



Searching for a career opportunity is a process that requires a careful eye when reviewing job descriptions and communicating with hiring managers. To help you avoid potential scams, here is a quick guide to the most common red flags.

The Pay Offered is Too High

- The "Too Good to be True" Rule: Be wary if the salary is 2–3 times higher than the industry average (e.g., \$72,800 for 20 hours of remote work).
- Do Your Research: Use sites like Glassdoor, O'Net, or Salary.com to verify the standard pay scale for the role



Lack of an Online Presence

- Verification: A legitimate company should have a functional website, a LinkedIn page, and reviews on Glassdoor. If they are invisible online, it is likely a scam.
- Pro Tip: If a job posting feels "off," trust your gut and verify the company through multiple independent sources before sharing any personal data

Requesting Confidential Information Upfront

- Confidential Data: Never provide your Social Security number or bank details before signing an official job offer.
- Payment: Legitimate employers will never ask for purchase of supplies to secure a job. They will not send money before you sign a contract and begin working.
- Identity Links: Avoid clicking links that ask you to "verify identity" by granting someone else access to your email account.



Unprofessional Communication

- Email Addresses: Scammers often use personal domains (like @yahoo.com) rather than official company domains (like @medtronic.com).
- Platform: Be suspicious if an interview is requested via an instant messaging service instead of professional platforms like Zoom or Microsoft Teams.
- Quality: Look for frequent errors in grammar, punctuation, or capitalization



Vague Job Requirements & Description

- Generic Descriptions: Scams often use common titles but list overly simple requirements, such as "must have internet access" or "know how to use a computer".
- Legitimacy: Real postings provide specific qualifications AND detailed day-to-day tasks.