Identifying Fraudulent Employers & Job Listings

Warning Signs

If you answer “yes” to any of these questions, you should be cautious.

- Does the posting or hiring manager promise a large salary with minimal work required? If it seems too good to be true, it probably is.
- Does the hiring manager offer you a position without talking or meeting with you? Legitimate employers will want to meet you in person before hiring you.
- Does the hiring manager use a personal email address (@gmail.com, @live.com, etc.)? Hiring managers and recruiters will always use an official company email address. If you are contacted from a personal email address, there may be cause for concern.
- Does the posting appear to be from a reputable, familiar company (often a Fortune 500) yet, the domain in the contact's email address does not match the domain used by representatives of the company (this is typically easy to determine from the company’s website)? Another way to validate is to cross reference the open positions on the company's official website.
- Does the position expect you to transfer or wire funds between accounts? Legitimate employers will never ask you to transfer or wire funds on their behalf.
- Does the posting ask you to provide a photo of yourself?
- Has the company sent you a large check and requested you cash it using your personal account? An employer will never ask you to cash or deposit a check using your personal bank account. If an employer asks you to cash a check against your personal bank account, stop all communication immediately.
- Has the company or hiring manager asked for personal information like a social security number or bank account? Employers should never ask for your personal information before you have become an official employee.

For more information visit the Federal Trade Commission (FTC) Consumer Information on Job Scams.

Tips for Verifying Employers

- Google the company name and the word ‘scam’ (ie. Acme Company Scam) and see if scam reports arise.
- Search for the company on Rip-Off Report.
- Google the employer’s phone number, fax number and/or email address. If it does not appear connected to an actual business organization, this is a red flag. You can also use Better Business Bureau (http://www.bbb.org/us/consumers/), Hoovers (http://www.hoovers.com/) and AT&T’s Anywho (http://www.anywho.com/) to verify organizations’ contact information.

What Should I Do If I Think I’m Already Involved in a Scam?

- Notify the police and take other legal action as desired. Complaints may also be submitted to http://www.ic3.gov/default.aspx.
- If it is a situation where you have sent money to a fraudulent employer, you should contact your bank or credit card company immediately to close the account and dispute the charges.
- If the incident occurred completely over the Internet, you should file an incident report with the: http://www.cybercrime.gov/, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

Sources: Columbia University Center for Career Education. (n.d.). Identifying Fraudulent Job & Internship Postings.