

SMARTDAILY

Job scams: How to avoid falling victim to fake employment opportunities

Looking for work during a pandemic not only means more competition for jobs but also an increased risk of being scammed. These are the red flags to look out for to protect yourself.

Melanie Burgess, Careers deputy editor, News Corp Australia Network

Subscriber only | October 15, 2020 6:00am

Looking for work in a recession and pandemic not only means more competition for jobs but also an increased risk of being scammed.

Cyber criminals are targeting Australians with fake job advertisements on platforms such as LinkedIn, Facebook and online job boards as well as phishing emails to defraud, siphon money from bank accounts or steal personal data.

But there are critical steps you can take to avoid being ripped off by a too good to be true opportunity.

More than 2500 Australian jobseekers were scammed by fake job ads in the last year, convinced to hand over personal details in the hope of landing work that didn't exist.

It cost them a total of \$1.7 million, according to the Australian Competition and Consumer Commission.

And the number of victims is set to rise with hundreds of redundancy workers flooding the job market.

Between January and September 30 this year, ACCC's Scamwatch received 2190 reports of jobs and employment scams, up from 1955 reports over the same period in 2019.




📷 Pure Security's Arni Hardarson says resumes should not include too much personal information. Picture: Tim Carrafa

The most common contact method for scammers in both years was email.

In some cases, when a candidate responds to a fake job advertisement, criminals take advantage by sending documents infected with malicious software, according to Arni Hardarson, head of assurance at Pure Security, which runs security awareness training to stop people falling victim to online scams and cybersecurity attacks.

“The ads are purporting to be online profiles but are actually a way to distribute malware thorough drive-by downloads or other methods,” he says. “These can be used to initiate ransomware attacks.”



 Jobs360 is a special News Corp roundtable discussion focused on how Aussies can get back to work.

ACCC deputy chair Delia Rickard says another tactic used by scammers is to offer a job that requires an upfront payment from the applicant.

“The job on offer may require you to do something simple such as stuffing envelopes or assembling a product using materials that you have to buy from the ‘employer’,” she says.

“To accept the job you will be asked to pay for a starter kit or materials relevant to the job or scheme.


“If you pay the fee you may not receive anything or what you do receive is not what you expected or were promised.”

ACCC’s Delia Rickard and Pure Security’s Arni Hardarson have this advice to avoid being scammed:

1. CHECK THE ORGANISATION IS LEGITIMATE

“Cross reference that the prospective employer is real by looking at their website and other information online and do the same with recruitment firms,” Hardarson says. “If the recruitment company is real, they will have a profile on LinkedIn and staff will have profiles with detailed biographies and photos. If you can’t find the company easily, be very wary.”



 Australian Competition and Consumer Commission deputy chair Delia Rickard warns against accepting a job that requires a payment from the applicant. Picture: Supplied

Rickard advises not to deal with an employer or company that does not have a street address,

as they can be difficult to contact or trace.

2. LOOK OUT FOR RED FLAGS

“Always follow the golden rule, if it looks too good to be true, it’s most likely a scam or has malicious purpose behind it,” Hardarson says. “If it’s a fake advertisement, candidates will be sent information to download or links to click purporting to be online culture assessments and so forth.

“Spelling mistakes may indicate the scammer has a lack of knowledge of how recruiters normally present and market themselves in Australia.”

Rickard warns against any arrangement with a stranger that asks for upfront payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. She also advises suspicion of unsolicited “work from home” job offers, particularly if they offer a “guaranteed income”.

3. LEAVE OUT UNNECESSARY PERSONAL INFORMATION

“Job seekers should only include information within their CVs that is absolutely required,” Hardarson says.



📷 Reports of job scams have increased since COVID-19 sent more Australians into the job market. Picture: William West/AFP

“There is no need to include your full home address, the city and country is sufficient. It’s critical to ensure that no unnecessary personally-identifiable information is exposed in the CV.”

Rickard says scammers may ask job applicants to provide personal details for more information about a job but they should not do this.

4. KEEP SYSTEMS AND SOFTWARE UP TO DATE

Hardarson says it is important jobseekers keep their computer operating system up to date, and ensure antivirus software is scanning attachments before they reach their inbox.

“The same applies to mobile devices,” he says.

MORE FROM JOBS 360:

[Where you can find a job in Victoria right now](#)

[Where you can find a job in Queensland right now](#)

[Where you can find a job in NSW right now](#)

[Where you can find a job in SA right now](#)

[Where you can find a job in the NT right now](#)

[Where you can find a job in Tassie right now](#)

Originally published as **['Be very wary': How to spot a fake job ad](#)**