Watch for Scams When Searching for a Job or Internship

ASU cares about our students and our employers. With this in mind, we have compiled a list of commonly seen hiring practices that should heighten your awareness to help you be successful in your job or internship search.

Scammers will tell you they found you on Handshake, LinkedIn, Indeed, at a conference or similar. Of course, real employers might tell you that too. Check your settings on each site to see if they could have found your profile and if they are on that platform.

Don't accept a job that you didn't apply to and/or didn't require an interview or barely asked you any questions, and/or gave you 1 day to accept. **Put your excitement on pause.** Speak with a trusted person about your interaction with the company and documents you are asked to sign. Keep copies of all communication.

Often the scammer will try to scare you by telling you they are going to report you to the police or immigration.

PROTECT YOUR PERSONAL AND FINANCIAL INFORMATION.

NEVER provide financial documentation before you start.

A company never needs your credit card, debit card or PIN.

NEVER accept and deposit a check before you start and do work.

Pay to Play?

- The position requires an initial investment, such as a payment by wire service or courier.
- The employer offers a large payment or reward in exchange for allowing the use of your bank account for depositing checks or transferring money.
- The employer tells you that they do not have an office set up in your area or that you will work from home. They tell you they need you to purchase equipment, or they need your bank account and social security information supposedly to make the transactions.
- You should not have to pay to get a job or training or purchase software and equipment.
- They want to pay you cash and off their official payroll records.

Is the company legit?

- The business name is not easily identifiable, and no clear business website is listed. Or, if there is a website, there is no substance to the content.
- The posting appears to be from a reputable, familiar company (often a Fortune 500). Yet, the email handle in the contact's email address does not match the domain used by representatives of the company (this is typically easy to determine from the company's website). Another way to validate is to check the open positions on the company's website, by checking their careers/jobs page. You could try contacting the real company directly stating that you think someone is spoofing them, but they might not respond.
- The street address is a non-US address, not at the company's address, or is a post office box.

How is the company representative interacting with you?

- Hover over the email address. Does it have a different email address?
- The employer contacts you by phone, but the number is blocked or not available and there is no way to return the call. When you ask for their number, they do not provide i

- The employer contacts or interviews you only by text.
- The contact email address contains the domain or an @ that is not affiliated with the company. Examples: @live.com, @gmail, @yahoo, @hotmail.

Are the job descriptions sketchy?

- There are significant spelling and grammatical errors within the posting.
- The employer requires you to pay money or a 'membership fee' in order to access opportunities.
- The posting neglects to mention the responsibilities of the job. 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. Or, the salary range listed is very wide (e.g., "employees can earn from $70K – $150K the first year!").
- The position is for any of the following: envelope-stuffers, home-based assembly jobs, or online surveys, clerical work at home, typing, shipping packages, and personal assistant/shopping duties. Often, for this type of opportunity, the employer never actually interviews you or wants to meet face-to-face.

No interviews or easy interviews?

- The employer offers you a job for which you did not apply.
- They offer you a job for which you are not qualified.
- The only interview is a general text chat.
- They don't ask you any technical questions.
- They ask you to pad your resume, so it looks like you have the experience.
- They want international students to work when they don't have work authorization.
- They ask for your date of birth, photos or similar items.

Do your research before applying for a job to make sure that the opportunity is genuine and meets your needs. When you research on a job or company, here are some tips to be aware of:

- The position initially appears as a traditional job. Upon further research, it sounds more like an independent contractor opportunity.
- 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 in which you are interested? Scammers often create quick, basic web pages that seem legitimate at first glance.
- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc., this is reason to proceed with caution. Fraudulent postings are illegal, so scammers will try to keep themselves well hidden.
- Do they have full LinkedIn pages with many and diverse connections?
- When you Google the company name and the word "scam" (e.g., Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is http://www.ripoffreport.com.
- Conduct an internet search of the employer's phone number, address, and/or email address. If it does not appear connected to an actual business organization, this is a red flag. You can use the Hoovers, AT&T's Anywho, and Better Business Bureau (used less frequently), to verify organizations. You can also check Who.is to see when the domain name was created. Proceed with caution if the domain name was created within the last few days.
- Be cautious about which job posting websites you submit your resume and complete contact information. When possible, apply directly to company websites.
- Watch This Video from the Federal Trade Commission on job scams.

IF YOU THINK YOU HAVE BEEN SCAMMED, immediately take the following steps:

- Do not respond and discontinue all contact. Keep screenshots and emails for your records.
- Anyone who has received a check, should hold on to the envelope and check. Do not deposit the check. It could become needed as evidence in the future.
- Anyone who has deposited the check or has done anything to transfer funds should contact ASU PD (if you live on campus) or the city police where you live to file a report.
- Report the incident to infosec@asu.edu