Be Empowered: Know the Red Flags that may Indicate a Job/Internship is Fraudulent

Although the vast majority of internships and job postings are legitimate, it is very important for students to know the warning signs to watch for. Scams can appear on legitimate sites such as Handshake, indeed.com, LinkedIn etc. Just because it is on the site, does not mean the posting/employer itself is legitimate. Some postings may be using the information of a real company but the contact information is directing you to a scammer or the scam may even come from the QCC email of another student or staff member, whose account was hacked. Students should notify the Career Services Office if they have any concerns by calling (**718.631.6297) or emailing careerservices@qcc.cuny.edu**. Being notified about negative internship/job experiences allows us to prevent other students from applying in the future.

CUNY Cybersecurity Awareness for Students

CUNY has launched a 25-minute interactive Cybersecurity Awareness for Students that is tailored to CUNY students and features a CUNY student. This course helps you gain a comprehensive understanding of the cybersecurity risks we all face, along with some best practices for safeguarding your data, so you can avoid opening the wrong link or attachment. You can find this course in Blackboard under your Organizations section. Please spend 25 minutes to learn how you can protect yourself against online threats. This brief time investment could protect you from serious financial, privacy or data loss consequences later on.

BEFORE RESPONDING TO A JOB AD or EMAIL ABOUT A JOB: STOP AND REVIEW THE FOLLOWING

- **Legitimate employers will not** ask for your bank account details or your SSN prior to a job interview, job offer and/or job acceptance. They will **not** ask you to send money or to deposit money.
- **Prior to a legitimate job acceptance, don't:** Provide financial information, a copy of your driver's license, a copy of your SS card or a copy of your Student ID.

READ THIS ARTICLE! LOOK OUT FOR THE RED FLAGS BELOW

The list below does not necessarily mean the position or company is not legitimate but it should cause you to do deeper research before proceeding. You might want to use this checklist as a way to screen postings/employers. Even if the posting is for a known company the scammer can be using their information to appear like a legitimate posting.

How They Contacted You/Want You to Contact Them (BIG RED FLAGS)

- You receive an email from someone you do not know. It may even appear to come from a student's school address.

- The posting forwarded to you says to use your personal email to respond and not your school email or they email you at your school email address but ask you to email them from a personal email to try to avoid the school's spam filters.
- The employer uses a personal email account to communicate. Be leery of those wanting to communicate on Google Hangouts, Skype, Glip or through text.
- The email came from one address such as a QCC email but after you respond they are emailing from a different email address.
- You did not apply for the position (this may happen but it is best to call the company to make sure it is a real person). **Tip: be careful what information you post on job search sites. Even legitimate sites can have scam job postings.**
- Contacts you via LinkedIn, or another social media outlet **(While this can be legitimate, you should always try to call or email the company's Human Resources department, to find out if they really have such a job opening and, if the name of a recruiter is given, ask if that person really works for them). For entry level jobs they usually won't reach out to you.**
- The organization uses street canvassers.
- The employer uses an e-mail address or website that may look legitimate but differs slightly from the real organization's e-mail address and/or website (one letter off). Or is pretty different from the URL of the company or emails listed on the site (might even say the company name but does not match the rest). The phone number or address does not match the company.
- They use an atypical way to contact you or to conduct the interview. An email should be reaching out to you via a professional email or phone number.

The Recruiter (BIG RED FLAGS)

- Difficult to contact or identify the person who posted the position. **Tip: Check on LinkedIn to see if the person is there** but even if you find the person's name on LinkedIn the scammer may be just using their name.
- The employer makes inappropriate comments or has unprofessional behavior during the interview or after.
- The employer asks illegal interview questions.
- The employer makes a job offer over the phone or via email without an interview.
- The employer requests for an interview during non-business hours.

Information They Ask For/Instructions Given (BIG RED FLAGS)

- The employer asks for your social security number or other personal information such as a copy of your ID, mailing address, and bank information especially before hiring you or interviewing you.
- Asks you to send money or to deposit money.
- Employment agencies that charge a fee; some legitimate agencies do charge but it is best to do a lot of research before paying.

Company/Job Details

- The organization has no established website.
- There is a generic description of what the company does, and not what the intern/employee will do.
- Limited details about the organization are available in the posting or online when you do research.
- You might even get something that looks legitimate, has their logo, address etc. but read the document carefully to see if what is written makes sense, has proper spelling and grammar.
- An internship is unpaid but does not comply with DOL's Guidelines for Unpaid Internships.
- The organization posted an internship after mid-semester when it is too late to make arrangements for academic credit.
- Be cautious of startup organizations; some can be unorganized and not in compliance with DOL guidelines.
- You are set to work in a home office or residence versus a business office setting - the internship/job can also be virtual where you work from home.
- The opportunity sounds too good to be true. An example of this can be the organization offers a high hourly rate or salary.

Examples of emails that look like they may be legitimate but are scams:

- **(sent to a QCC staff member)** My name is Alexandra, i am an Alumni of Queensborough Community College. I have an Uncle Doctor Paul <last name> who is moving to the College area, he needs someone to watch, bath and walk his dogs, he is offering $300 weekly. If you know a student who might be interested in this position have them email him via <different email address>. To make sure he sees their respond, interested student should message him from their personal email address.
- **(sent to a QCC student from another QCC student's email or appears to come from a QCC student's email)** I'm Denny <last name>. from Indeed. I am in urgent need of a Personal Assistant/Errands person (part-time) Pay is $500/week. Interested? Write to <different email address> from your personal email for more details about this job.
- **(sent to a QCC student through someone who got their email from LinkedIn)** You are welcome to <*name of real company*> Pharmaceuticals telecommute position, attached to this Email entails the company details and the job briefing of the position. I would like to chat with you for about 40-55 minutes to learn more about your background and what you are looking for in a career. To setup an interview, you are required to follow up by following steps below.

  Step 1.Download RingCentral application for your device (glip.com) on your PC, smartphone, IOS/Android.

  Step 2. Create an account using your existing email to create a username and password.

  Step 3. Add me to your contact using my email (barbara@careers-*name of real company*.com) after you might have created your account.

  Step 4. Send me your Interview Code: "PF501180" once you are set up.

  Let me know what time works best for you to interview. Note: This is a work from home position and you can work from anywhere within the states. Full training will be offered to

you. You are also welcome to apply for part-time, keep your other jobs and still enjoy full benefits.

Signed with name of actual employee from company (found on LinkedIn)

Types of Scams:

Never accept a check or any kind of funds from a company to purchase materials necessary for your position or send money. 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 check in the mail with instructions to deposit the check 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 check. The check will bounce and you, the job seeker, will lose whatever money you sent to the "employer". They will ask you to deposit a check, transfer some of the money to someone else or to purchase other items. But in reality, the money received is stolen, often the result of fraud on accounts, and is then laundered to overseas bank accounts.
- **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, postal service industry and security officers have been used as pawns in this scam.
- **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.
- **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" If a job sounds too good to be true, it almost certainly is…don't pursue it without diligent research.

What to do if you are caught by a Scam:

- Assess how much of your personal information is potentially out there.
- If they sent you a check, destroy it and let them know you are no longer interested in the position.
- Get in touch with your bank or credit-card company and dispute any fraudulent activity immediately.
- If you received the scam through your QCC student email or another QCC source notify the Office of Career Services so we can alert other students.
- Review the FTC's article on what to do if you were scammed

What to do if you experience Discrimination/Sexual Misconduct on an Interview?

- Review CUNY's Policy on Equal Opportunity and Non-Discrimination.

- Review Queensborough Community College's Sexual Misconduct Information and Resources available to you.
- Report it to the Office of Career Services.

For further information on recognizing and protecting yourself from job posting scams view the following links:

- Better Business Bureau
- Federal Trade Commission, Consumer Information
- Hoax Slayer
- Labor NY
- Protections for INTERNS in the Workplace
- The Muse - Job Scams Are on the Rise - Here's How to Spot them and Steer Clear
- The Balance Top Job Scam Warning Signs
- NACE Fraudulent Employers

Note

Queensborough Community College does not endorse or recommend employers, and a posting does not constitute an endorsement or recommendation. The College explicitly makes no representations or guarantees about job or internship listings or the accuracy of the information provided by the employer. The College is not responsible for safety, wages, working conditions, or any other aspect of off-campus employment without limitation. It is the responsibility of students to perform due diligence in researching employers when applying for or accepting off-campus paid or unpaid employment and to thoroughly research the facts and reputation of each organization to which they are applying. Students should be prudent and use common sense and caution when applying for or accepting any position.