IDENTIFYING FRAUDULENT JOBS & INTERNSHIPS

JOBS POSTING RED FLAGS MIGHT INCLUDE:

Requests for protected information
Employers should not request your social security or driver’s license information in the initial application.

Requests for money
You should not be asked to provide any financial documentation, credit card information, or bank numbers or to invest money or transfer funds.

The employer’s contact info is not tied to the organization
When you Google the employer’s email address or phone number, you should expect to see information about the organization.

It sounds too good to be true
The position description should not focus on the money to be made, and the job responsibilities should be clear.

Misleading website or email addresses
Website links should match the organization’s actual website, and contact email addresses should be tied to the organization.

Grammatical or spelling errors
Job descriptions should be free of grammatical errors or misspelled words.

IF YOU ENCOUNTER A QUESTIONABLE JOB POSTING:

IF YOU HAVE COMMUNICATED WITH THE EMPLOYER...
- End all communication with them
- Closely monitor your bank account for fraudulent activity
- Contact your bank or credit card company immediately if you shared any financial information

IF YOU SUSPECT THAT A POST MAY BE FRAUDULENT...
- Report it to the police
- Contact the Career Center if there is a UVM connection (i.e., you saw it in Handshake)
- If it came through your UVM email account, forward it to abuse@uvm.edu

802 656 3450
career@uvm.edu
uvm.edu/career