



## Warning Signs of Fraudulent Job Postings

The Texas A&M University Career Center wants to make you aware of the red flags that can help you identify those job opportunities that are simply too good to be true. Remember ANY TIME you have a question or concern about a posting or an employer, please contact the Career Center by sending an email to [cc\\_advisor@tamu.edu](mailto:cc_advisor@tamu.edu).

### Common Warning Signs:

- The employer or recruiter asks you to provide your credit card, bank account numbers, or other personal financial documentation.
- The position requires an initial investment, such as a payment by wire service or courier.
- You are asked to purchase training materials or other items before you are hired, usually for a significant amount of money.
- Search for 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.
- The posting appears to be from a reputable, familiar company (often a Fortune 500). Yet, the domain 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.
- You find the job on a networking or social media site for an actual company but cannot find the posting on the company's official website.
- The posting does not list the responsibilities of the job. Instead, the description focuses on the amount of money to be made.
- The posting includes many spelling and/or 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).
- You receive an unexpectedly large check (checks are typically slightly less than \$2,500, generally sent or deposited on Fridays).
- You are asked to provide a photo of yourself.
- The employer responds directly to you immediately, within minutes, after you submit your resume. Typically, resumes sent to an employer are reviewed by multiple individuals, or not viewed until the posting has closed. Note - this does not include an auto-response you may receive from the employer once you have sent your resume.
- The position indicates a "first year compensation" that is well above the average 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 to be legitimate at first glance.
- Watch for anonymity. Is it difficult to find an address, actual contact, company name, or email address? Fraudulent postings are illegal, so scammers will try to keep themselves well-hidden.
- The salary range listed is very wide (i.e. "employees can earn from \$40K - \$80K the first year!")

- When you search for the company name and the word "scam" (i.e. Acme Company Scam), the results show several scam reports concerning this company.
- The employer contacts you by phone; but there is no way to call them back. The number is not available.
- 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).
- And finally, if the job simply seems too good to possibly be true, make sure to contact the Career Center to confirm that is indeed a legitimate opportunity.