University of Houston-Downtown
Marilyn Davies
College of Business
Career Center

HOW TO SPOT A "FRAUDULENT" EMPLOYER

Not all employment opportunities are legitimate. Some organizations may pose as potential employers to collect personal information from or to defraud job seekers. Here are steps you can take to verify the legitimacy of an employer:

- 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 someone in your career center.

Bottom line, if you have any questions, talk to someone before pursuing any opportunity. If an opportunity sounds too good to be true, it probably is. If you believe you are the victim of a scam, contact your local police.

Courtesy of the National Association of Colleges and Employers.

If you receive a suspicious message to your Gatormail, notify UHD IT Security at security@uhd.edu or 713.221.8638.

For more tips on identifying scam emails go to www.uhd.edu/information-security/Pages/Job-Scams.aspx