

DETECTING JOB SCAMS: SAFETY IN THE JOB SEARCH

Job scams are a very real threat to job seekers in today's technological world. They can appear in different places including online or print advertisements, career websites, Craigslist or even in your email inbox. Ask yourself these questions before responding to any job posting or request.

Are the company name and details provided in the ad?

If the posting is missing pertinent details like company name, website or location, it may be suspicious.

Does the email address match the name?

Sometimes scammers use a domain name that is similar to a legitimate company to try and fool victims. Most large companies have corporate email accounts and will not use personal email accounts such as gmail or hotmail.

Are you asked for credit card or bank account numbers?

Job seekers should not have to provide financial information or pay a fee in order to complete a job application or view job postings.

Are they offering a lot of money to perform little work or to pay you before you begin?

Scammers often boast huge earnings or use enticing phrases such as "Work at Home," "No Experience Necessary," "Make \$1000 a week," or "Work just one hour a week." While there are certainly legitimate work-from-home and entry-level jobs, ask yourself if the rewards being offered to you are realistic.

Did they offer you a job without meeting you?

No legitimate employer will make you a job offer without having first met you in person.

Did you respond to one job posting and the "employer" responded back to you with information on a completely different job?

If you responded to an ad for a data entry position and you receive a response about a job in which you would be paid for transferring money or signing up for "offers," you may have found a scam.

Does the job involve transferring money from one account to another or are you being offered a large sum of money in exchange for the use of your bank account?

Legitimate companies have their own bank accounts. In other words, they don't need yours.

What to do if you are contacted by a fraudulent organization:

If you have sent money to a fraudulent employer, contact your bank or credit card company to close your account or dispute the charges. If you have already become a victim of an online false job posting/scam, please file a complaint with the Internet Crime Complaint Center at [ic3.gov](https://www.ic3.gov) and possibly the police.



Please know that the CBA Career Center does not provide resumes or student contact information without consent and remain cautious of any email indicating this.

Be extra suspicious of:

- Emails missing pertinent details like company name, website, or location
- Email addresses that don't match the sender's name
- Scammers who ask for credit card or bank account numbers
- Scammers who offer a lot of money to perform little work or to pay you before you begin
- Scammers who offer you a job without meeting you
- Jobs that involve transferring money from one account to another

For more information on job scams, please refer to [this Public Service Announcement](#) from the FBI. If you ever are in question of whether an email job offer is legitimate or not, contact the Information Security Help Desk at 402.554.4357 or the CBA Career Center at 402.554.2365 for assistance.