Don't Be A Victim:

Know the Signs of Fraudulent Employers and Postings

HOW TO TELL IF A JOB IS REALLY A SCAM

TOP 10 JOB SCAM WARNING SIGNS

The office of Career Services at Vanguard University makes every effort to check the legitimacy of opportunities being connected to the University through Handshake. At Vanguard we have many internet, email and Handshake safeguards in place to reduce the threat of internet and emails attacks using hardware and software applications, however, we cannot guarantee 100% safety from fraudulent employers.

Vanguard University makes no guarantee about positions listed on Handshake and is not responsible for safety, wages, working conditions, or other aspects of employment. It is the responsibility of each individual job seeker to research the validity of the organization(s) to which he/she is applying and verify the specific information for each posting. Job seekers should exercise due diligence and use common sense and caution when applying for or accepting any position.

For your privacy and protection when applying to an opportunity online, it is advisable that you do not provide your social security number or credit card or bank account information, or perform any sort of monetary transaction for an employer.

NOTE: Emails promoting jobs that DO NOT have the Career Services logo and/or Career Services contact information embedded in the email are most likely scams. Please contact Career Services at (714) 619-6477 or careerservices@vanguard.edu if you have any questions or concerns regarding the legitimacy of an employer posting.

When it comes to job scams, while each scam typically has a different design, most require their target to send money in a form that is not easily traced and, in a way, that the money cannot be recovered. The scammers often use a technique called 'spoofing' to make it appear as though the email came from an authentic VU email

address. Typically, the "employer" (aka scammer) asks you to send gift card information back to the sender in exchange for a sent check. No legitimate business will require this type of transaction and you should discontinue any correspondence at once. **Giving a person the codes from a gift card is the same as giving cash there is no way to reverse or stop this transaction.**

BELOW ARE RED FLAGS – BEWARE IF…

- The email is from what looks to be a legitimate vanguard.edu address, but it is bland and unprofessional. Note: Emails that come from Career Services will always have a Career Services logo and/or a Career Services signature embedded into the email.
- You are asked to give out any personal financial information.
- You are asked to send a payment by wire service or courier or are asked to transfer money.
- You receive an expected or unexpected large check or are offered a large payment or reward for depositing a check or transferring money.
- You receive an email from someone that says they received your application when you haven't sent one. Or an email that says they received your information from Career Services. If you receive a very general email that says they found your resume through the Career Services, please check with us at careerservices@vanguard.edu / (714) 619-6477 before responding to the employer.
- It sounds too good to be true. If that's the case, then it probably is.
- There are grammatical errors in the posting.
- The employer uses a personal account like gmail, live or yahoo or there is very little to no contact information for contacting them. Legitimate employers will always provide a valid phone number, email address or website.
- The posting appears to be from a legitimate company, but when you look closely, the email address is just slightly different – example - @wellsfargo.com may read @wellfargo.com. Check the company's website to verify postings.
- The job requirements are overly easy or there aren't any. Many of these types of scams are recruiting for an Administrative Assistant, Personal Assistant (someone to run errands) or Office Assistant type position. Be wary of postings for Mystery Shoppers, work at home or virtual assistant positions.
- You get offered a job without an in person interview.
- There is a phone number provided, yet you've never actually spoken to a human being and when you call the phone number provided no one answers.

- The company has a generic name such as Finance or Insurance Company. Conduct a google search to see if the organization is listed. When you google the organization name and the word "scam", the results may show several scam reports regarding the company. Check **spam-checker.com** to see if the job description is listed as one of their reported scams.
- A company charges a fee for anything (training, visa processing etc.) If a company offers free training, followed by assistance with job placement, this is a red flag. Often the training is not truly free and will cost you money if you break the contract that you signed.

ADDITIONALLY, FOR INTERNATIONAL STUDENTS SEEKING EMPLOYMENT – BEWARE IF…

- A company seeks out only international students who want H1b
- A company inflates a candidates credentials or asks you if it is okay if they do so.
- A company asks for extensive background information (copies of immigration documents, social security card, government issued ID, passport, or bank info). Never share copies of these documents with a company or individual you have not met. Only give these documents to your employer when you are physically at the place of employment.

For information on other types of scams, please see the **International Student and Scholar Services guide to Safety and Security**

If You Come Across or Respond to A Scam:

- Contact careerservices@vanguard.ed / (714) 649-6477. We will check to see if the organization is in our system and block them if they are. We will reach out to other students who may have been affected. We will also contact Vanguard's IT and Campus Safety Departments on your behalf.
- End communication with the "employer ".
- If personal information was disclosed, monitor your accounts closely for the next few weeks. If you receive unwanted emails or phone calls, you can contact your providers and ask for the person to be blocked.
- If you gave our any financial information or sent money to the "employer", contact your bank immediately and/or credit card company to close your account and dispute the charges.
- CLICK HERE FOR ADDITIONAL STEPS ON HOW TO REPORT A SCAM

Lastly, if you believe your financial or personal information has been compromised, below is a link that will take you to a company where you can request a free credit report:

https://www.annualcreditreport.com/index.action.

On this site you can see if any accounts have been opened in your name.

To place a fraud alert on your accounts go to:

http://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

The three credit reporting companies that they use are:

- Equifax - www.equifax.com/CreditReportAssistance
- Experian - www.experian.com/fraud
- TransUnion - www.transunion.com/fraud