

Introduction

Employment scams are designed for criminals to steal money, acquire identity credentials, or recruit unsuspecting individuals to launder money for criminal organisations.

Employment scams most commonly fall into two categories:

1. The employment opportunity and associated business is fraudulent and does not exist
2. The criminal is using the name of a legitimate business to advertise a job that does not exist

Fake employment advertisements can be found on legitimate employment websites and social media platforms. Before engaging, see our prevention checklist below.

Prevention checklist

How can I avoid an employment scam?

It is easy for scammers to copy logos and layouts from legitimate business websites or to create their own business and advertise roles that don't exist.

It is recommended you:

- ☐
 - Research the organisation, including using the ABN Lookup to confirm business registration and ABN status.
 - Call the organisation directly, using a number you find independently from the job advertisement or any communications received. Confirm the position advertised is legitimate and that the person you have been engaging with is genuine. Confirm the contact details they are using to communicate with are correct.
 - Look at the URL of the business website carefully and see if it uses unusual punctuation or numbers in place of similar letters (e.g. "1" instead of "l").
 - Do a reverse image search (for example, using Google or [Tineye](#)) of any images used on the business website, particularly of people. Do they appear under different names or positions on different websites?
 - Be wary of jobs offering high commissions, flexible hours, little or no experience required, on-the-job training, all while working from home.
- ☐ Keep track of all the jobs you apply for to reduce the risk of responding to job offers through phishing emails.
- ☐ Using a legitimate employment website for your job search does not guarantee the advertisement is real.
- ☐ Discuss the job opportunity with family and friends before applying.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist

If you are concerned that you or someone you know may be involved in an employment scam, this checklist may help.

The more boxes you tick, the more likely it's a scam.

- ☐ The role requires little to no experience, provides flexible hours, and is a remote working opportunity.
- ☐ The recruitment process is fast. There may be no interview conducted and your references were not contacted.
- ☐ You were required to provide copies of your personal identification documents, such as your driver licence, passport, tax file number, bank account details, prior to being offered the role or signing a contract.
- ☐ After submitting your documents, you do not hear from the recruiter again and they are unable to be contacted.
- ☐ You were required to make an upfront payment as part of the application or recruitment process, or before commencing your employment.
- ☐ The job requires you to receive money into a bank account in your name and then transfer those funds to other accounts, but you keep a percentage of the money as part of your commission – this is money laundering.
- ☐ You are allocated "daily tasks". The platform requires you to deposit money to complete these tasks, with the promise of a high commission once all tasks have been completed.
- ☐ You are added to a group chat, commonly on an encrypted or private messaging platform, with members who are employed by the same company and completing similar tasks. Members often share tips and how much money they are earning, but these are other scammers falsely endorsing the position.
- ☐ You receive payment after the first task has been completed (or first couple of tasks), then no further payments are made. You are unable to withdraw funds or told you need to complete all tasks or pay additional fees first. Even once all agreed tasks are completed you are still unable to withdraw funds.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document,

IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Detection checklist cont.

- ☐ The business offering employment is based overseas but may be looking at expanding into Australia or New Zealand.
- ☐ Your employer encourages you to recruit friends or families into similar roles.

Response checklist

If you or someone you know has been involved in an employment scam, the below checklist outlines some measures you can take to prevent further financial harm.

- ☐ Cease all communication with the scammer.
- ☐ Tell a trusted person what has happened if you need support as you work through the financial, emotional and practical recovery.
- ☐ Advise your bank(s) and superannuation company of the employment scam (if this information was provided).
- ☐ Notify the relevant document issuing organisations for any of the credentials that the scammer may have accessed. Common credentials include:
 - Driver licence
 - Passport (Australian passports contact [DFAT](#) on 131 232, for NZ passports contact [DIA](#) on 0800 22 50 50)
 - ATO details (Australian residents call 1800 467 033) or IRD details (NZ residents call 0800 257 777)
 - RealMe details (NZ residents call 0800 664 774 or online at [RealMe](#))
- ☐ If you have provided government issued identity documents, contact both credit reporting agencies for your [credit reports](#) and to request a [credit ban](#).

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Response checklist cont.

- ☐ If you have sent or received money or goods online, provided remote access to your computer, or shared credentials online that would enable identity theft and fraud, you can alert police through:
 - [ReportCyber](#) (in Australia)
 - Call 105 or [online](#) and choose "Report a Police non-emergency" (in New Zealand)
- ☐ Contact your GP if you feel you need additional support and strategies to deal with the stress of your situation.
- ☐ Be aware that you may see an increase in scam attempts.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.