









Spot the red flags of employment scams

Beat the scammers by knowing the scam

An employment or job scam is where a cyber criminal encourages you to apply for a position that doesn't exist. Job scams can take many shapes and forms and can have serious consequences. Some people have reported their identity being stolen after they provided their driver's license or passport, thinking it was part of the employment process. People have also unknowingly helped criminals to launder money.

If you're looking for a job, knowing how to identify a scam can help safeguard your money and identity details.

Spot the red flags

-  **Unexpected contact.** a "recruiter" contacts you unexpectedly through messages or an encrypted messaging platforms like WhatsApp, Signal or telegram about an exciting new opportunity.
-  **Promising high income for little effort.** You are told you can earn a high income while working from home with little effort, and it seems too good to be true, it probably is.
-  **Upfront fees.** To accept the job, you are asked to pay an "upfront fee" for a starter kit or training.
-  **Quick hiring process.** The recruiter schedules an interview to be done over the phone instead of via zoom or in-person and you are offered the job on the spot without discussion about your qualifications, experience and references.
-  **Request for identity documents.** You are asked to provide identity documents such as Driver's License, Passport, or Medicare details as a part of the initial application process.
-  **Commission based.** You are offered high commission just for transferring funds paid into your account to other channels. This may be offshore accounts or cryptocurrency or gift cards.



Stop, Check, Protect

to minimise your chance of being scammed



Stop before you act

If you receive an unexpected message or call from a 'recruiter' about an exciting opportunity with low effort and high returns, **stop** to consider, could this be a scam?

Never agree to receive or forward funds through your account as part of a job as these funds are likely from another scam victim and you could unknowingly be helping launder money



Check before you share

Check the company is legitimate by researching thoroughly and confirm the employment offer is genuine by contacting the organization directly using a publicly listed number. Ask the recruiter for references from other people who have worked there and make the effort to contact these people. Doing an internet search for reviews on the company can also help.



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/security

For more tips on protecting yourself, visit nab.com.au/employmentscams