



Spot the red flags of phishing scams





Beat the scammers by knowing the scam

Scammers are contacting people through phone calls, text or email, pretending to be from trusted businesses, government departments, and even family and friends – all with the aim of tricking unsuspecting people into handing over their personal information and stealing their money or identity.

There's even technology that allows a scammer's texts message to appear underneath previous messages from real companies, which makes them even harder to spot.

Use our tips to learn how to outsmart the scammers to protect your money and personal information.

Spot the red flags

-  **Messages that don't address you by your name or say who they're from.** Scammers often use generic greetings and sign-offs. If they're pretending to be family, they may call you 'Mum' or 'Dad'.
-  **A sense of urgency.** Scammers might ask you to click on a link, scan a QR code or download an attachment to avoid a problem, like missing a parcel delivery, being fined or blocking your account. NAB will never ask you to provide your personal or banking information through a link.
-  **Contact details and web addresses that are slightly different.** These can be hard to spot, such as an email address or website with a '1' instead of an 'i'.
-  **Poor spelling and grammar.** This is usually an obvious sign, but scammers are getting better at copying the look of legitimate emails, including language, logos and branding.

Did you know?

Multi-Factor Authentication (MFA) is quick and easy to set up on your banking, email and online accounts. It adds extra steps to confirm your identity when you log in, such as your password plus a one-time code. So if a criminal has your password, they'll need additional information known only by you to log in. Learn more at nab.com.au/mfa.

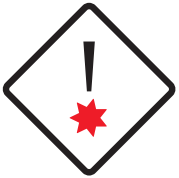


more
than
money



Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

If someone sends you a link, QR code or attachment – even if it looks like they're from someone you trust – **stop** to consider, could this be a scam?



Check before you share

If you're unsure if a message or call is legitimate, **check** the identity of the person who contacted before sharing any information. You can do this by calling the real organisation on their official, publicly-listed phone number.



Protect if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to **protect** your money and information, so if you think you've been scammed or your banking details have been compromised, call us on **13 22 65** and ask for our Fraud team.

Find out more

Visit nab.com.au/phishing.

