

# Signs A Job Posting Is A Scam

Searching for an internship or job opportunity is a process, and a component of that process is reading through job descriptions and interacting with a hiring manager. Here are some components of job descriptions and corresponding with a hiring manager to be aware of so you prevent yourself from applying for something that may be a scam.

## The Pay Offered Is Too High

If you find a job posting written similar to something like this it should be a red flag that the job is a scam "This is a work-from-home job. Work hours are 20 hours a week for \$72,800 annually. You are expected online at Yahoo Messenger during working hours."

Be wary of job postings that list a salary two to three times higher than the typical salary for a specific job.
Use sites such as <u>O'Net</u>, <u>Glassdoor</u>, or <u>Salary.com</u> to determine what the average pay scale is for the jobs you are seeking.

#### Lack Of An Online Presence

Always check online sources to help determine if a company is legitimate. Look for sources such as a company website or use <u>Glassdoor</u> to see if there are reviews of the company. Check social media pages like <u>LinkedIn</u>. If a company is legitimate they will have a presence in all of these places.

#### **Requesting Confidential Information Upfront**

Scammers will often ask respondents to their job postings to provide personal information such as a social security number early on in the interview process. If a potential employer is asking for ANY of this information before you have signed a job offer consider it to be a warning sign of a scam.

- Another tactic used by scammers is to request you to pay for equipment, training, or inventory to secure the
  job which enables them to obtain your credit card or bank info.
- A further red flag is a request to verify your identity by clicking on a link authorizing ownership of your email
  account be given to someone else.

### **Unprofessional Communication**

There are a few items to be aware of here:

- A scammer will use a personal email address like @yahoo.com instead of a company email address like @medtronic.com.
- The message will usually contain grammar, punctuation, or capitalization errors.
- They will request you interview via an instant messaging service whereas a legit company will use platforms like Zoom or Microsoft Teams.

# Vague Job Requirements & Description

Job listings that use a common job title such as "Executive Assistant" but then only list job requirements as "Must have access to the internet" and "Must know how to use computer programs" and list the job description as "Managing a busy calendar" and "Helping prepare PowerPoint presentations" are most likely scams. Legitimate job postings will tell you what you need to be considered qualified for the role AND provide specifics on what tasks you'll be completing day to day.