

# How to Avoid Fraudulent Job Postings

*It is easy to think that fraudulent job postings and scams will not affect you but it is best to be prepared and have the necessary tools.*

## What is a Fraudulent Job Posting?

Scammers might try to convince job-seekers to provide personal information by posing as talent acquisition managers offering part-time or internship positions



## Be on the Lookout

Some red flags to look out for are grammatical errors in the job title, job description or any additional information regarding the job. Make sure to pay attention to the email address.



Sometimes the email will not contain the company domain or have minor differences.

- ✗ jane.doe@bmo-inc.com
- ✓ jane.doe@bmo.com

## Do Not Release Personal Information

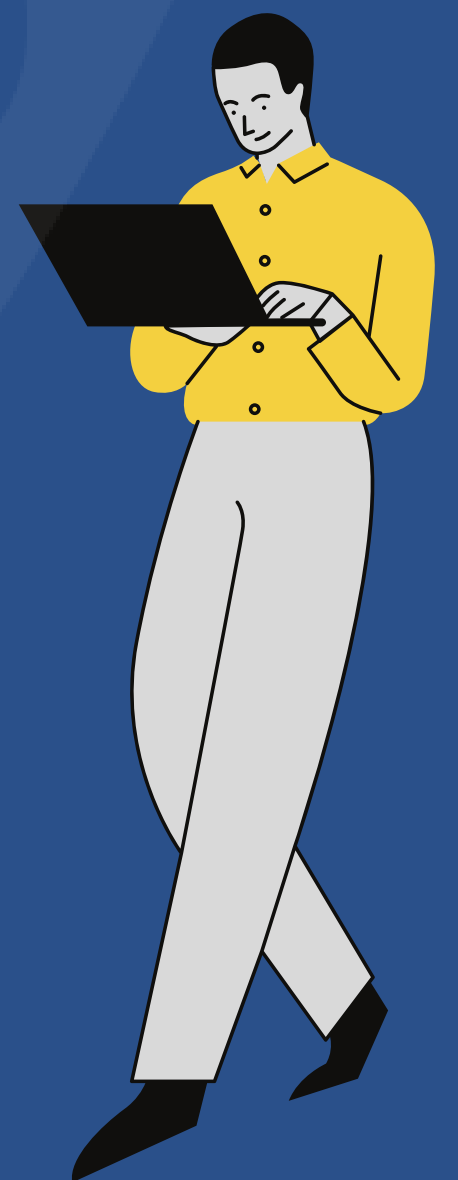
Scammers will often ask for personal documents or additional information to 'verify' your identity (ie. Driver's License, bank account, Paypal, etc).



If you are unsure, conduct some research on the company and identify the recruiter directly from the company's website.

## What are the Next Steps if You Get Scammed?

1. Immediately report the job posting.
2. File a complaint with the Federal Trade Commission (FTC).
3. Contact your local police using their non-emergency number.
4. Monitor your bank account or credit information in case of identity theft.
5. If the incident occurred completely online, file a report with the FCC at [cybercrime.gov](http://cybercrime.gov).



## Unsure about a Job Posting?

If you have questions or concerns regarding a job posting, contact Career Development at [careers@dom.edu](mailto:careers@dom.edu).

