Avoiding Job Scams: Staying Safe During the Job Search

Avoiding job scams: Staying safe during the job search

Unfortunately, not all employment opportunities are legitimate. "Scammers" are individuals or groups with malicious intent who may pose as companies hiring interns and full-time employees, and they may use realistic-looking but fraudulent job postings and direct-email campaigns ("phishing") to target students and others.

The scammers may put together a basic job/internship posting, website, interview, and offer letter, but **scams do not result in an actual job/internship.** Instead, job-search scams often involve a scheme to take money from unsuspecting job/internship candidates. **Scams may result in a financial loss for participating individuals.**

We periodically remind students about the existence of scams, to be vigilant when responding to job opportunities and job offers, and to speak with a Career Coach with any suspicions about the legitimacy of a job posting, job offer, or job communication.

Brandeis University's career centers, including the Career Strategies and Engagement Center, review and approve or decline new employer registrations on Handshake, and non-approved employers are unable to see resumes of Brandeis students via Handshake. However, scammers can find other ways to identify email addresses and/or to post positions on other job sites.

An example of how a scam might work:

- The scammer posts online jobs, or emails a student directly about job opportunities
- At some point in the process, the student receives a check in the mail as payment and is asked to deposit the check into their personal bank account - the check appears legitimate but is counterfeit
- The scammer directs the student to withdraw funds from their personal bank account, and to send money to another person for materials or software deemed vital for the job
- The result is that the scammer withdraws from, or depletes, the student's personal bank account

Some examples of "red flags" (signals that something is wrong) you should look for when responding to job correspondence:

- Misspellings, typos, sentences, or demands in the job posting, job offer, or job communication that don't quite make sense
    - Employer's email address is from a general email domain (for example, Gmail or Outlook) and does not match the company's website name or domain
    - Employer is willing to hire you without an interview; they may claim to be traveling for business
    - Position initially appears to be with a traditional job/organization, but turns out to be an individual contractor - the address may be a residential address rather than an office building
    - Internship employer hesitates to comply with offer letter requirements as listed in the Brandeis CPT Application Checklist (https://www.brandeis.edu/isso/documents/current/employment/curricular-practical-training/application...)
- Requirement to deposit a check into your personal bank account, then wire or transfer money to someone else
    - 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 will receive a check (maybe an unexpectedly large sum) in exchange for services rather than for performing typical job responsibilities - for example, you are asked to make specific purchases and then send them to another party
- Requirement to share private financial or personal information, such as credit or debit card numbers, PINs, passwords, birthday, address, mother's maiden name

Whom to contact if you become involved in (or suspect) a scam:

- Contact **Brandeis University Campus Police at 781-736-3333 immediately** if you have engaged with a scammer
- Contact **your financial institution immediately** to confirm steps to secure your account If a scam has involved your bank account in any way
- Consult the **Brandeis University phishing awareness website** at **https://www.brandeis.edu/its/services/information-security/phishing.html**
- Forward suspicious phishing or employment scam emails to **security@brandeis.edu** (Brandeis Library & Technology Services) and **phishing@brandeis.edu** (Brandeis Information Technology Services)
- Report suspicious job postings, job offers, job communications, or Handshake postings to your **Career Coach and/or Program Advisor**
- Report instances of fraud to FBI Internet Crime Complaint Center, IC3 at **www.ic3.gov**

Please refer to the sources below to learn more about job scams:

Federal Trade Commission resource regarding the signs of a job scam:
https://www.consumer.ftc.gov/articles/0243-job-scams

How to stay safe on Handshake:
https://support.joinhandshake.com/hc/en-us/articles/115008792627-Understanding-Job-Postings-How-to-Stay-Safe-on-Handshake

What to do if you've given your personal information to a fraudulent employer:
https://support.joinhandshake.com/hc/en-us/articles/115011570487-What-To-Do-If-You-ve-Given-Your-Personal-Information-To-A-Fraudulent-Employer-?source=search&auth_token=eyJhbGciOiJIUzI1NiJ9.eyJhY2NvdW50X2lkIjo5ODc1NjcsInVzZXJfaWQiOjM4MDI2MzkwMTQ3MywidGlja2V0X2lkIjo0MjQ1MjEsImNoYW5uZWxfaWQiOjYzLCJ0eXBlIjoiU0VBUkNIIiwiZXhwIjoxNTg5MDYwNzEzfQ.0F9JGwwDxTzrFYkbXnSwE0oJ2vTrbKcYF72BUDCp_zw

Your Career Coach and the Career Strategies and Engagement staff (globalcareers@brandeis.edu) welcome any questions about these topics. Thank you!