TEXAS TECH UNIVERSITY
University Career Center™

Avoid job scams

1. Do your research

- Visit the organization's website: Review websites to help verify legitimacy. If the company doesn't have a website, 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 organization 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, and 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.

2. Follow these tips!

- Do not provide bank/credit card/financial information when applying for a job. There should be no request for fees or money associated with a job application.
- Be skeptical of emails received from employers that contain grammatical errors, promises of high salaries, and minimal details about the actual position or qualifications.
- Do not agree to have funds directly deposited into your account without verifying the employer first. Many employers will provide the option for direct deposit (for your paycheck); but this typically occurs within the first week of employment.
- Do not participate in wiring or transferring funds from a personal account or Paypal/Venmo/CashApp account to another account (even if you are offered a portion for your salary)

3. Look for red flags

- Unsolicited email(s) or text(s) sent directly to you

- Email sent using a personal/free service provider (yahoo, Hotmail, Gmail, etc.) instead of a company domain (example john.doe@ttu.edu)
- The correspondence or job description is poorly written, contains typos, and spelling and grammatical errors
- The position is described “work from home and make thousands from your computer”
- Request that the job seeker provide “photo ID” before meeting in person
- Request the job seeker to conduct business on their behalf (run errands) as they are out of the country
- The position advertised is different from the position offered