CAREER & CO-OP CENTER

Avoiding Job Scams

UMass Lowell and Handshake make reasonable efforts in reviewing job postings and employers for potentially fraudulent job postings or inappropriate recruiting practices. Students and alumni are responsible for researching any opportunity that interests them by reading information about the organization, visiting the organization's website, searching for the organization on the internet, or asking questions during the interview.

Fraudulent Posting Red Flags

What are fraudulent posting red flags? Here are some fraud warning signs:

- 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 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 the Ripoff Report website.
- 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, Hooversand 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 come across any suspicious employer job postings, cease any communication with that employer and alert UMass Lowell's Career & Co-op Center by email career_services@uml.edu or call 978-934-2355.

What if I Am Already Involved in a Scam?

The Federal Trade Commission (FTC) suggests the following instructions:

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). If you are a current student, you may file a report with the UMass Lowell's University Police by calling them at 978-934-2398.

Visit the Federal Trade Commission's IdentityTheft.Gov website for step-by-step recommendations to protect yourself.

If it is a situation where the student has sent money to a fraud employer, the student should contact their bank or credit card organization immediately to close the account and dispute the charges.

If the incident occurred completely over the Internet, the student should file an incident report with the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS), or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).