



# Phishing scams



Phishing scams occur when a scammer pretends to be from a trusted organisation such as telecommunications or internet providers, financial institutions, online retail, courier and delivery services and more, in an attempt to gain personal or financial information.

## How to spot a phishing scam

- You receive an unsolicited email, phone call, text message or instant message asking you to confirm or verify personal details or alerting you to suspicious activity on an account.
- You are asked to verify a payment that has been made from your account by verifying your credit card or bank details so the bank can investigate.
- The scammer recites your credit card number and asks you to confirm the security code.
- The message you receive has spelling or grammatical errors and the branding is slightly different from the legitimate organisation.

## How to protect yourself

- If you receive an email or message from a bank or trusted organisation, be wary of clicking links, particularly if the communication seems urgent or unusual.
- 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](http://www.scamwatch.gov.au)) or the police ([www.cyber.gov.au](http://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.