# FRAUDULENT JOBS OR SCAM JOB POSTINGS

**The following security-related tips and resources will help you evaluate job or internship postings.** If you suspect a position you encounter through the Handshake database or through your UW email is fraudulent, please contact the Career & Internship Center at askcic@uw.edu or 206.543.0535.

## WARNING SIGNS

There are common 'red flags' that we encourage you to look for as you evaluate opportunities, as they often indicate that an opportunity is fraudulent:

- The employer asks you to send money as a condition of application or employment.
- Positions that ask you to give credit card or bank account numbers, or copies of personal documents.
- An employer asks you to cash checks, wire or transfer money, or utilize your bank account to deposit checks or transfer money as part of the application process or as a condition of employment.
- The position indicates the candidate will be "working from home" or will be a "virtual" employee; while legitimate home-based or remote-work opportunities do exist, this is a common element of fraudulent postings as well and opportunities with these qualities deserve additional scrutiny on your part.
- The employer asks you to send your resume to a generic email address (Gmail, Hotmail, Yahoo, etc.). (*NOTE*: this is not necessarily an immediate hallmark of illegitimacy, as many small businesses and/or start-ups utilize generic email accounts as they are getting started; but use of a generic email address should trigger some additional research on your part).
- Position listings with bad spelling or very poor grammar.
- The promise of a large salary for very little work (especially those that state thousands of dollars of income per month with little or no experience required).

Overall, ***if something sounds too good to be true, it probably is***. Do your homework, and be sure to research any job opportunity that interests you. Pay attention to anything that seems 'off'.

## RESEARCH THE EMPLOYER

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

## PROTECT YOURSELF

- 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.

- Never wire funds via Western Union or any other wire services to a potential employer.
- Never accept any kind of offer to cash checks or money orders on someone's behalf.
- 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. 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.
- Exercise caution when dealing with prospective job contacts outside of the United States at companies with which you are not familiar**.**

## 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 concerns and you are contacted by the company after you apply, we would discourage you from filling out any additional application materials or responding back at all.

- **You should immediately contact police** – either UWPD (206-685-8973) or the non-emergency number for your local police. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state).
- **If it is a situation where you have sent money to a fraudulent employer**, contact your bank or credit card company immediately to close the account and dispute the charges. **If the incident occurred completely over the Internet**, file an incident report with the: https://www.cybercrime.gov/ or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).
- **If the position was posted to Handshake,** please also contact the Handshake Program Manager at handshake@uw.edu.

## 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 https://privacyrights.org/categories/identity-theft and the Identity Theft Resource Center https://www.idtheftcenter.org/. There, you will find fact sheets and detailed information about specific steps you may wish to take.

## UNIVERSITY OF WASHINGTON

The University of Washington's Office of the Chief Information Security Officer (CISO) has also created some resources with phishing examples, tips for identifying scams, and how to protect yourself.

Using Handshake, the Career & Internship Center strives to maintain a job and internship board full of compelling and legitimate opportunities. We review each employer and job posting before they are approved to remove the occasional fraudulent opportunity, and support students if fraud is discovered. **Ultimately, however, a student's safety during their job search process is their own responsibility.** The University of Washington and the Career & Internship Center are not liable for any losses incurred by students, financial or otherwise.