

Protect yourself from job scams

What are job scams?

Job scams usually take the form of a posting or job offer that appears legitimate at the surface but is intended to swindle the applicant out of their money, identity, time, or all of the above.

Opportunities that seem too good to be true usually are. Scammers will often offer large sums of money for little to no effort or experience to lure their victims in. While those are the most common, there are more sophisticated scams out there that can mislead applicants into providing this information without realizing until it's too late.

Common job scams

Moving money

A scammer might ask you to deposit a cheque and e-transfer money back to “test their payroll.” The cheque will bounce, so you’ve lost your own money and can’t recover it. These scams will often use terms like “financial agent” or “payment processor.” Or, scammers will ask you for your bank or credit card details for “hiring purposes,” before they’ve even set up an interview or offered the job.

Phishing for personal information

Perhaps a recruiter wants to set up an interview. But first, they ask you to fill out an online form and provide your *full name, SIN, home address, a scan of your passport, and banking information* so they can create a profile for you. While your name might be necessary, the other information isn't.

If an employer is asking for your social insurance number, your passport/visa information, bank details or more very early in the process, take extra precaution and do some research to confirm that it's legitimate.

Paying for training or materials upfront

If a company is promising “unlimited earning potential” and asking you to pre-purchase the products you're selling, or providing lengthy unpaid training, beware! Other common scams that involve paying for materials or products now might also require you to recruit others.

Things to watch out for

Vague job details

Very little or confusing information about the job is provided and no skills or experience is required.

Suspiciously high pay

Highly paid jobs require a lot of expertise, diligence, and dedication. While it's important to find a job that pays you well, if the salary seems *disproportionately* high for the type of work you'll be doing, or your skills and experiences, then it may be a scam.

Unsolicited offers

Someone is offering you a job that you never applied for, especially via email or text message. Legitimate recruiters have been known to headhunt using social media, email or LinkedIn, but they will often provide more detail and interview you before hiring.

No interviews

Most reputable companies will interview you first before offering you a job. If you were offered a position before you provided a resume, references, had an interview or met in person, do more research.

Unprofessional communication

If you received a job offer from a messaging app like WhatsApp, WeChat, or Messenger when "recruiting," do some research before accepting or providing any information.

Suspicious contact information

While it's not uncommon to use Yahoo, Gmail, Hotmail or other free email providers, most employers will also use a corporate email address to contact you.

You should also beware if the job posting or communications you received from the supposed employer have many spelling or grammatical errors, slang, or are poorly written or translated.

Always double-check the email address, as some scammers can create a fake corporate email address that's similar to a legitimate company's name, but with a minor detail changed.

Extra costs or fees

Scams might involve paying an upfront fee for "training" or "software" or buying the products before you sell them. Typically, candidates aren't required to pay any costs for the job they are being offered. If you're being asked to send money or pay fees as a condition of the job, stop and do some research first.

Requesting sensitive information

Identity theft is an extremely common motive for scammers. Don't provide your SIN or direct deposit information until you are absolutely sure the job offer is legitimate, and you have met the employer, interviewed for the position and signed a formal offer.

How can I protect myself?

Research the job and company

Doing extra research never hurts. Look up the company or company representative online or on LinkedIn and check out the company website whenever possible. Does their address, contact information and history check out? Is this job posted anywhere on their official channels?

Know where to go for help

Career Services staff are always happy to help you identify if a job is legitimate or not. If a job opportunity or offer doesn't feel right, email us at careerservices@flemingcollege.ca for help. You can also book an appointment or visit during drop-in hours.