact your financial institution** as soon as possible. They may be able to find out where the money was sent, block the scam accounts, or help others avoid sending money to the same scammer. If you are not satisfied with the response from your bank, you can seek free advice from the Australian Financial Complaints Authority https://www.afca.org.au/.
- **Report the call to Scamwatch** at https://www.scamwatch.gov.au/report-a-scam. Scamwatch uses the reports it receives to provide timely warnings about emerging scams and works with government and industry to try and disrupt and stop scams.
- **Get in touch with IDCARE** if you have given bank information or personal identifying documents to a scammer. IDCARE is Australia and New Zealand's national identity and cyber support service and can help you recover from a scam and protect yourself in the future.

  Call IDCARE on 1800 595 160 or visit their website https://www.idcare.org/.
- **Identify Scams** - There are some tell-tale signs that can help you identify a tax or super scam. Visit www.ato.gov.au/scams for further details