Characteristics of a Fraudulent Employer

Wiring Money and Private Information
A fraudulent employer may
• Ask for personal details, such as bank account information, social security numbers, credit card numbers, Paypal information, passport information—do not provide this information to the employer even if they say it’s a condition for employment and/or needed to conduct a background check.
• Offer to send a check in the mail to you as an incentive for employment—do not send a check to the employer or wire money as an investment in your employment with the company. Paying employers is not a part of the job search process.
• Send you a large check in the mail unexpectedly—do not accept or cash these checks.
• Request access to your bank account so that money can be wired to you—do not share your bank account number with a prospective employer.

Email and Communication
• A fraudulent employer may contact you but isn’t willing to share his/her contact information or can be difficult to reach.
• The domain name for a fraudulent employer contact’s email is slightly misspelled or doesn’t match that of the company that is hiring. For example, if the employer is Nike, then the correct email address would read @nike.com. A fraudulent employer, however, may misspell the email address slightly and have it read @nikke.com.
• The domain name of a fraudulent employer contact may appear as a personal email such as @yahoo.com and @gmail.com. While some startups, for example, may have staff using personal emails, the use of personal emails should raise a red flag for the job seeker until additional information about the company and position is verified.
• The email address of a fraudulent employer may combine a personal domain name with a more official company name: ie- IBM-recruiter@yahoo.com. However, most legitimate employer email addresses will have their company name as the domain name and should have the following format: ie- j.smith@ibm.com.

Employer Information
A fraudulent employer website may not provide much detail about the company and/or it may not have the position posted on the website. An exception to this may be a startup organization that is working on constructing their website, in which case a conversation with the contact from the organization would provide a way for a student to acquire additional information about the organization.

Characteristics of a Fraudulent Job Posting:
• Multiple grammatical and spelling errors throughout the posting.
• A variety of font types and font sizes used.
• The job is an opportunity that seems too good to be true with a large salary range.
• Information regarding the company and/or the opportunity is difficult to come by and few details are provided, such as the company name and the location of the position.

Tips and Resources for Researching Employers
Think you've encountered a fraudulent employer? Want to check the legitimacy of an employer? The sites below can assist you with identifying employers that have been reported as fraudulent.
• Google the employer—sometimes scam reports on the employer will appear as a search result.
• Federal Trade Commission
http://www.ftc.gov/jobscams
• Domain White Pages—Will provide when the company site was created. If it is less than a year old, be on guard
http://www.domainwhitepages.com/
• Better Business Bureau
https://www.bbb.org/

What Should You Do if You Spot a Fraudulent Employer or Job Posting in CareerConnections
To report the suspected fraudulent activity
• Call the Duke Career Center at 919-660-1053 or send an email to career-employer@studentaffairs.duke.edu.
• Stop communication with the employer immediately.
• Do not accept or cash check or money orders.