Fraudulent Job Postings Warning

Since it is impossible to ensure that every job posting is legitimate, we are sharing common "red flags," things that alarm us in postings, so you too, can attempt to identify such scam and fraudulent job postings.

The following "red flags" are general markers to help you conduct a safer job search and protect your identity. These "red flags" in no way cover all possible instances of fraud or all the red flags. Therefore, please always use your own discretion when applying to a position or interacting with a potential employer.

Fraudulent job postings try to take your money, personal information, or both. The jobs often appear easy and convenient ways to make money with very little effort.

Core Essentials to Avoiding a Job Posting Scam

- Do not give your personal bank account, PayPal account, or credit card information to a new employer.
- Do not agree to have funds or paychecks directly deposited into any accounts by a new employer. (Arrangements for direct deposit or paycheck should be made during your first day or week of actual employment on site – not before.)
- Do not forward, transfer or send by courier (i.e. FedEx, UPS), or "wire" any money to any employer, for any employer, using your personal account(s).
- Do not transfer money and retain a portion for payment.
- Do not respond to suspicious and/or "too good to be true" unsolicited job emails.
- In general, applicants do not pay a fee to obtain a job (but there are some rare exceptions – so be careful, and consult with a professional at University Career Services first).

Red Flags: How to Identify a Potentially Fraudulent Job Posting

(Reference: Georgia State University Career Services; Kevin Gaw, PhD & Melanie Jauch)

1. You must provide your credit card, bank account, PayPal, or other personal financial information.

Legitimate jobs will not ask for this kind of information on an application, by phone or email.

2. The contact email address contains a non-business email domain or a personal email address. Sometimes the posting may even appear to be from a reputable, familiar company, but the email address does not match the domain used by representatives of the company.

Legitimate recruiters are directly associated with the company for whom they work. Therefore, the email addresses used should match the company's domain. The email should always come from an official email address that reflects the organization's domain or a subsidiary of the organization.

3. You are asked to forward payments, by wire, courier, bank transfer, check, PayPal, etc…

Never forward payments – they want to access your bank account and money.

4. The position requires an initial investment, for instance, having to purchase equipment or products in order to earn a wage or paying for necessary training.

Legitimate jobs never ask for an initial investment. However, some network marketing companies may ask you to pay a fee (or "pay a deposit") to obtain their sample product for demonstration. In essence, they are still asking for money so you can have a job.

5. The "company" website is not active, does not exist, or re-routes users to another website unaffiliated with the "company."

If the listed website is not working, does not exist, or the URL goes to another unassociated website, then the employment opportunity is most likely not real.

6. The posting includes many spelling and grammatical errors.

If the employyr kant spel, du u reely wanna werk 4 them? Poor spelling and grammar suggests the job announcement was written by a non-professional and therefore the job is probably not legitimate.

7. A high salary or wage is listed for a job that requires minimum skills.

This is designed to entice you, to get you to apply. Think wisely – how many legitimate companies can afford high wages for low skilled jobs? Why would they pay these wages?

8. The position states you will be working from home, need access to a personal computer, etc.

Most formal jobs will have an office as your base. "Working from home" is often a "convenience hook" that takes advantage of people who want an easy job situation. In addition, working from home forces you to use your personal resources. However, working from home may be legitimate so carefully research these jobs.

9. The job is a start-up business, a new small private company, and entrepreneurial enterprise just getting off the ground.

These postings create excitement for some students because you get to be "on the ground level." These may be very legitimate jobs but it is important to research them carefully.

10. The position initially appears as a traditional job, but upon further research, it sounds more like an independent contractor opportunity.

Independent contractor jobs ("1099 type self-employment) mean you will be self-employed and accountable for associated IRS tax obligations. Your will not have benefits and are not really an employee of the company. No contract? Don't apply!

11. You are offered a large payment or reward in exchange for allowing the use of your bank account (often depositing checks or transferring money) or you receive an unexpectedly large check.

Legitimate employers do not need to use your bank account! Also, these checks typically bounce – but you are then held responsible for all the bank charges and any money used, wired, or processed.

12. You are asked to provide a photo of yourself.

In the US, most legitimate jobs do not ask for a photo. On some very special applications a photo may need to be attached – but this only happens with profession-specific jobs and is actually very rare.

13. The posting neglects to mention what and where the responsibilities of the job actually are. Instead, the description focuses on the amount of money to be made.

Legitimate employers will openly and willingly provide a detailed job description of the job responsibilities and duties to see if you are a good fit for the position and will also state the work location. Any "employer" who hesitates…be careful!

14. The employer responds to you immediately after you submit your application. This does not include an auto-response you may receive from the employer stating receipt of your application.

Legitimate employers take time to sort through applications to find the best candidates. Fraudulent jobs are just looking for personal information, not your skills, which is why they respond immediately. They are hoping an immediate response makes you feel special – a trick used to get you to share personal information.

15. It is difficult to find an address, actual contact information, a name, the company name, etc.

Fraudulent job postings are despicable and designed to take you in without knowing you are being scammed, so scammers will try to keep themselves well-hidden.

16. The employer contacts you by phone, however, there is no way to call them back. The number is not available or disconnected.

A legitimate business wants to be reachable for clients, business partners, and applicants so the number will be active!

17. The company website is not detailed and only contains information about the job in which you are interested.

Legitimate organizations and companies use their websites to attract clients and customers, not just potential employers. Check the URL – is it a real company website? Scammers often create quick, basic webpages that seem legitimate at first glance.

18. The employers tells you that there is no office in your geographic area and you will need to help them get a "new" office up and running.

Sounds exciting, but, these postings often include a request for your banking information, supposedly to help the employer make transactions. What they want is access to your bank account and money.

19. Research (i.e. Google) the employer's phone number, fax number, and/or email address to be sure it is connected to an actual business organization.

If information about the company is difficult to find, it is most likely a scam.

Researching Possible Scams

You can check to see if a company is legitimate through various websites (some listed below).

- **Better Business Bureau**: http://www.bbb.org/
- **Hoover's**: http://www.hoovers.com/
- **White Pages**: http://www.whitepages.com/business

If you contact the company directly, you can ask if the person actually works there. Don't share personal information unless you are confident that the person and the company they work for are legitimate.

If you search the internet using key phrases, such as "fraudulent job postings" or "scam job postings," you'll get many online articles and reports that may be helpful.

You can also search the company name with the word "scam" to get a variety of internet hits associated with the company. Know that some of the links that come up may be just discussion, but there may be actual articles or references.

Protect Your Personal and Private Information

For job applications, you should not provide your credit card number, bank account number, PayPal account, or any PIN number over the phone or online.

Many job applications will ask you to provide your social security number and date of birth, but this information is not solicited over the phone or email. This information is typically a part of a formal job application that candidates complete in writing, often on the day of their first in-person interview.

Always know with whom you're sharing personal information – and how it will be used. If someone asks for sensitive personal information, get the person's name, the company they work for and the phone number. If they hesitate, something's up!

What to do if you Discover You've Been Scammed

If you have encountered a fraudulent posting, company or organization, please contact the College of the Mainland Career Services via phone (409.933.8524) or email ckater@com.edu so the posting can be investigated and appropriate action can be taken.

You should immediately contact the local police. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state).

If you have sent money to a fraudulent employer, you should contact your bank and/or credit card company immediately to close the account and dispute the charges.

If the incident occurred completely over the internet, you should file an incident report with The United States Department of Justice (www.cybercrime.gov) and the Federal Trade Commission (http://www.ftc.gov) or 1-877-FTC-HELP (1-877-382-4357)

File a complaint with the Internet Crime Complaint Center (www.ic3.gov)