Identifying and Avoiding Fraudulent Jobs / Employers

It is important to educate yourself about potential scams when searching for employment and use your best judgement, research and discretion when pursuing opportunities.

What is at stake?

Cybercrime is pervasive and is estimated to exceed the revenues of international drug trafficking. Personal data such as social security numbers, bank accounts, educational and health records, as well as credit card numbers are considered at high risk for theft. Other examples for data at risk for compromise are employment and educational records, contracts and other financial information.

What does a fraudulent employer and/or posting look like?

Understand that while most employers and postings are legitimate, there are some out there that are not. The following tips may be used to help you know when to do more in depth research:

- **If you are offered an interview or job without having applied, proceed with caution.** Typically, organizations will first ask you to apply for a position before extending an interview or job offer. However, you may also be directly contacted by an employer if you have made your resume public in Handshake or other job boards such as LinkedIn, Indeed.com, etc. In these cases, the employers should disclose how they obtained your contact information.
- **If the money sounds too good to be true, it probably is!** Steer clear of opportunities guaranteeing you thousands of dollars a week and/or exceedingly high salary ranges for entry level positions.
- **Match email addresses with domain names.** Email addresses should match the company the contact person represents. While some smaller start-up companies have not purchased domain names, be aware of those using domain names from sites such as Yahoo, Gmail, Hotmail, Live, etc. Also, fraudulent employers will often use domain names similar to a recognizable company but with a slightly different spelling, e.g. @deloitte.com versus @deliotte.com or @us.deloitte.com.
- **Look for poor spelling and grammar.** Be wary of postings featuring spelling and grammatical errors.
- **Do not click links in a suspicious email.** As a rule, if a link is unsolicited and you are unsure of the source, do not click on it.
- **Never send or accept money as part of the application process.** Never, and we mean never, send money or accept personal checks from employers. Never allow employers to have access to your bank account for transferring money and/or depositing checks.

University Career Services posts jobs through Handshake to assist Mason students and alumni with their job search. A posting, however, does not constitute an endorsement or recommendation for any employer by the University. Fraudulent job postings are illegal and not always easy to recognize so it is important to stay vigilant during your search. If you suspect that you have been a victim of a scam via a position posted in Handshake, please notify University Career Services by phone 703-993-2370 and/or email careers@gmu.edu.