Recognizing and Protecting Yourself from Job Posting Scams

Understanding Job Posting Scams

In an attempt to access personal information (bank account information, SIN, or identity) and/or attempt to get money from you, experienced con artists, posing as recruiters or employers, create fraudulent job postings. Employment scams are often promoted through online advertisements, unsolicited emails, or in newspaper ads. Typically, scam postings promise a lot of income—or even guarantee it—for little or no effort.

Assessing Job Postings

When in doubt, get the job description from the company's official website. Job posting scams often capitalize on well-known companies' names and images. Always verify the legitimacy of the job posting by reviewing the "official" employment page to confirm the opening is real. Refrain from following a link from a suspicious posting. Often scam links will take you to a similar looking page. If you are still unsure after visiting the company's website, call the company in question using publicly-available contact information and ask questions about the job opening. If there is no phone number given for the company, do not pursue the opening.

Job seekers using online job postings or responding to "employment" emails should always exercise caution and common sense. It is very important that you know what to look for and always research all job postings carefully. This includes **all** job postings, whether they appear in **MyCareer** job postings, at Queen's University (through classes or common areas), on other online bulletin boards, or through unsolicited emails.

While we thoroughly screen all postings to MyCareer, you should still be alert if you encounter anything concerning.

Red Flags

Warning signs of possible fraudulent emails and websites include:

- Poor grammar and spelling
- Requests for personal information
- Difficulty contacting or identifying the person posting
- You are contacted by phone, but the number is not available
- Posting contains vague descriptions that focus on the money rather than the job
- Email domain (the @123corp.com part of the address) does not match the company's official website domain (ex. queensu.ca is correct, whereas queens.ca is not. Check for discrepancies.
- Email domain of a free provider is used (real companies almost always have their own email systems) i.e. @live.com, @yahoo.co, @hotmail.com, etc.
- Website includes information only about the job for which you are applying, rather than also including general company information
- You have been made an offer without having submitted a resume or participating in an interview
- Requests for an initial investment from you or for you to cash cheques and wire money
- Request for access to your bank account

Types of Scams

The frequency, complexity, and variety of employment scams are on the rise. Below you will find examples of four common employment scams.

Payment Forward Scams

After you apply for a "position" or reply to an e-mail the bogus "employer" replies with instructions to complete a task. The task: you receive a cheque in the mail with instructions to deposit the cheque into your account, and send a percentage, via wire transfer, to another person. The employer promises that you will keep a percentage. This scam is sometimes referred to as a "money mule," posted under the titles of "financial manager", "payment processor", or "transaction specialist".

Do not accept the cheque. The cheque will bounce and you, the job seeker, will lose whatever money you sent to the "employer". The Car Wrap Advertising scam is a recent popular variation on the cheque scam.

Application Fee or Training Scams

These scams charge you an "application fee" or ask you to pay for "mandatory training" in exchange for "guaranteed" employment. The cruise line and postal service industry and security officers have been used as pawns in this scam. The Security Job Scam is a recent example. Job positions are not guaranteed on paying application and training fees upfront.

Phishing Scams

Unsolicited emails or texts from "employers" declaring that they are responding to your posted resume are typically examples of phishing scams. They will often state that your skills match the position that needs to be filled, but they need more information from you. The information they are seeking is often personal information, which can be used to steal your identity. Refer to this RCMP link for more information on E-mail phishing. The following is an email example that was recently brought to our attention:

> *To: XXXXXXXX*
> *Subject: Work At Home*
> *We are pleased to inform you that vacancies exist in our foreign department as offshore representatives. We would be very glad if you accept to be appointed and earn 10% of every payment made through you to our office. There is no Advance fees involved. Subject to your satisfaction you will be given the opportunity to correspond with our customer(x). Send your Name, Address and telephone number for more details.*
> *Regards,*
> *Davis Frost*

Mystery/Secret Shopper Scams

There are legitimate mystery shopping companies that hire college students and others to provide feedback to retailers and restaurants. Unfortunately, many mystery shopper postings are scams. This scam also occurs through unsolicited emails or via online job posting boards. Typically, the "company" asks you to pay a fee to become an "employee" or "mystery shop" a money transfer company and complete a money transfer. See a recent example from The Windsor Star

If a job sounds too good to be true, it almost certainly is…
don't pursue it without diligent research

Legitimate employers will not…

- Ask for your bank account details or you SIN prior to a job interview, job offer and/or acceptance.

Prior to a legitimate job acceptance, don't

- Provide financial information
- Provide a copy of your driver's license
- Provide a copy of your SIN card
- Provide a copy of your Student ID

What to do if you are caught by a Scam

- Immediately contact the RCMP and file a report with the Canadian Anti-Fraud Centre 1-888-495-8501
- File a complaint with Consumer Protection Ontario
- Assess how much of your personal information has been shared
- Get in touch with your bank or credit card company and dispute any fraudulent activity immediately
- If you saw a suspicious posting anywhere at Queen's, contact Career Services mycareer@queensu.ca even if you haven't applied to the posting, please report it!

For further information on recognizing and protecting yourself from job posting scams:

Better Business Bureau
Beware of Employment Scams
bbb.org/article/tips/12261-bbb-tip-employment-scams

Competition Bureau Canada
The Little Black Book of Scams: your guide to protection against fraud, The Canadian Edition 2012
http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03074.html

Federal Trade Commission, Consumer Information
Job Scams
http://www.consumer.ftc.gov/articles/0243-job-scams

Queen's University Information Technology Services - Cybersecurity Education and Awareness Program
https://www.queensu.ca/its/security/security-services/cybersecurity-education-awareness