WILLIAM & MARY | OFFICE OF CAREER DEVELOPMENT & PROFESSIONAL ENGAGEMENT

AVOIDING ONLINE SCAMS

wm.edu/career

How can you tell if a job posting or offer is legitimate?

Does a job or internship offer sound too good to be true?
Did you receive a message from someone offering you a position you didn't apply to?
These are two indicators that you may want to approach the posting or offer with skepticism. We've included additional tips to spot a scam below (please note that this is not an exhaustive list, and every case is unique):

Some indicators that an employer email may be fraudulent include:

- There are typos or spelling mistakes in the email you receive
- The message is sent from a personal account, rather than an employer email account
- The email account doesn't match the employer website URL
  - Example: *@hotmail.com* rather than *@thecompanyname.com*
  - Example: *@company-name.com* instead of *@thecompanyname.com*
- The employer asks you to send them confidential information or money
- You receive an unsolicited interview or job offer
- The company LinkedIn page is not updated or does not have employees attached to it
- The company address or headquarters are not verifiable by a map or online search

Tips to avoid online scams:

- Always safeguard your personal information
- Never provide your social security number, bank account information, or other sensitive information via email
- Never respond to requests for check deposits, package pickups, or money transfers
- The only time an employer should ask for your bank account information is after you have accepted an offer and are filling out payroll forms
- A legitimate employer will always ask you to fill out tax forms
- Unfortunately, scammers can be very savvy at avoiding detection and finding ways to email or call potential victims - Be cautious when using job boards and social media

What should you do if you were scammed? Review next steps.

- Find out what to do if you paid someone you think is a scammer, gave out personal information, or if they have access to your phone or computer at the following webpage: Federal Trade Commission: What to do if you were scammed.
- Report the activity to the Internet Crime Complaint Center at https://www.ic3.gov/
- Report the activity to the website on which the posting was listed
- Report the activity to the company the cyber criminals impersonated
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sentReview the following information for additional tips to keep your information safe while job searching: FTC Advice for Avoiding Job Scams