Fraudulent or Scam Job Postings

Familiarizing yourself with the following security-related tips and resources will help you evaluate job postings.

Look for warning signs:

- You must provide your credit card, bank account numbers, or other personal financial documentation; or you must purchase any products on behalf of the employer as part of your employment (such as Green Dot MoneyPaks, gift cards, phone cards, etc.)
- The position requires an initial investment, such as a payment by wire service or courier.
- The posting includes many spelling and grammatical errors.
- 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).
- The employer is ‘out of the country’ so unavailable to meet, but asks to conduct the business over email.
- You receive, or are promised, an unexpectedly large check
- You are asked to provide a photo of yourself or provide personal, detailed information (marital status, age, weight, etc.).
- The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys, Personal Assistant.
- The posting neglects to mention what the responsibilities of the job actually are. Instead, the description focuses on the amount of money to be made.
- The position indicates a "first year compensation" that is in high excess to the average compensation for that position type.
- 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? Scammers often create quick, basic web pages that seem legit at first glance.
- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc. - this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well-hidden. While it possible for reputable companies to have no online presence, it is unusual and infrequent in this day and age.
- When you Google the company name and the word "scam" (i.e. Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is: http://www.ripoffreport.com.
- The employer contacts you by phone, however there is no way to call them back. The number is not available.
- The employer refuses to give you a W-4 and wants to pay you under the table.
- The employer is not a home-based business but asks you to interview at their home.
- The employer asks you to use your money to pay for their personal or business needs.
- The employer tells you that they do not have an office set-up in your area, and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).

If you suspect a position you encounter through the HuskyJobs database or through your UW email is fraudulent, please contact Emma O’Neill, Assistant Director for Employer Relations at the UW Career Center: econeill@uw.edu or 206.543.9109.

Research the employer

1. Read the employer/company description (if available) before submitting any application materials.
2. If you have doubts about a company’s legitimacy, research the company using web sites operated by the Better Business Bureau (http://www.bbb.org/us/consumers/), Hoovers (http://www.hoovers.com/) or AT&T’s Anywho (http://www.anywho.com/).

Protect yourself

1. Make informed decisions before sharing your Social Security Number with a potential employer. Most employers will not ask
for personal information until you arrive at their offices for an interview and are given a formal job application, so be wary if you are asked to give your Social Security Number by phone, email, or online. Asking for a Social Security number is not illegal, but they should have a good reason for doing so at the initial application.

2. Never wire funds via Western Union or any other wire services to a potential employer.
3. Never accept any kind of offer to cash checks or money orders on someone's behalf.
4. Refrain from providing credit card or bank account numbers or engaging in any financial transactions over the phone or online with a potential employer/recruiter.
5. Withhold offering personal information (such as marital status, age, height, weight). Such questions might violate federal hiring standards, and job seekers are not obligated to answer them.
6. Exercise caution when dealing with prospective job contacts outside of the United States.

What if you have already submitted your resume?
As long as you did not include your social security number, bank numbers or a photo with your application, there is a low risk that your privacy would be compromised at this point. However if you have misgivings and, as a result of your application, you are contacted by the company we would discourage you from filling out any additional application materials or responding back at all.

If you have already been in contact with a company outside of your original resume submission; and you have provided any other personally identifying information such as your social security number, you may get more information about reporting potential identity theft or fraud with the Federal Trade commission by calling (1-877-FTC-HELP) or by using the FTC’s online information and filing system at: http://www.ftc.gov/bcp/edu/microsites/idtheft/ This is also a great resource for information about protecting yourself from identity theft or fraud.

You are also encouraged to contact the local police immediately – either the UWPD or police department in your area.

Learn More
If you have concerns about identity theft problems resulting from your resume submission, you can also find helpful information at the Privacy Rights Clearinghouse www.privacyrights.org/identity.htm and the Identity Theft Resource Center www.idtheftcenter.org. There, you will find fact sheets and detailed information about specific steps you need to take. The Privacy Rights Clearinghouse also has guides on SSNs and other workplace privacy issues.