HOW TO SPOT FRAUDULENT JOB POSTINGS

Both on Racer Tracks full-time job and internship postings and part-time job postings, we strive to review them for legitimacy. However, on occasion one slips through the cracks. It is imperative that you, the job searcher, know how to distinguish legitimate job postings from scam attempts.

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 and check the employment page to confirm the opening is real instead of following a link from a suspicious posting, which could take you to a cosmetically similar page.
- Call the company in question using publicly available contact information and ask questions about the job opening. If there is no phone number for the given company...do not pursue it.
- Legitimate employers will not ask for your bank account details or your SSN as possessing this information can be used for disreputable purposes
  - Don't provide financial information
  - Don’t provide a copy of your driver’s license card
  - Don’t provide a copy of your Social Security card
  - Don’t provide a copy of your Student ID
  - Don’t give out your driver’s license, Social Security or M numbers
- *Note: Before hiring, some employers will request your SSN to conduct a background check - make sure you are comfortable with the company before supplying this information*
- If posting your resume online where it can be accessed by anyone, omit personal information like specific details about past employers and birthday
- If a job sounds too good to be true, it almost certainly is...don't pursue it without diligent research

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.

These are all clear signs of trouble:

- 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) does not match the company's official website 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 Services representative if you have questions.*
- Website includes information only about the job for which you are applying , rather than also including general company information
- Request for an initial investment or for you to cash checks and wire money
- Request for your bank account access

WHAT TO DO IF CAUGHT BY A SCAM

- Immediately contact the local police
- Contact Career Services 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

ADDITIONAL RESOURCES

Federal Trade Commission (FTC)
Job Scams page
consumer.ftc.gov/articles/0243-job-scams

Better Business Bureau (BBB)
Employment Scams page

bbb.org/us/article/280

Resource: jobs.auburn.edu

MURRAY STATE UNIVERSITY
Career Services

IMAGINE YOUR FUTURE. EXPLORE YOUR CAREER.

100 Oakley Applied Science Building | 270.809.3735
msu.careerservices@murraystate.edu | murraystate.edu/career