



Employment scams



Scammers target individuals by offering employment opportunities so they can steal money and personal information. These jobs often offer a high income with low or minimal effort – and sometimes the job does not exist at all. The scam often starts with a request for payment to start the role – be wary of any role that requires you to pay money to make money. These funds are often impossible to recover.

How to spot an employment scam

- The recruitment process is quick, with little focus on your qualifications, experience or references.
- You are told to top up an account with your own money or crypto currency to complete tasks.
- The job involves transferring money, making purchases or receiving packages on behalf of someone else.
- You are required to pay a 'recruitment fee' or pay for training materials before you begin the job.
- A recruiter contacts you out of the blue via text message or instant message service.

How to protect yourself

- Never send money or give your personal information, credit card or banking details or crypto currency account details to anyone you have only met online, through email or over the phone.
- Verify the employment opportunity by contacting the recruitment agency representative or via phone numbers you have sourced independently. Be aware that scammers often use trusted websites to post fake ads.
- Don't be pressured to act quickly. A legitimate offer won't require you to make a fast decision.
- Never send your passport or identity documents to an employer or recruitment agency unless you are certain they are genuine.

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.