

SCAMS
AWARENESS WEEK

27 November–1 December

#ScamsWeek2023



Scams Awareness Week 2023

72.5% of scams reported to the National Anti-scam Centre via Scamwatch involve **impersonation** of a real organisation or person.

This makes these scams really **hard to spot**.

This year Scams Awareness Week empowers us all to **slow down** and think about who we're really dealing with before acting.



What is an impersonation scam?

Scammers can impersonate trusted businesses or people you recognise to steal your money or personal information.



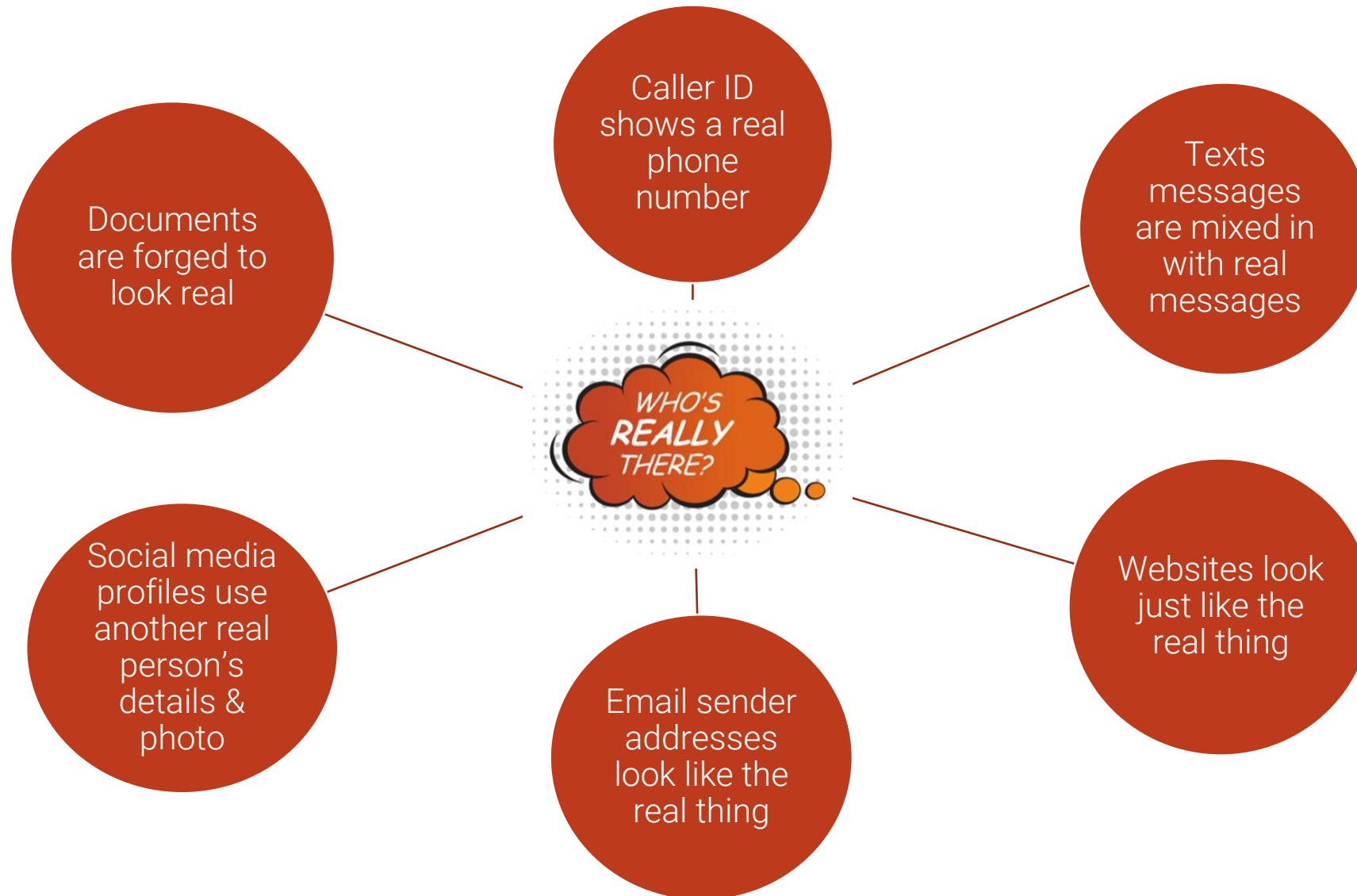
Impersonation scammers can reach you by lots of different ways like text, messaging apps, websites, social media, email or phone.



Scammers say they are government officials, well-known companies, charities, celebrities, law enforcement or even family and friends.



How scammers reach people





How to spot impersonation scams

- 🔍 **Urgent request** to provide personal details or money quickly.
- 🔍 Asks you to **click on a link** and provide your username, password, or personal information.
- 🔍 Tells you there has been an unauthorised transaction or **asks you to confirm** a payment that you didn't make.
- 🔍 Asks you to **use a different bank account** and BSB from the last payment you made.
- 🔍 **Threatens you** with immediate arrest, deportation if you don't pay money.
- 🔍 Asks you to **transfer money** to an account to 'keep it safe' or for 'further investigation'.
- 🔍 Presents an offer that looks **too good to be true**.

How to avoid impersonation scams



STOP

Pause before giving money or personal information to anyone.



THINK

Ask yourself: could the message, call or information be fake?



PROTECT

Independently check who you're dealing with and act quickly if something feels wrong!

NEVER AUTOMATICALLY ASSUME A PERSON YOU ARE DEALING WITH IS WHO THEY SAY THEY ARE.

Check who you're dealing with



Contact the person or organisation directly



Watch out for slight variations in Caller or Sender IDs and web addresses



Research people and organisations who you've only dealt with online



Check for the correct registration details of organisations through registers

KNOW WHO YOU'RE DEALING WITH BEFORE YOU GIVE ANY MONEY OR PERSONAL INFORMATION.

Bank impersonation scams



Mon, 10 Oct at 12:09 pm

[REDACTED], Congratulations your Home Loan has been conditionally approved. Please contact us when you are ready to proceed. Thanks [REDACTED]

Wednesday 10:53 am

Your purchase for \$780 to PAYPAL has been put under review, If this was NOT yourself, Get in touch with our team urgently on +61862340895 Mon-Sun 9am-9pm.

scam

Different phrases to other messages in thread

Sense of urgency

Unverified phone number

! Other warning signs:

- Suspicious looking links
- Tells you to transfer money to a different account to 'keep it safe' or for 'further investigation'

YOUR BANK WILL NEVER ASK YOU TO TRANSFER FUNDS TO ANOTHER ACCOUNT, OR FOR YOUR PASSWORD, PIN OR CODES.

Phishing scams



Text Message
Today 1:06 am

TRANSPORTATION
ALERT: Your travel bill
has not been paid.

Please process as soon
as possible: [http://](http://ewj.one/wCDJE)

ewj.one/wCDJE

Avoid high fines .

Urgent request for
action



Link to fake website



Threatening



! Other warning signs:

- Linked website asks for your username, password, or personal information
- Asks you to pay a different bank account and BSB than usual

NEVER CLICK LINKS ON TEXTS.

Fake retail websites



Link to illegitimate site →

Very low prices →

Broken links or filler text →

Sponsored

macpaoutdoor.com
https://www.macpaoutdoor.com

Hiking Shoes Clearance Sale - Save Up To 70% Off - Macpac Online

Outdoor clothing, hiking and camping gear on sale. New in puffer jackets & vest only AUD\$39

About Us

Beach Tents

Camping Tents

Ultralight Tents

! Other warning signs:

- Limited or unusual payment options
- Fake social media accounts
- Bad Independent reviews

ALWAYS ACCESS WEBSITES VIA AN INDEPENDENT SEARCH NOT VIA LINKS IN MESSAGES OR SOCIAL MEDIA

Celebrity endorsement scams



Sounds too good to be true



After week 4, I stopped using it because it was too effective

Images of celebrity do not relate to product



! Other warning signs:

- Link to fake site
- High pressure tactics
- Investment opportunity not supported by the proper licence

IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.



Support

Contact your **bank or card provider** immediately.

IDCARE on 1800 595 160.

National Debt Helpline online or on 1800 007 007.

Lifeline online or on 13 11 14 24

Beyond Blue online or on 1300 22 463

Protect your **friends and family** and tell them about your experience.

Reporting impersonation scams



30% OF SCAMS CURRENTLY GO UNREPORTED.

By reporting scams, you help protect others and we know where to focus efforts to disrupt and stop scammers.

Report the scam to the National Anti-scam Centre via [Scamwatch.gov.au](https://scamwatch.gov.au).

You can also make an official report to the police via cyber.gov.au.

Report scams to the digital platform where they were encountered to assist with removal of the offending content.

WHO'S REALLY THERE?

SCAMS
AWARENESS WEEK