

Fraudulent Job Posting: Red Flags

Here are some fraud warning signs:

Financial/Personal Information

- 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.
- 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 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).
- 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 to deposit into your bank account.
- Remember, never process ANY financial transactions. For example, some organizations offer opportunities to "make quick money." They will offer a "one-day only special." Their intent is to defraud you by sending or wiring money to your bank account. They will ask you to cash the check or send the monies to other accounts. Once your bank or financial institution processes the scammer's check or financial request, you may be informed the monies are invalid or "not real." In the meantime, you are held responsible for the funds the bank has sent at your direction to other accounts.

Unusual Salary

- The position indicates a "first-year compensation" that is in high excess to the average compensation for that position type.
- The salary range listed is very wide (e.g., "employees can earn from \$40K – \$80K the first year").
- The position initially appears as a traditional job. Upon further research, it sounds more like an independent contractor opportunity.

Website, Email Address, and Social Media Verification

- The posting appears to be from a reputable, familiar organization (often a Fortune 500). Yet, the email handle in the contact's email address does not match the domain used by representatives of the organization (this is typically easy to determine from the organization's website). Another way to validate is to check the open positions on the organization's website by checking their careers/jobs webpage.
- The contact email address contains the domain @live.com or an @ that is not affiliated with the organization. Example: @gmail, @yahoo, @hotmail, etc. If this is the case, then verify that the email address matches what is found on the organization's website.

- Does the organization's website 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 basic webpages that seem legitimate at first glance.
- Watch for anonymity. If it is difficult to find an address, actual contact, organization name, etc., this is cause to proceed with caution. Scammers will try to keep themselves well hidden.
- The employer contacts you by phone, but there is no way to call them back (the number is not available).
- Use social media to research each employer, e.g., Facebook, Twitter, Snapchat, and LinkedIn. Research the organization on websites such as Glassdoor.com for feedback and complaints.

Other Red Flags

- 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 posting includes many spelling and grammatical errors.
- The posting neglects to mention the responsibilities of the job. Instead, the description focuses on the amount of money to be made.
- Be cognizant of unsolicited emails that are not specifically directed to you. Spammers/scammers can obtain student emails fairly easily. If the unsolicited email references a referral from your career center, contact your career center to verify the employer.
- When you Google the organization name and the word "scam" (e.g., Acme Company Scam), the results show several scam reports concerning this organization. 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 [Anywho](#) to verify organizations.
- Fraudulent employers are phishing for the unsuspecting, including you. Be aware of what you share and post online. If you feel uncomfortable or are not sure about certain organizations or individuals claiming to represent an employer, talk to your career center.
- [Read more tips](#) on identifying fraudulent employers from the National Association of Colleges and Employers (NACE).

What to do if caught in Scam

- Immediately contact campus police
- Contact the RCPD or OCA so the posting can be removed and other students can be notified
- End all communication with the employer.
- Get in touch with your bank or credit card company and dispute any fraudulent activity immediately
- Depending on what personal information was disclosed, monitor or close your accounts.
- Depending on the situation, you may need to notify the three credit bureaus: Experian, Equifax and Transunion.
- If the incident occurred entirely over the internet, file an incident report with the FCC at <http://www.cybercrime.gov>