# Avoiding Online Job/Internship Scams

Job seekers who use online posting boards and search sites must be careful to avoid fraudulent postings and job scams.

#### Do Your Research

Visit the company's website - Review websites to help verify legitimacy. If the company doesn't have one, it takes you to a different website, or it is poorly developed, consider that a red flag. How professional is it? Is there legitimate contact information? Are jobs/internships and career information posted on the site?

**Use Google** - Search by company name to see what information you can find (if a company name isn't provided, consider that a red flag). Take it one step further and search by "[company name] scam" to see if you can find information on reported scams. The following sites may help you to find additional information including any negative reviews: www.ftc.gov, www.bbb.org, www.glassdoor.com, www.ripoffreport.com

Review Job/Internship Details - Make sure you receive a complete description of the opportunity including specific responsibilities and required qualifications. If it isn't included in the posting, ask about compensation. If the position is paid, ask about pay range, how often you will be paid, and method of payment. If the company does not pay an hourly rate or salary, carefully investigate the details. If the offer is too good to be true then it probably is.

## Be Aware of Red Flags

- Company/organization does not have an established website or website is poorly developed
- Email was unsolicited and sent directly to you (may begin with "Dear Sir or Madam")
- Email is sent using a free email service (Yahoo, Hotmail, Gmail, etc.) instead of a company domain
- Email/ correspondence is poorly written and contains misspellings, grammatical errors, or typos
- Position described as "work from home and make thousands from your computer"
- Request for social security number (SSN) or bank account information
- Request to provide a photo ID to "verify identity" before meeting an employer in person
- Position advertised is different from the position offered

## Don't Be a Victim of Payment Transfer/Forwarding Scams

#### DO NOT:

- Provide personal bank account, PayPal account, or credit card information.
- Participate in wiring or transferring funds from a personal bank account or PayPal account to another account. Often times you may be asked to retain a portion of the funds as payment for your services, which is money you never end up seeing.
- Agree to have funds or payments direct deposited into your account without knowing and verifying the employer first. Many employers provide the option for direct deposit; however, this typically will not occur until the first day or week of employment not before.
- Pay upfront fees for an employer to hire you (there may be some rare exceptions to this).

### Steps to Take for Victims of Job Scams

Have you been scammed or almost scammed? Here's what you can do...

- Notify all banks/credit unions and close all accounts at the places where scam-related transactions were made.
- Order a credit report from all three credit bureaus every 2-3 months to look for unusual activity on accounts. Place fraud alerts if needed.
- Permanently close the email address used to communicate in the scam.
- Fraud victims should file a police report with local law enforcement officials and contact the local secret service field agent (for international payment scams)
- Report the scam to The Internet Crime Complaint Center: www.ic3.gov
- Report the scam to job sites where the posting was found and/or any companies the scam tried to copy

#### Resources

#### **Federal Trade Commission**

File a complaint by calling 1-877-382-4357 or visiting www.ftc.gov

#### Better Business Bureau

www.bbb.org

#### **Credit Bureaus**

Equifax: 1-800-685-1111, www.equifax.com Experian: 1-800-397-3742, www.Experian.com TransUnion: 1-800-888-4213, www.transunion.com

#### Privacy Rights Clearinghouse

https://www.privacyrights.org/avoiding-online-job-scams

