Protecting yourself from scams- what to look for

Here at Coe College's Center for Creativity and Careers, we care about our fellow Kohawks, and this means making our campus aware of possible red flags when conducting job searches and undergoing a hiring process. Below you will find some common red flag behaviors to watch out for in job advertisements and potential employers. We hope that this guide will not only serve to make job hunting more efficient, but also safer and more reliable for students and alumni.

A key element of identifying red flags and avoiding scammers is by taking the time to thoroughly overview job listings before applying. Examples of careful overview of a job listing and/or potential employer are:

- The listing does not provide a street address
- The listing does not provide a clear business name
- The listing does not provide a website, and when a website is available, it is not functional or low quality
- The recruiter does not have an email address, and when there is one present, the email does not end in the company's website address. Instead it ends with: @gmail, @yahoo, @hotmail.
- The listing features a vague job description. Expected responsibilities and qualifications of the job are vague. Scammers often limit the detail placed in job descriptions so that the scam can appeal to a larger net of people.
- The advertised salary in the job description is well out of the expected range in regards to the position being advertised.
- The job is listed on an obscure website, as opposed to common employer websites like: indeed.com, LinkedIn.com, Handshake.com, etc.
- The listing requires a form of financial information or payment
- The listing is from a foreign company that cannot be easily verified
- The posting appears to be from a reputable, familiar company (often a Fortune 500 company). Yet, the domain in the contact's email address does not match the domain used by representatives of the company.
- The position states you will be working from home
- The job is for a start-up business, a new small private company, and entrepreneurial enterprise just getting off the ground.
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys, Check Writing and Processing.
- The employer responds to you immediately after you submit your resume. Note - this does not include an auto- response you may receive from the employer once you have sent your resume.
- The employer contacts you by phone, however, there is no way to call them back. The number is not available or disconnected.
- Look at the company's website. Does it have an index that tells you what the site is about; or does it contain information only about the job you are interested in?
- Grammatical errors. Legitimate employers rarely make grammatical errors in job listings.

Steps to Verify a Potential Employer and/or Job Posting

- Google the employer's phone number, fax number and/or email address. If it does not appear connected to an actual business organization, this is a red flag.
- You can use the Better Business Bureau (www.bbb.org/council/consumer-education), Chambers of Commerce (www.uschamber.com/chamber/directory) Hoovers(www.hoovers.com), and AT&T's Anywho (www.anywho.com) to verify organizations.

- Before entering personal information online, check to make sure the website is secure by looking at the web address bar. The address should be https:// not http://
- Legitimate companies don't ask for money. If you're told that you need to purchase software or pay for services, beware.
- Go to the DomainWhitePages.com and type the company's web address into the "domain or IP address" box and click the "go" button. The results will tell you the date when the website was created. If the website is less than a year old, be on your guard.

What to do if You Encounter a Fraudulent Employer and/or Job listing

If you encounter a fraudulent employer, there are a few steps you can take. If they are currently listed on a job searching engine report them to the host site. If the posting is listed on Handshake, report the listing and employer to the Coe College Center of Creativity and Careers at o-career@coe.edu to be removed.

If the incident occurred completely over the Internet, you should file an incident report at this site: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

Job Scam Video and information from the Federal Trade Commission
http://ftc.gov/jobscams

Job Scams List: A – Z List of the Most Common Job Scams
http://jobsearch.about.com/od/jobsearchscams/a/job-scams-list.htm
The list of red flags, comments and suggestions in this document are not necessarily comprehensive and definitive; they are provided to assist you with your job search and to help you be aware of fraudulent and scam job postings.

Examples of Job Scams
Healthcare Admin Assistant: "This is a work from home job. Work hours is from 9am-4pm Monday-Friday You will earn $45 per hour for this position, you are also expected online at Yahoo Messenger during working hours. We also offer flexible hours...."

"The Human resources have just reviewed your resume due to the one you posted on www.allstarjobs.com.You are now scheduled for an interview with the hiring manager of the company. Her name is Mrs. Ann Jernigan; you are required to set up a yahoo mail account(mail.yahoo.com) and a yahoo instant messenger."

"The scammer's email address was jobs@senergy-world.com. The real company email is jobs@senergyworld.com"

"Once you receive the check, first of all, I want you to head right away to your bank and get the check cashed. Deduct your first-week pay which is $500, and Deduct extra $100 for the Money Gram sending fee and proceed to the nearest Money Gram outlet around you to make payment to my wife travel agent."

This guide adapted from information from Coe College Center of Creativity and Careers, the National Association of Colleges & Employers, University of North Carolina Wilmington Career Services, the Federal Trade Commission, and Arizona State University Career Center