Avoid Job Scams

Finding a job can be tough! Remember to carefully evaluate all job postings, interviews, and offers. Students should be aware that there are criminals and scam artists who may prey upon your money, physical safety and personal information. Career Opportunities & Employer Relations (COER) wants to help you avoid scams and find meaningful employment.

Fraud Postings: Red Flags

The job seems too good to be true!

Be wary of jobs that pay extremely well for working from home or sites that promise a job position. The position states a “first year compensation” which is in high excess to the average compensation for that position type. A description that says “employees can earn from $40K – $80K the first year!” is usually untrustworthy.

You are asked to send, transfer money or provide credit card information.

Fraudulent money transfers are a common job scam. 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.

Bank account, social security number or other personal information is requested up front.

Employers will require this information to complete the hiring process; however, NEVER share this information until you are absolutely certain that the opportunity is real.

The site advertises “secret” job postings for a fee.

Job postings should be free and available on social media and employer websites; it raises a red flag when websites ask you to pay for viewing the job listing.

Poorly written and/or vague job description that mainly advertises how much money you can make.

Be alert when job descriptions are vague because in reality, an employer would want to hire the right person and spare no effort to write a thorough job description. A fraudulent job description is written in a vague manner and sometimes it neglects to mention job responsibilities and instead describes in detail how much money you can make. The posting may also include many spelling and grammatical errors.

Does the email address of the contact person match the company domain name?

A small company or start-up may have a generic email (e.g. Gmail, Yahoo) account but most companies should have a company domain. Fraudulent email addresses may

contain the domain @live.com or highly suspicious addresses (e.g., evelin155@gmx.us) that are not .com or .org. Some 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.

Does the employer have a legitimate website?

When you Google the employer's phone number, fax number and/or email address, and it does not appear connected to an actual business organization, this is a red flag. You can check to see if a company is legitimate by using these websites:

- Better Business Bureau (http://www.bbb.org/us/consumers/)
- Hoovers (http://www.hoovers.com/)
- AT&T's Anywho (http://www.anywho.com/)

Does the website include company history, career opportunities, and address? Scammers will often create quick, basic web pages that seem legitimate at first glance.

Interviewing in a suspicious or dangerous location.

Always ensure that you interview at a legitimate place of business or in a public place. You should never interview in someone's home unless working in a private household (babysitter, lawn mower, etc.). Remote spots and buildings that are unmarked should raise real concern. If your instincts tell you it's suspicious, it probably is. Someone should always know of your plans to interview and the location.

Other Job Scams.

Many job scams take advantage of people's desire to "make money fast", however that is often an illusion. Common job scams include, Envelope Stuffers, Home-based Assembly Jobs, Online Surveys, Mystery Shoppers, Craft Assembly, Email Processing, and Multi-level Marketing.

If you are in doubt, Google and report it!

If you have never heard of a website before, and you are suspicious of it being a scam, Google the URL with the word "scam" next to it and research the company. You can usually find previous victims or complaints related to that scam.

Handshake

If you have questions or suspect any Handshake jobs or employers of unethical or criminal behavior, immediately report it to:

Sara Earl
COER
(573) 341-4230
earls@mst.edu

COER will take action and investigate the posting and related employer. Remember that your report will effectively protect other students from harm. If you have questions about the legitimacy of a job listing outside of HireMiners.com, contact the Better Business Bureau or the Federal Trade Commission.

Victim of a Scam?

Contact the Rolla Police Department immediately for investigation. If the incident occurred completely online, you should also file a report to the Federal Trade Commission.

If you have already been victimized by a scam, for example, you sent money or released your bank account information to a fraudulent employer, you should contact your bank and/or credit card company immediately to close the account and dispute the charges.

Disclaimer:

While COER reviews each company profile and job posting on Handshake, it makes no endorsements, representations, or guarantees about the positions listed on the website and is not responsible for safety, wages, working conditions, other aspects of employment, or whether the students/alumni have the requisite training and work experience to qualify for a position.

It is the responsibility of the student/alumnus to obtain all of the necessary information concerning the employer and the position and to take all necessary precautions when interviewing for, or accepting positions with any employer.

Sources:
Federal Trade Commission, University of Georgia, Rutgers University, University of Southern California, University of Washington, University of Missouri.