JOHNS HOPKINS
CAREY BUSINESS SCHOOL

Career Development

AVOID SCAMS & FRAUD

While Johns Hopkins University does not knowingly accept fraudulent job postings into the Handshake system, unfortunately, fraudulent job postings may surface. Scammers find job seekers through other job search platforms and tactics. Fraudulent job listings are typically used to illegally collect personal information and steal money from job seekers. If you see a questionable job posting, please contact the Career Development Office.

Clues a Job May be Fraudulent

It is very important for you to educate yourself about potential scams. Here are some things to know when job seeking:

- Do not accept checks or money transfers sent to you to cover the cost of training materials, software or equipment (printers, laptops, etc.) before you actually start a job.
- Do not send money for a job, job search or training materials. If an offer requests money transferred via money order, PayPal, Venmo, or any other online payment platform, do not proceed.
- An employer will not make an official job offer before meeting or interviewing you.
- Do not provide a Social Security number (SSN) unless a job has been offered in writing and you have accepted the offer.
- Do not provide personal documents (Driver's license, Social Security card, Passport) in the application process or interview.
- Watch for mismatches in company and contact domain names. For example, a job posting from a Google company contact should only have an email address @google.com. If the contact had a @yahoo.com address and not @google.com, more research may be required to validate the position.
- Beware of communication with potential employers through chat platforms or text. Typically legit employers will contact candidates via email or phone number listed on your resume, LinkedIn, Handshake, Indeed and possibly WeChat or WhatsApp. Interviews will typically happen via phone, skype, Zoom, or another widely used video platform.

Clues a Job May be Fraudulent (cont.)

- Watch out for anonymity. If you cannot find a company website, address, contact information, staff members listed on LinkedIn, this is cause to proceed with caution.
- Check the company's website for the job posting you have been contacted about.
- Never provide any banking account information during a job search. The only valid time you should provide banking account information is if you have accepted a job and are asking for direct deposit for your paychecks. This would be initiated by you, the employee.
- If you see the word "fraud" listed anywhere in company reviews during your research, please do not proceed with your application and you should contact CDO. Fraud means a person or thing intended to deceive others.
- Beware if the job posting or offer letter contains spelling and grammatical errors.
- Referrals are great, but if you did not apply for a job, and are called for an interview, do more research.

Research Potential Employers

When applying for any position, it is important to research the company thoroughly before agreeing to an interview or considering a job offer.

- Review the company's website for anything suspicious.
- Google search the company name for web articles, reviews and news.
- Search for company on Glassdoor or RipOffReport and read reviews.
- Search for your contact on LinkedIn and confirm matching company name.

Other Online Resources

- JHU Office of International Services – Fraud and Scams
- Common Fraud Themes – FBI

You should always trust your intuition when job searching—if something doesn't feel right you should ask follow-up questions of the employer or connect with a CDO staff member and get an opinion.