Tips on Fraudulent Employers and Jobs

Fraudulent Employers: Tips for Students

The University Career Services center makes every effort to screen employers and job postings on Handshake. However, the center acts only as an intermediary between employers posting job opportunities and candidates searching for job opportunities.

By the NACE Principles for Ethical Professional Practice Committee
Unfortunately, not all employment opportunities are legitimate; entities may pose as employers as part of a scam to elicit personal information from or otherwise defraud their victims. Career centers and students alike must be vigilant about fraudulent employers and should identify steps to take to verify the legitimacy of an employer.

STUDENTS: RED FLAGS TO CONSIDER (NACE)
What are some “red flags” students should be aware of and consider 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 job 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 cautious 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.

**Bottom line, if you have any questions, talk to someone before pursuing any job opportunity. If it sounds too good to be true, it probably is.**

If you are suspicious of a job posting or email, immediately end communication with the employer and contact University Career Services at ucs@unc.edu [1].

If You Have Been the Victim of a Job Scam:

- Contact UCS at ucs@unc.edu [1] to report the incident and receive additional support navigating your next steps and action.
- If the incident occurred completely over the internet, you can file an incident report with the US Department of Justice or by calling the FTC at 1.877.FTC.HELP (1.877.382.4357).
- Once you are hired, if you have any concerns about the legitimacy of the company or believe the work environment to be unsafe, contact the US Department of Labor.

*The majority of this content comes from the National Association of Colleges and Employers [2]*

---

**Source URL:** https://careers.unc.edu/students/tips-fraudulent-employers-and-jobs

**Links**

[1] mailto:ucs@unc.edu