Being Aware of Fraudulent and Scam Job Postings

THE UNIVERSITY OF TENNESSEE KNOXVILLE

CENTER FOR CAREER DEVELOPMENT & ACADEMIC EXPLORATION

201 Student Union
career.utk.edu
865-974-5435

The information contained in this booklet was originally prepared by Kevin Gaw, PhD, and Melanie Jauch of Georgia State University. We would like to thank them for sharing this valuable resource with The University of Tennessee Center for Career Development & Academic Exploration.

Fraudulent and Scam Job Postings

The University of Tennessee Center for Career Development & Academic Exploration (CCDAE) offers Handshake as a resource for employers to connect with UT students and alumni seeking internships, part-time jobs, and full-time positions. We strive to keep fraudulent postings off Handshake by using some common "red flags" that are considered suspicious. "Red flags" don't automatically remove a job posting – we research the company and posting if suspicion arises and then make a decision. You should research suspicious companies or postings, too – or don't apply. We are sharing these "red flags" below, so you, too, can attempt to identify such scam or fraudulent postings. Our guidance: never apply to a suspicious job.

The following "red flags" are general markers shared to help you conduct a safer job search and to help you 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 or your personal information. The jobs often look like easy and convenient ways to make money with very little effort. The old adage is accurate: If it looks too good to be true, then it probably isn't true!

Contents:

Core essentials to avoiding a job posting scam:

1. Do not give your personal bank account, PayPal/Venmo/Zelle account, or credit card numbers to a new employer.
2. Do not agree to have funds or paychecks direct deposited into any of your accounts by a new employer – you should know them first. (Most employers give the option of direct deposit or a paycheck and make these arrangements during your first day or week of actual employment, on site – not before.)
3. Do not forward, transfer, send by courier (EX: FedEx, UPS), or "wire" any money to any employer, for any employer, using your personal accounts(s).
4. Do not transfer money and retain a portion for payment.
5. Do not respond to suspicious and/or "too good to be true" unsolicited job emails.

6. 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 the CCCDAE first).

If you are ever concerned about a job or internship posting, the career center will help you research the posting. Contact Katie Wiley, Assistant Director, or Miciah Burns, Career Systems Manager, for such assistance: 865-974-5435

How to identify a potentially fraudulent job posting

Red Flags: **The "employer" asks for, or posts….***	**But in truth,…**
You must provide your credit card, bank account numbers, PayPal/Venmo/Zelle account, or other personal financial documentation.	**Legitimate jobs will not ask for this kind of information on an application or via email or by phone.**
The posting appears to be from a reputable, familiar company (often a Fortune 500 Company). Yet, the domain in the contact's email address does not match the domain used by representatives of the company.	**Legit recruiters are directly associated with the company for whom they work. Therefore, the email addresses used should match the company's domain.**
The contact email address contains the domain @live.com, or a non-business email domain	**The email should always come from an official email address that reflects the organization's domain or a subsidiary of the organization. Employer email addresses from Gmail, Yahoo!, etc., all suggest the employer does not have an official company domain and may not be a legitimate enterprise; research is required to verify status.**
The "employer" is using a personal email address instead of a company email address	**Same as above – the email should be associated with the company. Employment communications are always official – so why not use an official email address?**
You are asked to forward payments, by wire, courier, bank transfer, check, or through PayPal…	**This is a clear red flag. Never forward payments – they want to access your bank account and money!**
The position requires an initial investment, such as a payment by wire service or courier (EX: UPS, FedEx).	**Legitimate jobs never ask for an initial investment. <u>Never!</u> Some network marketing companies may ask you to pay a fee (or "pay a deposit") to obtain their sample product for demonstration. We do not post such positions as this is the same thing – they are asking for money so you can have a job.**
The "company" website is not active, does not exist, or re-routes users to another website unaffiliated with the "company," even though	**This is a significant red flag because if they listed the website and it is not working or does not exist, or if the URL goes to another unassociated**

the "employer" listed a URL or website in the job announcement	**website, then the employment opportunity is most likely not real.**
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 a legitimate job.**
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?**
The position states you will be working from home	**This is a red flag because most formal jobs have you working at an office or out of an office, using the office as your base. "Working from home" may be one of those "convenience hooks" that takes advantage of people who want an easy job situation because of their busy schedules.** **Working from home may be legitimate, and you may be a "1099 independent contractor" rather than a regular employee - meaning – you will be responsible for all your tax liabilities. Always carefully research these jobs.**
Key terms and phrases are used that suggest access to the top level of company management and you are a student (examples: CEO, Co-founder, CFO, etc.)	**It is possible selected candidates will have access to top level management personnel of a company, but typically this does not happen when you are a student. The times it does happen is when there is a specific management training program, for example, that is designed to have c-level leaders meet future leaders within the company. These programs are formalized and have printed documentation (brochures, part of the recruiting materials, etc.) Just so you know: even seasoned employees often have infrequent access to the top. Some fraudulent job postings entice applicants with such lofty access – it sounds so good!**
The job is for a start-up business, a new small private company, and entrepreneurial enterprise just getting off the ground…	**These are red flags simply because new business efforts are used by scam artists as an exciting creative hook – because you get to be in "on the ground level." These may be very legit jobs – you just have to research them carefully.**
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. You will not have benefits and are**

	not really an employee of the company. A contract needs to be made with the parent company. No contract? Don't apply!
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).	**Legitimate employers do not need to use your bank account! This is an old scam with some new twists. Don't allow "employers" to use your bank account since these checks are often fraudulent and will bounce, leaving you to cover the consequences.** **In-home "check processing services" are a recent version of this scam.**
You receive an unexpectedly large check (checks are typically slightly less than $500, generally sent or deposited on Fridays).	**Remember this old and very true piece of wisdom: If it sounds too good to be true, then it probably is not true!!! These checks typically bounce –but you are held responsible for all the bank charges and any money you have used, wired, or processed.**
You are asked to provide a photo of yourself.	**In the United States, most legitimate jobs do not ask for a photo. Usually, the "employer" does not know this standard of practice in the US, indicating they are posting from another country.** **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. Be careful as photos can be used for selection reasons not associated with your skills, abilities, and knowledge.**
The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys. Check Writing and Processing.	**It is not to say that every envelope stuffer job you come across is a fraudulent posting! However, these positions often offer flexible hours and great pay -- and may be after your information… Be Cautious!**
The posting neglects to mention what the responsibilities of the job actually are. Instead, the description focuses on the amount of money to be made.	**Legitimate employers will provide a good description of the job responsibilities and duties to see if you are a good fit for the position. The description should state the work location. They will do this openly and willingly. And any "employer" who hesitates…. Be careful!**
The employer responds to you immediately after you submit your résumé. Typically, résumés sent to an employer are reviewed by multiple individuals, or not viewed until the posting has closed. Note - this does not include an auto-	**Legitimate employers take their time to sort through applications to find the best candidates. Fraudulent jobs are just looking for your personal information, not your skills, which is why they respond immediately. They are**

response you may receive from the employer once you have sent your résumé.	**hoping an immediate response makes you feel special – a trick used to get you to share personal information.**
Watch for anonymity. If it is difficult to find an address, actual contact information, a name, the company name, etc. - this is cause to proceed with extreme caution.	**Fraudulent postings are despicable and are designed to take you in without you knowing you are being scammed, so the scammers will try to keep themselves well-hidden.**
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!**
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.	**Legitimate organizations and companies will use their website to attract clients and customers, not just potential employees.** **Check the URL – is it a real company website?**
The employer tells you that they do not have an office in your geographic area and will need you to help them get a "new" office up and running	**Sounds exciting, right?! 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 your money.**
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.	**You can use the Better Business Bureau (http://www.bbb.org/us/consumers/), Dun&Bradstreet (https://www.dnb.com/) and AT&T's Anywho (http://www.anywho.com/) to verify organizations.**

If you believe you have encountered a fraudulent job posting, please contact Katie Wiley with the Center for Career Development & Academic Exploration at 865-974-5435 so we can investigate.

Researching Possible Scams

Research the company to see if they are legitimate. Many people check companies through websites like the Better Business Bureau, local Chambers of Commerce, and other listings.

BBB: http://www.bbb.org/us/consumers/
Chambers of Commerce: http://www.uschamber.com/chambers/directory
ATT: http://www.anywho.com/

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 come up with many online articles and reports, such as:

http://talkabout.hubpages.com/hub/Job-Hunting--10-Red-Flags-that-the-Job-Post-in-Craigs-List-may-be-a-Scam

If you Google the company name with the word "scam" in the phrase (e.g., "ACME Inc scam"), you will get a variety of internet hits associated with the company. Know that some of the links that come up may be just chatter – but there may also be articles or references to actual.

Also try: http://www.ripoffreport.com for scam reports.

Protect Your Personal and Private Information

For job applications, you should not provide your credit card number, bank account number, PayPal/Venmo/Zelle 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 this sensitive personal information, get the person's name, the company they work for and the phone number. If they get squirmy when you ask – something's up!

What to do if you discover you've been scammed

If you have encountered a fraudulent job posting, please contact the Center for Career Development & Academic Exploration at 865-974-5435 so we can investigate and/or remove the employer from the system.

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: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

The list of red flags above and the comments and suggestions are not necessarily comprehensive and definitive; they are provided to assist you with your job search and to help you be aware of fraudulent and scam job postings.