Fraudulent Job Postings

Unfortunately, not every job posting is legitimate, even on trusted platforms like Handshake, Indeed, or LinkedIn. Some postings are scams designed to steal personal information or money. It's critical to know how to identify real opportunities and avoid fraud.

Never send or accept money as part of the application process.
No legitimate employer will ever ask you to pay for training, equipment, background checks, or application fees upfront. Also, be cautious if you're asked to cash a check or transfer money on behalf of the company — this is a common scam tactic known as a "check fraud scam." If money movement is involved before you've officially started the job and signed proper employment paperwork, it's almost certainly fraudulent.

Be cautious of job offers that seem too good to be true.
Scammers often lure victims with promises of high pay for little effort, such as "work from home and make $2,000 a week with no experience required!" Real jobs, especially entry-level and internship positions, offer pay that is appropriate for the role and location, not excessive amounts for minimal tasks. Use salary research tools or check sites like Glassdoor to see what's normal in your field.

Watch out for unsolicited job offers.
If you didn't apply for the job, yet someone reaches out offering you the position, be skeptical. This is especially true if the communication is generic (e.g., "Dear applicant") or lacks specific details about how they found your information. Authentic employers usually conduct interviews before extending offers, and they rarely hire without at least some screening process.

Scrutinize email addresses and web links.
Fraudsters often use email addresses that look similar to real companies but have small differences — like extra letters, hyphens, or strange domain names (e.g., using @gmail.com instead of @companyname.com). Similarly, fake job postings may link to sites that look like real company pages but have slightly misspelled URLs. Always check links carefully and only apply through official company websites or trusted job platforms.

Don't click on suspicious links or download unknown attachments.
Clicking on malicious links can lead to phishing websites that steal your information, or download malware onto your device. If you receive an unsolicited email with a link or attachment, even if it appears to come from a known contact, verify with the sender through another channel before clicking.

Pay attention to poor spelling, grammar, or unprofessional communication.
Many scam messages are written quickly or by non-professionals and contain noticeable errors. Additionally, legitimate employers use professional language and often have structured, formal emails when communicating about hiring.

Verify company details and do your own research.
Before applying or engaging with an employer, check their official website, look them up on LinkedIn, and search for reviews or reports about the company. Trustworthy companies will have a clear digital presence, including contact information that matches the details in the job posting.

Be aware that even legitimate-looking emails can be hacked or faked.
Sophisticated scams can make an email appear as if it's from a university or trusted company domain. If something about the message feels off — like an unexpected offer, unusual requests, or high-pressure tactics — take a moment to confirm its authenticity by contacting the employer directly through publicly listed contact info.

Office of Career Services

COSTELLO COLLEGE OF BUSINESS
George Mason University

Examples of Common Job Scams

Fake Personal Assistant Jobs
Scammers pose as executives or professors and offer flexible "personal assistant" roles. They may ask you to run errands that involve handling money, like buying gift cards or wiring funds.

Check-Cashing and Reshipping Scams
You're sent a check and asked to deposit it, keep part of the money, and send the rest back or buy items (like electronics) to ship elsewhere. The check eventually bounces, and you're left owing the full amount.

Mystery Shopper Scams
You're hired to evaluate stores or services and asked to deposit a check, spend money, and report back. These checks are fraudulent, and you're responsible for the losses.

Fake Remote Job Offers
Scammers exploit the popularity of remote work by offering well-paying online jobs that require you to buy "training materials" or special software — always at your expense.

Phishing for Personal Data
Some fake job ads are designed just to collect your sensitive information (Social Security Number, bank account, copies of your ID) which is then used for identity theft.

Fraud Checklist: Spot the Red Flags

- ☐ Did they ask for money or offer to send you a check?
- ☐ Is the pay unusually high for little work?
- ☐ Did you get an offer for a job you didn't apply for?
- ☐ Are there spelling and grammar mistakes in the message?
- ☐ Is the email from a free account (like Gmail, Yahoo) instead of a company domain?
- ☐ Is the website link slightly misspelled?
- ☐ Does something just feel off? Trust your instincts.

If you suspect fraud:

The FBI warns that job scams continue to target students and job seekers nationwide. If you believe you've encountered a fraudulent job post or have fallen victim to a scam, report it immediately.

If you suspect you've seen or been sent a fraudulent job offer, contact Career Services at 703-993-2140 or email mycareer@gmu.edu.

For scams outside the university, file a complaint with the Federal Trade Commission at reportfraud.ftc.gov or with the FBI's Internet Crime Complaint Center at ic3.gov.