UNIVERSITY OF TORONTO

Fraud on Job Boards: Things you need to know!

Unfortunately, job posting scams are on the rise. The University of Toronto reviews job postings that appear on CLN by checking for the legitimacy of email addresses and websites provided by employers, we do not always catch clever scammers. Therefore, **students need to exercise caution and common sense when responding to any job posting and even after you have accepted a job.**

Common Themes in Job Board-Related Fraud

Scammers are typically trying to a) convince you to send them money, or b) steal your identity so they can obtain credit in your name. These fraudulent postings and "job offers" typically involve the "employer" asking the candidate/job seeker to do one of the following:

- Send money from your own bank account to the "employer" (for pre-employment screening, training, or materials/software) via wire transfer, money order, or Interac e-Transfer; you never hear from them again and the money is not recoverable.
- Deposit an "employer" cheque into your personal bank account, immediately withdraw the funds, run minor errands for the employer and send the unspent money (from a few hundred to several thousand dollars) back to the employer; a day or two later, your bank calls to tell you that the cheque was a fake, and you are now responsible for repaying paying the lost money to the bank.
- Provide detailed personal information as part of the application process; the "employer" then uses the information to steal your identity and take out credit in your name, thereby damaging your credit history.

Before accepting a job offer, YOU SHOULD …

- ***Have an interview!*** It could be in-person or via Skype. Look for signs of legitimacy: the company has a website, office location and the person you meet with provides you with a business card to show you that they work there. In some cases, employers who are hiring for home-based businesses may not an office location but should be able to verify their legitimacy website and contact information.

As part of being offered a job, you should receive verbal and written notification from the employer. Typically employers will provide you with a contract with terms of employment including details such as date of employment, rate of pay, job responsibilities.

Before accepting a job offer, YOU SHOULD NOT…

- Provide financial information (debit card number, credit card information, etc)
- Provide a copy of your bank account information
- Provide your Social Insurance Number
- Provide a copy of your student ID card, driver's license, or passport

Fraudulent Job Posting/Hiring Examples

(adapted from http://jobsearch.about.com/od/jobsearchscams/a/fake-job-scams.htm)

UNIVERSITY OF TORONTO

Other things to look out for

Pay for Background Check Scam:

With this scam, a job seeker is told a position has just opened up and an over the phone interview is conducted. The applicant is notified that they would be responsible for the cost of the background check. Then the applicant is told that they have to purchase pre-paid $75 Visa debit card and send it to the interviewer to pay for the background check. No legitimate company would ask for this.

Pay for Software/Programs or Pay for Online Training Scam:

The company asks applicants to set up a Yahoo Messenger account for the job briefing and interview. The company then explains that the applicant will need to buy software/training program in advance and say they will reimburse the candidate. They do not reimburse the candidate.

Credit Report Scam:

Here's an email sent to a Craigslist applicant: Company would like to take this moment to thank you for your response to our Craigslist job posting, as well as inform you that, after reading through your resume, we are interested in discussing this job opportunity with you in person. In order to proceed to the next step of the hiring process you will need to get your credit score checked. The applicant is directed to a website where they will input personal information including name, address, social security number… enough to steal an identity. No legitimate company needs a credit check **before** an interview.

Fake Job Application Scam:

This email asks to complete a job application online. The link takes the candidate to a website where you are to fill out all info needed to steal your identity (e.g., date of birth, credit card information, social insurance number). The email says: "We look forward to reviewing your application and bringing you in for an interview, but cannot do so until you complete our company application." Employers only need information to contact you for an interview at the application stage. Information to verify your eligibility to work will only be asked when registering as an employee.

Direct Deposit Before Interview/Trial Employment Scam:

The applicant is offered the job as a "trial period" via email and told that all employees are paid via Direct Deposit with the company's banking institution - no additional cost for you. The applicant is sent to a website to sign up and told: "After registering your Direct Deposit confirmation, please respond back to this email with your ideal interview date/time. Remember, you need your Direct Deposit account info prior to your interview, as we will be processing your payment information at that time." No legitimate employer needs to know how to pay an employee before they have even interviewed the potential employee.

If you are caught by a Scam…

Get in touch with your bank or Credit Card Company and dispute any fraudulent activity immediately!

You may report the incident and gather additional advice here:

Canadian Anti-Fraud Centre:
http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm
Consumer Protection Ontario:
https://www.ontario.ca/page/report-scam-or-fraud

If you see a suspicious job posting in the Career Learning Network, email us careers@utoronto.ca

Some of the content for this document were collected from Queen's University and Brock University