

## Spotting Shady Job Postings

---

While most employers who post jobs and internships are legitimate, there are also some bad apples out there preying upon naive job seekers. It is important to pay attention to postings and research opportunities before applying.

### **So how do you know when to be suspicious?**

- Be wary of unsolicited emails from unknown employers offering you an internship or job.
- If it sounds too good to be true (earn \$2000/week without leaving home), it is!
- Posting includes many spelling and grammatical errors.
- If it is difficult to find an address, actual contact, company name, etc., be cautious. Fraudulent postings are illegal, so scammers will try to reduce visibility.
- Posting fails to describe job responsibilities but focuses on how much money you can make.
- Employer responds immediately after you submit your resume (no time to review it first) or hires you without an interview.
- Salary range seems uncharacteristically high for an entry-level or internship role.
- Salary range listed is very broad (e.g. "earn from \$30K - \$100K the first year!")
- Posting appears to be from a reputable, familiar company (often a Fortune 500) but when you look closely, the domain in the contact's email address does not match the domain used by representatives of the company (e.g. @Towers.com may read @Towars.com). Slightly different spellings make it easy to miss at first glance. You can also check company's website for current openings to see if these match what is being referenced.
- Contact's email address contains the domain @live.com.
- Position requires an initial investment, such as a payment by wire service or courier.
- Position initially appears as a traditional job but upon further research, it sounds more like an independent contractor opportunity.
- Employer contacts you by phone but there is no way to call them back. The number is not available.
- You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
- You receive an unexpectedly large check (checks are typically slightly less than \$500, generally sent or deposited on Fridays).
- You are asked to provide a photo of yourself.
- Position is for titles like envelope stuffers, home-based assembly jobs, online surveys or data entry.
- There are legitimate opportunities to work from home, be sure to research the position in advance of applying.

### **Tips to help you research further**

Look at the company's website.

- Does it have an index that tells you what the site is about?
- Does it contain information only about the job advertised?

Scammers often create quick, basic web pages that seem legit at first glance but lack depth or details.

When you Google the company name and the word "scam" (e.g. XYZ Company Scam), the results show several scam reports concerning this company.

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 use sites below to verify organizations:

- Better Business Bureau (<http://www.bbb.org/us/consumers/>)
- Hoovers (<http://www.hoovers.com/>)
- AT&T's Anywho (<http://www.anywho.com/>)

### **Help! I missed the warning signs and am involved in a scam.**

- You should immediately contact the local police who are responsible for conducting an investigation (regardless of whether the scam artist is local or in another state).
- If you have sent money to a fraudulent employer, contact your bank or credit card company immediately to close the account and dispute the charges
- If the incident occurred completely over the Internet, file an incident report with the Federal Trade Commission (FTC) online at <http://www.cybercrime.gov/> or by calling 1-877-FTC-HELP (1-877-382-4357).