

Protecting yourself from Fraudulent Employers

"Earn \$3000 in one day"

Either you have an ambitious New Year's resolution or you've come across what is most likely a fraudulent job posting. Unfortunately, in today's market, fraudulent postings are becoming more prevalent, whether you're finding jobs through Hamline Career Link or another site. Earlier this year, system enhancements were implemented within Hamline Career Link that have significantly reduced the number of fraudulent postings. These enhancements combined with the vigilance of our office, have stopped several repeat offenders from entering jobs in our system. However, these measures are not fool proof. In an effort to help you identify potential warning signs, review the list below and use it when evaluating job and internship postings and email you receive.

Fraud Posting Red Flags

- You must provide your credit card, bank account numbers, or other personal financial documentation.
- The posting appears to be from a reputable, familiar company (often a Fortune 500). Yet, the domain 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.
- The contact email address contains the domain @live.com.
- The position requires an initial investment, such as a payment by wire service or courier.
- 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.
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys.
- The posting neglects to mention what the responsibilities of the job actually are. 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 you are interested in? Scammers often create quick, basic web pages that seem legit 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 (i.e. "employees can earn from \$40K - \$80K the first year!")
- When you Google the company name and the word "scam" (i.e. 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 (<http://www.bbb.org/us/consumers/>), Hoovers (<http://www.hoovers.com/>) and AT&T's Anywho (<http://www.anywho.com/>) to verify organizations.
- The employer contacts you by phone; however, 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).

Let us know

If you see a position in our system that you believe may be a scam, please notify our office immediately! If you receive an email that meets any of the following criteria, do not respond - delete the email.

Beware if the email:

- *does not indicate the company name*
- *offers to pay a large amount for almost no work*
- *offers you a job without ever interacting with you*
- *wants you to transfer money from one account to another*
- *offers to send you a check before you do any work*
- *asks you to give your credit card or bank account numbers, or copies of personal documents - but you get nothing in writing*
- *says you must send payment by wire service or courier*
- *offers you a large payment or reward in exchange for allowing the use of your bank account - often for depositing checks or transferring money*
- *sends you an unexpectedly large check*

Additional Resources

- <https://www.bbb.org/council/news-events/bbb-warnings/2017/09/phishing-scam-claims-to-be-from-bbb-cites-federal-violations/>
- <https://www.thebalance.com/list-of-fake-job-scam-examples-2062168>
- <https://www.bbb.org/nashville/news-events/bbb-in-the-news/2017/06/bbb-warns-scammers-target-job-seekers/>

If you have any questions or concerns about fraudulent postings, please contact our office:

Career Development Center

Drew Science, Room 113

651-523-2302

workshop@hamline.edu