Common "Red Flags" When Searching for a Job/Internship

ASU Career and Professional Development Services 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.

> **Oftentimes red flags can be identified just by looking a little closer at the job description. Here are some common themes to be on the lookout for when searching for jobs.**

- 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.

- 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 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.

- The contact email address contains the domain @live.com or an @ that is not affiliated with the company. Example: @gmail, @yahoo, @hotmail, etc.

- The position is for any of the following: envelope-stuffers, home-based assembly jobs, or online surveys.

- 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 $40K – $80K the first year!").

- The job duties entail 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.

> **Beyond the job description the employer's interactions with you can be a red flag. Here are some items to be on the lookout for:**

- The employer contacts you by phone, but the number is blocked or not available and there is no way to return the call.

- The employer contacts you by email offering you a job you did not apply for or inviting you to apply for a job. For more information, please visit this Student Jobs Email Scam article.

- Personal financial documentation (credit card, bank account) are requested of you. Or, the position requires an initial investment, such as a payment by wire service or courier. Another method could be 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 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).

> **Always do your research before applying for a job to make sure that the opportunity is genuine and meets your needs. When you do 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 cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well hidden.

- 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.

- 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, Hoovers and AT&T's Anywho to verify organizations. You can also check WhoIs.net to see when the domain name was created. Proceed with caution if the domain name was created within the last few days.

- For more information, please Watch This Video from the Federal Trade Commission on job scams.