

HANDSHAKE STUDENT/ALUMNI DISCLAIMER

East Carolina University Career Services approves job listings for the convenience of students. The university does not endorse or recommend employers, and a posting does not constitute an endorsement or recommendation. The university explicitly makes no representations or guarantees about job listings or the accuracy of the information provided by the employer. The university is not responsible for safety, wages, working conditions, or any other aspect of off-campus employment without limitation. It is the responsibility of students and alumni to perform due diligence in researching employers when applying for or accepting private, off-campus employment and to thoroughly research the facts and reputation of each organization to which they are applying. Students and alumni should be prudent and use common sense and caution when applying for or accepting any position.

Red Flags to Consider

Tips to avoid fraudulent employers when using online job and internship sites

- Research company websites thoroughly: Does the company have a website? Does the website match up with the posting? Does the website look legitimate? Look to see if the organization is using a company domain versus a general Gmail or Hotmail account. Match the e-mail address to the company domain. Watch for e-mail addresses that are similar looking, but not the same. Look for "stock photos," grammatical errors, and poor use of English language.
- Be leery of non-approved employment flyers on college campuses and other establishments.
- Use social media to research each employer, e.g., Facebook, Twitter, Snapchat, LinkedIn.
 Research the company on websites such as Glassdoor.com for feedback and complaints.
- Be cognizant of unsolicited e-mails that are not specifically directed to you. Many employers have access to resumes via career centers. Therefore, reach out to your career center should you have any concerns or questions.
- Keep your private information private! Don't share personal information, e.g., social security numbers, banking information, credit or debit card numbers, PINs, passwords, birthday, address, mother's maiden name).
- Never process ANY financial transactions. For example: Some companies offer opportunities to "make money really quick." They will offer a "one day only special."
 Their intent is to defraud you by sending or wiring money to your bank account. They will ask you to cash the check or send the monies to other accounts. Once your bank or financial institution processes the scammer's check or financial request, you may be

- informed the monies are invalid or "not real." In the meantime, you are held responsible for the funds the bank has sent at your direction to other accounts.
- Fraudulent companies are phishing for the unsuspecting, including you. Be aware of what you share and post online. If you feel uncomfortable or aren't sure about certain companies or employers, talk to your career center.

If a student or alumni has given any personal information to a fraudulent employer, the following steps should be taken:

NOTIFY <u>EMPLOYERRELATIONS@ECU.EDU</u> IMMEDIATELY

- 1. Collect the following information.
 - Name of the company
 - Details of fraudulent action on the part of the employer
- 2. Contact Bank: If you have sent or received money from a fraudulent employer, immediately contact your bank or credit card company to protect the account and dispute any charges.
- 3. Report to local police. Police are responsible for conducting an investigation (regardless of whether the scam artist is local or not). If you are an on-campus student, you would want to notify ECU Campus Police and if you are off campus you would want to contact the Greenville Police.
- 4. File a Report with the FTC: Report the job scam to the Federal Trade Commission, the nation's consumer protection agency, which collects complaints about companies, business practices, and identity theft at the link below.

https://www.ftccomplaintassistant.gov/?utm_source=takeaction#crnt&panel1-1