How to Spot Fraudulent Employers and Postings

Beware If You See These Red Flags

- You are asked to give out any personal financial information (name, birthdate, social security number, immigration documents, passport, or bank account number) by phone, mail, or online).
- You are asked to send a payment by wire service or courier or are asked to transfer money or you receive an unexpectedly 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 the USM Job & Internship Board. While some employers may legitimately contact you through USM Job & Internship Board, the email would be more detailed. If you receive a very general email that says they found your resume through the USM Job & Internship Board, please check with The Career & Employment Hub before responding to the employer.
- If it sounds too good to be true, it probably is.
- Be aware if there are a lot of grammatical errors.
- The employer uses a personal account like gmail or yahoo or there is very little or no contact information. Legitimate employers will always provide a valid phone number, email address and/or website.
- The posting appears to be from a legitimate company, but when you look closely, the email address is just slightly different –example - @bankofamerica.com may read bankofamerca.com. It is best to check the company's website to verify postings.
- The job requirements are minimal or no job requirements are stated. 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 interviewing.
- 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 Scam Detector to see if the job description is listed as one of their reported scams.

If You Encounter or Have Already Responded to One of These Scams

- Please contact The Career & Employment Hub. We can check to see if the organization is in our system and block them if they are. We can reach out to other students who may have been affected by the scam. We can also help you determine your next steps.
- End all communication with the employer and 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 email and phone providers to ask them to block the person.
- If you have given any financial information, out or have sent money to an employer, contact your bank and/or credit card company to close your account and dispute the charges.
- You should contact the local police who can conduct an investigation. Contact the campus police if you live on campus and your local police if you live off-campus.
- If the incident occurred completely over the internet, you can file an incident report with the Federal Trade Commission