Job Search Safety Tips: Avoiding Job Scams

As you conduct your job search, remember to carefully evaluate all job postings, interviews, and offers. Unfortunately, there are scammers and criminals who post fraudulent job postings in hopes to scam individuals for money and/or personal information. Read below to learn about job search safety tips and common red flags of fraudulent job postings.

It is the responsibility of the student/job seeker to perform due diligence in researching employers when applying to and accepting employment. Job seekers should use common sense and caution when applying for or accepting any position. After performing due diligence, if you have any questions about the legitimacy of a job posting and/or offer, feel free to contact the Career Services Center for guidance.

Job Search Safety Tips:

Use common sense when applying for employment/internship opportunities.

- If a position or salary sounds "too good to be true," it most likely is.
- Be alert when job descriptions are vague, promotes mainly how much money you could make, and/or includes many spelling and grammatical errors.
- If a job is offering a lot of money for very little work, it more than likely is a scam.
- Postings offering a job "guarantee" or that ask you to buy study materials, send money for certification or placement should be avoided. Legitimate organizations do not make guarantees or ask for payment to hire or train you.
- If an employer asks you to participate in an activity that makes you feel uncomfortable, say no.

Never cash a check for, or give any money to, an employer.

- Don't apply to job listings that use language such as "money transfers" or "wiring funds."
- Beware of check-cashing scams. If someone asks you to deposit a check or money order into your personal account and send money to another individual, don't do it.
- Do not agree to have funds or paychecks directly deposited into any accounts by a new employer. (Arrangements for direct deposit or paycheck should be made during your first day or week of actual employment on site – not before.)

Research the employer. Meet in-person at their place of business.

- Research (i.e. Google) the employer's physical address, phone number, and/or email address to be sure it is connected to an actual business organization. Research a company for legitimacy by visiting the Better Business Bureau (www.bbb.org) and/or Hoovers (www.hoovers.com).
- Meet face-to-face with a potential employer. An in-person interview or informal chat will help you determine the employer's intentions.
- Reputable employers normally require an interview (and more) before hiring. If you are offered a job without an interview, be suspicious.
- Never agree to a background check unless you have met the employer in person.

Do NOT give out personal information.

- Do not give your personal bank account, PayPal account, or credit card information to a new employer. Never give out personal information over email or phone.
- Do not fax copies of your identification or Social Security number to an unknown person. Offer these documents to your employer only when you are physically at the place of employment.

Red Flags – How to Identify a Potential Fraudulent Job Posting:

The Job Description and/or Email Address Looks Fishy.

- The job description is vague with minimal company information, promotes mainly how much money you could make, and/or includes many spelling and grammatical errors.
- The contact email address contains a non-business email domain or a personal email address. Sometimes the posting may even appear to be from a reputable, familiar company, but the email address does not match the domain used by representatives of the company.
- The email address of the recruiter is from a Gmail, Hotmail, or Yahoo account and not a company account. (Small companies may have a generic email using Gmail or Yahoo.)
- Email address of contact person doesn't match the company domain name. scammers use the name of a real person in a legitimate company to construct the email, but again, the real recruiter would always use their email address with the company domain.

You Have to Pay Money, Cash a Check, Give Out Personal Information, etc.

- You are asked to send, transfer money or provide credit card information. You should never be asked to send money as payment for training, initial investment, supplies or company "placement" expenses nor should you transfer money from one unknown person to another, even if you are first sent a check. Fraudulent money transfers are a common job scam.
- The position requires an initial investment, such as having to purchase equipment or products in order to earn a wage or paying for necessary training.
- Bank account, social security number or other personal information is requested up front. (Legitimate employers will require this information to complete the hiring process. However, NEVER share this information until you're certain the opportunity is real and a job offer is made.)
- You are asked to provide a photo of yourself. How you look is not something employers need to know to determine whether or not you have the right skill sets for the job.

Very Little Information Can Be Found When Researching the Company.

- The "company" website is not active, does not exist, or re-routes users to another website unaffiliated with the "company."
- It is difficult to find a mailing address, contact information, a name, the company name, etc.
- The company doesn't have a legitimate website or the website offers very minimal information. You can check to see if a company is legitimate by using these websites:
    - Better Business Bureau: www.bbb.org
    - Hoovers: www.hoovers.com

Additional Red Flags:

- The employer hires you based on your resume alone, without a formal interview.
- The employer responds to you immediately after you submit your application. (This does not include an auto-response email you may receive from the employer stating receipt of your application.)
- You are contacted via phone or email for a job you never applied to.
- The employer contacts you by phone, however, there is no way to call them back. The number is not available or disconnected.
- The employer tells you that there is no office in your geographic area and you will need to help them get a "new" office up and running.
- The position states you will be working from home and/or is with a small start-up business. There are legitimate "work at home" jobs and start-up companies, but perform due diligence. Do significant research and ask tough questions.

What to Do if You Are Already Involved in a Job Scam

Cease all contact with the employer and:

- **Contact the local police.** Report the fraudulent employer to the local police, who may choose to conduct an investigation (regardless of whether the scam artist is local or in another state).
- **Contact your bank.** If you sent money to a fraudulent employer and/or shared your personal banking information, contact your bank or credit card company immediately to protect the account and dispute the charges.
- **File a complaint with the Federal Trade Commission (FTC).** The FTC is the nation's consumer protection agency, which collects complaints about companies, business practices, and identity theft. File a complaint by going to www.ftccomplaintassistant.gov or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).
- **Contact the Career Services Center** so we can review the position/employer and be informed about the job scam. Email career@nsc.edu.

Disclaimer:

The Career Services Center advertises jobs through Handshake and other platforms to assist students and alumni with their job search. However, an advertisement/posting does not constitute an endorsement or recommendation of any employer by the college or the Career Services Center. The Career Services Center makes no representations or guarantees about job listings or the accuracy of the information provided by the employer. The Career Services Center in not responsible for the accuracy, legality or any other aspect of the content of a job posting and/or embedded link. The Career Services Center is not responsible for safety, wages, working conditions, or any other aspect of employment. It is the responsibility of the student/alumnus to obtain all the necessary information concerning the employer and the position and to take all necessary precautions when interviewing for, or accepting positions with any employer.

This resource has been sourced and adapted from:

University of Missouri Career Center: Avoid Job Scams
University of Arizona Student Engagement & Career Development: Avoiding Employment Scams
University of North Carolina Charlotte University Career Center: Job Posting Scams