# Red Flags for Fraudulent and Scam Job Postings

While thousands of legitimate job opportunities are posted in SeaWork and other online listings every year, students and alumni need to be vigilant about the integrity of any employer. All internships and jobs in SeaWork are individually reviewed before being posted. However, some opportunities may turn out to be different than what was described. Even though scam listings rarely occur, even one can harm you with lost time, money or personal identity. Therefore we have developed this checklist of red flags to look out for with fraudulent and scam job postings.

The following "red flags" are general markers 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!

**If you are concerned about a job or internship posting in SeaWork or elsewhere, the UNCW Career Center will help you research the posting. For assistance, contact the Career Center at 910-962-3174, careercenter@uncw.edu, or drop by our office in Fisher University Union 2035.**

**Depending on the circumstances of a job scam, you may want to immediately contact the police, your bank, credit card company, and state or federal regulatory offices. Some of these resources are listed at the end of this document.**

## Core essentials to avoiding a job posting scam:

1. ***A lucrative new job is yours! Identity verification required.*** **Do not give your personal bank account, PayPal account, credit card or PIN numbers, Social Security number or other personal financial information to a new employer.**

2. ***Your first impressive paycheck is attached! Deposit within 24 hours.*** **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- or by telephone or email.)**

3. ***Work at home and make big money as a check processing agent!*** **Do not forward, transfer, send by courier (EX: FedEX, UPS), or "wire" any money to any employer, for any employer, using your personal account(s).**

4. ***Make money while you sleep!*** **Do not respond to suspicious and/or "too good to be true" unsolicited job emails.**

5. ***High paying professional jobs in Wilmington guaranteed! Join Top Tier Placement Group today!*** **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 UNCW Career Center first).**

## How to identify a potentially fraudulent job posting

| **Red Flags:**<br>**The "employer" asks for, or** | **But in truth,...** |
|---|---|
| You must provide your credit card, bank account numbers, PayPal account, PIN numbers, Social Security number, or other personal financial documentation. | Legitimate jobs will not ask for this kind of information on an application or via email or by telephone. |
| 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. | 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!, live.com, 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. |
| 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! In-home "check processing services" are a recent version of this scam. |
| 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. Never! 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 the "employer" listed a URL or website in the job announcement | 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 website, then the employment opportunity is most likely not real. |
| The posting includes many spelling, grammatical, capitalization or punctuation 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 nonprofessional 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.<br>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. |
| 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 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 U.S., indicating they are posting from another country.<br>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 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. | 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 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. Or they are out of the country on business. | 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. And they want a legitimate-sounding reason for not meeting you in person. |

| | |
|---|---|
| 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 (www.bbb.org/council/consumer-education/), Chambers of Commerce (www.uschamber.com/chamber/directory ) Hoovers (www.hoovers.com/ ), and AT&T's Anywho (www.anywho.com/ ) to verify organizations.<br>Come into the UNCW Career Center – we have other databases, too! |

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

**Job Scam Video and information from the Federal Trade Commission**
*http://ftc.gov/jobscams*

**Job Scams List: A – Z List of the Most Common Job Scams**
*http://jobsearch.about.com/od/jobsearchscams/a/job-scams-list.htm*

**The Ripoff Report** *www.ripoffreport.com*

**Avoiding Online Job Scams** *www.privacyrights.org/avoiding-online-job-scams*

**Message Boards for Job, Work-At-Home and Multi-Level Marketing (MLM)/Pyramid Scams***http://www.scam.com/forumdisplay.php?f=1*

## What to do if you discover you've been scammed

**If you have encountered a fraudulent job posting, please contact the UNCW Career Center @ 910-962-3174 so we can remove the job and employer from SeaWork.**

You should immediately contact your local police. The police are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state). Wilmington Police Department: (910) 343-3600

If you have sent money to a fraudulent company, 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 at this site: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

The list of red flags, comments and suggestions in this document 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.

*This guide adapted from information from the National Association of Colleges & Employers, Georgia State University Career Services, and the Federal Trade Commission.*