
Evaluating Fraudulent Job Postings

If your encounter with an employer makes you feel uncomfortable or suspicious, it is extremely important that you proceed with caution as you pursue an employment/internship opportunity.

If you suspect a position *listed in Handshake* is fraudulent, please contact the Office of Career Services at 443-352-4477 immediately and end all communication with the employer. If you believe you are a victim of fraud resulting from a job listing, please contact the police, as well.

If the incident occurred completely over the Internet, you can file an incident report with the US Department of Justice at <http://www.cybercrime.gov/>, or by calling the FTC at: 1-877-FTC-HELP (1-877-382-4357).

If you feel uncomfortable about a job opportunity you are exploring, DO NOT click on any links and DO NOT provide any personal information.

Generally, if the posting or email contains any of the following, please proceed with caution and alert the Office of Career Services immediately, so that we can advise you of the next steps.

- Offers to pay a large amount of money for very little work.
- Offers you a job without ever meeting or interacting with you.
- Requests personal information from you such as your Social Security Number, bank account numbers, credit card information, copies of your passport/license/or other personal documents.
- Requests you to transfer or wire money from one account to another or payment by wire service, Money Order, or courier.
- Offers you a large payment in exchange for allowing the use of your bank account — often for depositing checks or transferring money.
- Offers to send you a check before you do any work or sends you a large check unexpectedly.
- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc., this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well-hidden.

- While there are legitimate opportunities for individuals to work from home, be sure to research the position (Envelope Stuffers, Home-based Assembly Jobs, and Online Surveys) in advance of applying.
- A contact email address that is not a primary domain. For example, an employer calling itself "Balston Realty" with a Yahoo! Or Gmail email address.
- The posting includes many spelling and grammatical errors.
- You are asked to provide a photo of yourself.
- Hover your cursor over any links in the email or posting, and look to see if the actual link matches the one in the email/posting, if not, DO NOT CLICK on it.
- Once you have verified the URL, (see previous) look at the company's website. Does it have an index that tells you what the site is about or does it contain information only about the job you are interested in? Scammers often create quick, basic web pages that seem legitimate at first glance.
- The employer contacts you by phone; however there is no way to call them back. The number is not available.
- The employer tells you that they do not have an office set-up in your area, and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).
- 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.
- When you Google the company name and the word "scam" (i.e., "Acme Company scam"), the results show several scam reports concerning this company.
- Monster.com lists descriptive words in job postings that are tip-offs to fraud. Their list includes "package-forwarding," "money transfers," "wiring funds," "eBay," and "PayPal".

Additional Resources for Fraudulent Online Postings & Online Privacy Rights

Job Hunting/Job Scams (Federal Trade Commission)	ftc.gov/jobscams
Online privacy rights	www.privacyrights.org
Tips for Job Seekers to Avoid Job Scams	www.worldprivacyforum.org/jobscamtipspayforwarding.html
Is This Job Real? What Should I Do If I Applied?	www.rileyguide.com/realjob.html
Avoiding Job and Work at Home Scams	jobsearch.about.com/cs/workathomehelp/a/homescam.htm
Postal Money Order Security	postalinspectors.uspis.gov/radDocs/consumer/moalert.htm
Better Business Bureau	www.bbb.org/us/article/beware-of-employment-scams-280