TigerRecruitingLink

your LINK to jobs, interviews and employers

FRAUDULENT POSTING GUIDE

1. INTRODUCTION

While we strive to review every job posting for legitimacy, on occasion one will slip through the cracks. It is imperative that you know how to distinguish legitimate job postings from scam attempts.
(Start by taking a look at this MSNBC story about a typical scam.)

2. BASIC TIPS

- **When in doubt,** get the job description directly from the company's official website. Much like phishing emails, scam job postings often capitalize on well-known companies' names and images.
  - **Google** (don't follow links from the suspicious posting, which could take you to a cosmetically similar page) and check the employment page to confirm the opening is real.
  - **Call** the company in question using publicly available contact information and ask questions about the job opening.
- Don't provide **financial information** or your **Social Security number**. Legitimate employers will not ask for your bank account details or your SSN, and this information can be put to disreputable purposes. **Note**: Before hiring some employers will request your SSN for purposes of a background check. Make sure you are comfortable with the company before supplying this information.
- If you are posting your resume online where it can be accessed by anyone, omit personal information like specific details about past employers and your date of birth.
- If a job sounds too good to be true, **it almost certainly is.**

3. RED FLAGS

- **Warning signs** of fraudulent emails and websites include: bad grammar and spelling, requests for personal information, and difficulty contacting or identifying the person posting are all clear signs of trouble.
- **Additional Red Flags**:
  - You are contacted by phone, but the number is not available
  - The posting contains **vague descriptions** that focus on money rather than the job
  - Email domain (the @xyzcorp.com part of the address) that **doesn't match** the company's official website's domain. Check for discrepancies in .com and .org, etc. also.
  - Email domain of a **free provider** is used (real companies almost always have their own email systems) i.e. @live.com, @yahoo.com, @hotmail.com, etc. Note: Sometimes they are valid. Feel free to ask a Career Center representative if you have questions.
  - Website that has information **only** on the job you're applying for, rather than about the company in general
  - Request for an initial investment or for you to cash checks and wire money
  - Request for your bank account access

4. WHAT TO DO IF YOU ARE INVOLVED IN A SCAM

- Immediately contact the local police.
- Contact the Career Center so the posting can be removed and other students can be notified.
- Get in touch with your bank or credit card company and dispute any fraudulent activity immediately.
- If the scam happened online, file a report with the FTC's cybercrime division

5. ADDITIONAL RESOURCES

- The FTC's Job Scams information page
- The BBB on employment scams