Identifying and avoiding Fraudulent Jobs and Scams

It is very important that you educate yourself about potential scams. Fraudulent jobs or scams are typically generic and non-specific in order to garner the greatest possible number of applicants. Jobs for file clerk, personal assistant, envelop stuffer, mail services, mystery shopper, and the like should be approached with caution and read thoroughly. **Use your best judgment, research and discretion when applying for jobs.**

Disclaimer

The Office of Career Development and Placement Assistance posts jobs through FutureLinks to assist students with their job search. However, a posting does not constitute an endorsement or recommendation of any employer by the University, or any relationship between the employer and the University. The University makes no express or implied representations, warranties or guarantees about job listings or the accuracy of the information provided by the employer. The University has no control over any links embedded in a job posting and is therefore not responsible for the accuracy, legality or any other aspect of the content of a link(s). The University is not responsible for safety, wages, working conditions, or any other aspect of off-campus employment without limitation.

Whether a student pursues an employment opportunity through FutureLinks or any other forum, such student is responsible for performing due diligence in researching employers when applying for or accepting employment and for thoroughly researching the facts and reputation of each organization to which they are applying. For reference, the University has developed tips relating to identifying and avoiding fraudulent jobs and scams, which can be found here. Students should be prudent and use common sense and caution when applying for or accepting any position.

Indicators that a job MAY be fraudulent?

1. You are asked to provide your credit card, bank account numbers, or other personal financial documentation or position requires an initial investment, such as a payment or deposit of a mailed check by wire service or courier.
2. You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
3. You receive an unexpectedly large check (checks are typically slightly less than $500, generally sent or deposited on Fridays).
4. The posting appears to be from a reputable, familiar company (often a Fortune 500) yet, the domain in the contact's email address does not match the domain used by representatives of the company (this is typically easy to determine from the company's website). Another way to validate is to cross reference the open positions on the company's official website.
5. The contact email address contains the domain @live.com.
6. The posting includes many spelling and grammatical errors.
7. You are asked to provide a photo of yourself.
8. The posting neglects to mention the responsibilities of the job. Instead, the description focuses on the amount of money to be made.

9. The employer responds to you immediately after you submit your resume. Typically, resumes sent to an employer are reviewed by multiple individuals, or not viewed until the posting has closed. Note - this does not include an auto-response you may receive from the employer once you have sent your resume.
10. The position indicates a "first year compensation" that is excessively higher than the average compensation for that position type, or lists a very wide range *(i.e. "employees can earn from $40K - $80K the first year!")*.
11. Look at the company's website. Does it have an index that tells you what the site is about; or does it contain information only about the job you are interested in? Scammers often create quick, basic web pages that seem legit at first glance.
12. Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc. - this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well-hidden.
13. When you Google the company name and the word "scam" (i.e. Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is: http://www.ripoffreport.com.
14. Google the employer's phone number, fax number and/or email address. If it does not appear connected to an actual business organization, this is a red flag. The Symplicity team often uses the Better Business Bureau (http://www.bbb.org/us/consumers/), Hoovers (http://www.hoovers.com/) and AT&T's Anywho (http://www.anywho.com/) to verify organizations.
15. The employer contacts you by phone; however there is no way to call them back. The number is not available.
16. The employer tells you that they do not have an office set-up in your area, and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).

What should I do if I think that I am already involved in a scam?

1. Notify the police and take other legal action as desired. Call the Pitt Police at 412-624-2121. Complaints may also be submitted to http://www.ic3.gov/default.aspx. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state).
2. Notify the Office of Career Development and Placement Assistance immediately so the job can be taken down and the employer blocked to prevent more students from applying. (412-383-HIRE).
3. If it is a situation where you have sent money to a fraudulent employer, you should contact your bank or credit card company immediately to close the account and dispute the charges.
4. If the incident occurred completely over the Internet, you should file an incident report with the: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

For more information about fraudulent jobs, visit http://www.consumer.ftc.gov/articles/0243-job-scams.

Common Job Scams to look out for:

1. **419 scams**
   A type of fraud and one of the most common types of confidence trick. The scam typically involves promising the victim a significant share of a large sum of money, which the fraudster requires a small up-front payment to obtain. If a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears.
2. **Nigerian Check Cashing Scam**
   The Nigerian check cashing scam usually involves transferring funds internationally. The scam artist attempts to reassure the victim by offering apparently legal contracts, forged or false documents bearing company letterhead, false letters of credit, payment schedules and bank drafts. Once the scammer has obtained the victim's trust, checks, money orders or wire deposits are sent to the victim for "processing." The victim is asked to cash the check or money order (wire deposits will send the money directly to the victim's account) and send a percentage of the funds back to its origination. The need for the "middle man" is often explained as being a way around international fees or taxes. Once the funds are sent back to the scammers (usually the victim is told to keep a percentage for themselves, as payment for their services), the victim's bank or financial institution learns that the check/money order/wire transfer was fraudulent. The funds are then subtracted from the victim's account and he or she is made liable for the lost money.
3. **Reshipping**
   Reshipping scams often begin with an employment offer, usually via e-mail. As with the Nigerian scam, these "employers" offer bogus contracts and other documentation to make them appear legitimate. Once the victim's trust has been obtained, packages are shipped to the victim's residence with instructions to reship the packages to another address. Once the package has been reshipped, the victim is "guilty" of receiving and shipping stolen property. This often leads to a visit from police, as the return address or shipping receipts lead back to the victim.
4. **Phishing**
   Phishing scams are cleverly hidden attempts to get your account information. These e-mails appear legitimate -- with professional-looking company logos and information -- and often claim that there is an urgent need for you to log into your account and verify personal information. If you receive one of these e-mails, check the destination URL on the provided link before attempting to login or submit any information; the links could actually lead the recipient to a false Web site. The victim may be asked to update their banking information or other sensitive information, which the site owner (aka scammer) will use for any number of illegal purposes.

Symplicity Corporation. *Protect Your Student from Fraudulent Employers.* http://www.symplicity.com/blog/_1/17/fraud_posting_tips. 2010. Web. Accessed December 8, 2014.

Federal Trade Commission. *Consumer Information-Job Scams.* http://www.consumer.ftc.gov/articles/0243-job-scams. 2013. Web. Accessed December 8, 2014.

Career Builder. *Too Good to Be True? 6 Common Job Scams.* http://www.careerbuilder.com/article/cb-563-job-search-too-good-to-be-true-6-common-job-scams/. 2009. Web. Accessed January 15, 2015.

Wikipedia. *419 Scams*. http://en.wikipedia.org/wiki/419_scams. 2015. Web. Accessed January 15, 2015.