HOW TO SPOT FRAUDULENT JOB POSTINGS

On Handshake, we strive to review employers and their full-time and part-time job and internship postings to confirm that they are legitimate. However, on occasion one slips through the cracks. It is imperative that you, the job searcher, know how to distinguish legitimate job postings from scam attempts.

Basic Tips

- When in doubt, get the job description directly from the company's official website. Much like phishing emails, scam job postings often capitalize on well-known companies' names and images.
- Google the company's employment page and read the job description directly from their site rather than click a link from a suspicious posting, which could take you to a cosmetically similar page. This will confirm the opening is legitimate .
- Call the company in question using publicly available contact information and ask questions about the job opening. If there is no phone number for the given company...do not pursue it.
- Legitimate employers will not ask for personal information so do not provide the following:
  - Financial or banking information
  - Copy of your driver's license card
  - Copy of your Social Security card
  - Copy of your Student ID
  - Driver's license, Social Security or Student ID numbers
  - *Note: Before hiring, some employers will request your SSN to conduct a background check - make sure you are comfortable with the company before supplying this information.*
  - *Note: Do sign your Social Security Card, but do not carry it around; keep it in a secure location that you can access.*
- If posting your resume online where it can be accessed by anyone, omit personal contact information
- If a job sounds too good to be true, it almost certainly is...don't pursue it without diligent research

Red Flags

Warning signs of fraudulent emails and websites include: bad grammar and spelling, requests for personal information and difficulty contacting or identifying the person posting.

These are all clear signs of trouble:

- You are asked to give credit card, bank account or PayPal account numbers.
- You are asked to send a payment by wire service or courier.
- 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 receive an unexpectedly large check.
- You are asked to transfer money, including via e-Bay, PayPal or Western Union.
- You are asked for personal information, such as your Social Security Number.
- You are requested to send a photocopy of your ID, i.e., driver's license to "verify identity."
- You are asked to complete a background check before you can be considered for a position.
- The posting appears to come from a legitimate company or organization, but the contact's e-mail address doesn't match the company's website domain (i.e., jdoe@gmail.com rather than jdoe@companyname.com) or the company's website domain is misspelled (e.g. jdoe@microsft.com).
- The job posting doesn't mention the responsibilities of the job; rather, it focuses on the amount of money you will make.
- Website includes information only about the job for which you are applying, rather than also including general company information.
- You receive a job offer in response to your application to a legitimate-appearing position description, but it is actually a marketing e-mail to sell you job search "help."

What to do if Caught in Scam

- Immediately contact campus police
- Contact CPAD so the posting can be removed and other students can be notified
- End all communication with the employer.
- Get in touch with your bank or credit card company and dispute any fraudulent activity immediately
- Depending on what personal information was disclosed, monitor or close your accounts. Depending on the situation, you may need to notify the three credit bureaus: Experian, Equifax and Transunion.
- If the incident occurred entirely over the internet, file an incident report with the FCC at http://www.cybercrime.gov.

Additional Resources for Safe Online Job Search

- consumer.ftc.gov/articles/0243-job-scams
- worldprivacyforum.org/2009/02/consumer-tips-job-seekers-guide-to-resumes
- monster.com/career-advice/article/A-Safe-Job-Search
- Better Business Bureau: bbb.org

If you have questions or concerns about job postings, a position for which you've applied or a task you've been asked to complete as part of the application process or a job offer, please contact Career Planning and Development to discuss it.

Adapted from Case Western Reserve University, October 2015