Fraudulent Jobs & Email Scams

The Career Center works very hard to ensure that job postings in UMBCworks are legitimate positions, however, scammers are becoming more and more creative, especially in these difficult economic times.

The Career Center is here to support you. If you encounter a position that you fear may be fraudulent, don't hesitate to reach out to us careers@umbc.edu

If you feel that you have already been scammed, there are important steps you should take.

- If you have already given your personal information, you should follow DoIT's recommendations. You may want to alert the campus police about your particular concerns.
- ***In order to assist the DoIT Security Team's investigation, recipients of the email should send security@umbc.edu a notification including the full header set of the message. These headers are not normally displayed but can be easily accessed. For more instruction on how to send the full header set of the message, please refer to: https://wiki.umbc.edu/pages/viewpage.action?pageId=1867970
- If you have already fallen victim to this scam and transferred funds to someone, please file a complaint with the FBI Internet Crime Complaint Center. They can be reached at the following web address: Internet Crime Complaint Center
- If you have not wired money to the criminals, please stop communicating with them. You should still report the situation to the campus police and follow DoIT's instructions. There is no need to report it to the FBI.

In this challenging climate, scammers are becoming more cleaver and deceptive. Below we provide some helpful information to assist you with spotting scams before engaging with them.

- Look at the email domain of the sender (john@gmail vs. john@avalidcompany) Be CAUTIOUS if the domain does not match the domain of the company.
- NEVER provide your credit card, bank account numbers, social security number or other financial documentation.
- BE CAUTIOUS of an employer offering a check before work has commenced and NEVER deposit a check before work has commenced. This is almost always a scam.
- NEVER engage with an employer that requires an initial investment, such as a payment by wire.
- BE CAUTIOUS of an employer whose posting includes many spelling and grammatical errors.
- BE CAUTIOUS of an employer who asks for anything out of the ordinary such as a picture of you or who is not operating by normal hiring procedures, such as hiring you without interviewing you.
- 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. Better Business Bureau (http://www.bbb.org/us/consumers/), Hoovers (http://www.hoovers.com/) and AT&T's Anywho (http://www.anywho.com/) can be used to verify organizations.

Scammers often use phishing emails. Some key things to note are:

- The FROM address on an email can easily be spoofed/faked. *Just because an email you receive looks like it came from an **"@umbc.edu"** address or someone you know, does not always mean it actually came from that person.*

- Some people may ask, *"How does a scammer get my UMBC email address in the first place?" Your email address is not private information*. If someone knows your name, they can look up your UMBC email address in the campus directory, or if you have your email address attached to social media or other online accounts and those get hacked, or if someone you know has had their email hacked, etc. There are many different ways your email address can end up in the hands of a scammer.
- Never click on the links in a phishing message. Just by clicking on the link, you may download a malicious program onto your computer.
- For more information from DoIT on phishing, click HERE
- Please see the information and recommendations from DoIT at UMBC about online safety and best practices HERE.

*You will continue to receive scam emails periodically from all types of sources. Please refer to Page 65 of the Career Guide - "Is this Posting for Real?". HERE is a link to that page. For a more in depth look at how to evaluate employer emails and identify fraudulent offer, please see the Career Center page on Fraudulent Jobs & Email Scams HERE

Disclaimer

UMBC is not responsible for employers' representations or guarantees with regard to job postings, nor is it responsible for wages, working conditions, safety, or other work-related issues that may arise after placement with an employer. UMBC is not responsible for fraudulent job postings, however if a job listed on UMBCworks is found to be fraudulent, please report it immediately to careers@umbc.edu or call 410-455-2216 so that it can be removed from UMBCworks and any other applicants can be notified.