

Tips for Spotting a fraudulent job

Landing an internship or job can be stressful enough without finding yourself involved in a scam. It may not be possible to spot every bogus job, but here are some signs that the announcement isn't above board:

- You must provide your credit card, bank account numbers, or other personal financial documentation. Do NOT give out any financial information at any point during your job search and hiring process.
- The posting appears to be from a reputable, familiar company (often a Fortune 500). Yet, the email handle in the contact's email address does not match the domain used by representatives of the company (this is typically easy to determine from the company's website). Another way to validate is to check the open positions on the company's website, by checking their careers/jobs page.
- The contact email address contains the domain @live.com or an @ that is not affiliated with the company. Example: @gmail, @yahoo, @hotmail, etc.
- The position requires an initial investment, such as a payment by wire service or courier.
- The interview is conducted online, via chat and an offer is given almost immediately.
- The posting includes many spelling and grammatical errors.
- The position initially appears as a traditional job. Upon further research, it sounds more like an independent contractor opportunity.
- You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
- You receive an unexpectedly large check (checks are typically slightly less than \$500, generally sent or deposited on Fridays).
- You are asked to provide a photo of yourself.
- You are asked to provide your social security and driver's license information in the initial application. Personal information should never be asked during the initial application process.
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, or Online Surveys.
- The posting neglects to mention the responsibilities of the job. Instead, the description focuses on the amount of money to be made.
- The employer responds to you immediately after you submit your resume. Typically, resumes sent to an employer are reviewed by multiple individuals or not viewed until the posting has closed. Note: this does not include an auto-response you may receive from the employer once you have sent your resume.
- The position indicates a "first-year compensation" that is in high excess to the average compensation for that position type.
- Look at the company's website. Does it have an index that tells you what the site is about; or does it contain information only about the job in which you are interested? Scammers often create quick, basic web pages that seem legitimate at first glance.
- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc., this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well hidden.
- The salary range listed is very wide (e.g., "employees can earn from \$40K – \$80K the first year!").

- When you Google the company name and the word “scam” (e.g., Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is <http://www.ripoffreport.com>.
- Google the employer’s phone number, fax number, and/or email address. If it does not appear connected to an actual business organization, this is a red flag. You can use the [Better Business Bureau](#), [Hoovers](#) and [AT&T’s Anywho](#) to verify organizations.
- The employer contacts you by phone, but there is no way to call them back (the number is not available).
- The employer tells you that they do not have an office set up in your area and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).

If you believe you have applied to a fraudulent job or internship posting you should immediately contact the local police. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state). Notify ESU Career Services so that the appropriate steps can be taken to protect other students.

If it is a situation where you have sent money to a fraudulent employer, you should contact your bank or credit card organization immediately to close the account and dispute the charges. If the incident occurred completely over the Internet, you should file an incident report with: <https://www.cybercrime.gov/>, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

In a nutshell – if the announcement seems too good to be true, or your instincts tell you that something isn’t right, then don’t apply. A healthy amount of scepticism is a good thing and if you have any doubts, contact Career Services.