****

**BE A SMART JOB SEEKER AND AVOID ONLINE FRAUD!**

Online scam artists take advantage of people looking for jobs to try and get them to apply for fake jobs or pay money for false job leads.

Students, in particular, must keep a close eye out for possible scams, phishing schemes, or fraudulent employers.

**Please pay close attention to job postings to look for the following red flags or warning signs**:

* You are requested to provide your credit card, bank account numbers, or other personal financial documentation.
* The employer has a contact email address that is not a primary domain. For example, the posting lists the company name as “Omega International” but they provide a Yahoo! email address.
* The position requires an initial investment, such as a payment by wire service or courier.
* The posting includes many spelling and grammatical errors.
* The position initially appears as a traditional job but upon further research, it sounds more like an independent contractor opportunity.
* 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).
* You receive an unexpectedly large check (checks are typically slightly less than $500, generally sent or deposited on Fridays).
* You are asked to provide a photo of yourself.
* The position is for any of the following: Envelope Stuffers, Home-based Assembly Jobs, Online Surveys.
* 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.
* The position indicates a "first year compensation" that is in excess to the average compensation for that position type.
* 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.
* Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc. - this is cause to proceed with caution.
* The salary range listed is very wide (i.e. "employees can earn from $40K - $80K the first year!")
* 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 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).

**Keep reading to learn how to protect yourself from scams**

**How to protect yourself from scams**

1. If you post your resume online, make it private. When it comes to resume databases, job search sites put the responsibility on the job seeker to understand the risks involved in posting a resume online.
2. If you are unsure about an employer’s reliability, check with outside sources like the Better Business Bureau ([www.bbb.org](http://www.bbb.org)) or local consumer protection offices.
3. Do not give out your credit card or bank account information over the phone unless you are familiar with the company and agree to pay for something. Anyone who has your account information can use it to take money from your accounts improperly.
4. Unless you are applying to the Federal or State government, never put a Social Security Number on your resume. (See tip #4 in the previous section about legitimate government job posts.) Keep your SSN off of your resume, and be very cautious about emailing it to people who ask for it. You should only give your SSN to an employer after you have fully validated them as a legitimate employer.
5. Follow up with the corporate offices of any company listed in an ad by an employment service, to find out if that company is really hiring.
6. If your resume has been posted online for several months, it is a good idea to just take it down and start over. In the World Privacy Forum year-long Job Search Study, research showed that the best job offers usually came within the first month of the resume being posted. After that, you are more likely to receive illegitimate job offers.
7. If you decide to post your resume to a site, consider using an email address that you can cancel if you start getting spam, and don’t give out your full name, phone number, or home address. Use a post office box, and do not give your street address to an employer until you have verified them fully.
8. When you post a resume online, do not include your references in order to protect them from scam artists.
9. School information is tricky. Education is a necessary category on a resume. The problem is that anyone can call up your school and get what is called “directory information” without your consent. This can include your name, date of birth, home address, and other vital information. If you are a current college student, you can sign what is called a FERPA form to stop your school from giving this information out to just anyone. (FERPA stand for Family Educational Rights and Privacy Act.)

Sources of the above information:

Better Business Bureau ([www.bbb.org](http://www.bbb.org))

Federal Trade Commission ([www.ftc.gov](http://www.ftc.gov))

Privacy Rights Clearinghouse ([www.privacyrights.org](http://www.privacyrights.org))

World Privacy Forum ([www.worldprivacyforum.org](http://www.worldprivacyforum.org))

Overseas Digest ([www.overseasdigest.com](http://www.overseasdigest.com))

**Please do not hesitate to contact Career Services if you have any questions, or to report a fraudulent posting.**

**CAREER SERVICES**

**(209) 667-3661 | www.csustan.edu/career | career@csustan.edu | @stanstatecareer**