



Impersonation scams



Impersonation scams can occur via email, social media, phone call or SMS and attempt to gain your personal or banking information by pretending to be a trusted organisation such as government, telecommunications providers, financial institutions, and other well-known businesses.

How to spot an impersonation scam

- Messages look incredibly genuine by using the same branding or formats.
- Messages appear in the same conversation thread or use the same phone number or sender ID.
- You receive a verification code you have not requested.
- The message contains a suspicious looking website link.
- You receive a generic notice of suspicious activity or fraudulent transactions.
- You're directed to a website via an unfamiliar looking link and asked for information you do not usually need to provide.
- The scammer requests personal or banking details or asks to confirm information they have (obtained fraudulently) such as full name, phone number, email address or residential address to imply legitimacy.

How to protect yourself

- Do not click on any links or open emails claiming to be from your bank or another trusted organisation.
- Never provide your personal, banking or credit card details if you receive an unsolicited call regarding an account. If in doubt, hang up and call the organisation directly via contact details you have sourced independently.

Scams continue to evolve and grow more sophisticated in their attempts to gain personal, banking information or access to devices.

Stop

Say no, hang up or delete suspicious messages. Take your time, trust your instincts and avoid giving out any personal information or money if you're unsure.

Check

Ensure the person you're dealing with is real. Contact organisations directly using contact details you find yourself. Verify investment offers through ASIC and confirm with family, friends or a professional before acting.

Protect

Act quickly if you're concerned you've been in contact with a scammer. Contact us immediately and help others by reporting scams to Scamwatch (www.scamwatch.gov.au) or the police (www.cyber.gov.au).

People First Bank will never contact you to request your passwords, VISA card or account details.

We will not send you SMS containing links. Never share your password or Online Banking login credentials.

If you have been contacted or are concerned about your privacy, please call us directly on **13 11 82** or visit a branch.