

JOB SCAM

RED-FLAG CHECKLIST

A practical, printable guide from **HomeHireHub** to help you spot warning signs before you share information, pay money, or accept a remote job.

Pause before you proceed. One warning sign deserves a closer look; several together are a strong reason to stop and verify the opportunity independently. A polished website, professional-looking email, or online interview does not prove a job is legitimate.

1. The offer sounds suspicious

- The pay is unusually high for the duties, experience, or hours—or earnings are guaranteed with little work.
- You are offered the job almost immediately, with little or no discussion of your skills or qualifications.
- The job description is vague, copied, inconsistent, or does not explain the actual work.
- The recruiter pressures you to decide quickly or says you must act immediately to secure the position.
- The role promises easy money for receiving, forwarding, reshipping, or moving money or packages.

2. The recruiter or communication raises concerns

- The message comes from a free or look-alike email address instead of a verifiable company domain.
- The recruiter contacts you unexpectedly through text or social media and avoids normal hiring channels.
- The person refuses a reasonable live conversation, gives inconsistent answers, or cannot explain the role.
- The sender's name, email domain, phone number, company details, or job title do not match official company information.
- You are asked to continue only through a suspicious link, unfamiliar app, or encrypted messaging account.

3. They ask for money or financial activity

- You must pay an application fee, training fee, background-check fee, or deposit directly to the recruiter.
- You are told to buy equipment from a specific vendor or send money back from a check or payment.
- You are asked to deposit a check, transfer funds, purchase gift cards, or send cryptocurrency.
- You are asked to receive and reship packages as part of a work-from-home job.
- You are asked to provide bank details for anything other than a verified, legitimate payroll process after hiring.

4. They request sensitive information too early

- They ask for your Social Security number, government ID, banking details, or a photo of sensitive documents before you have verified the employer and reached a legitimate hiring stage.
- A form or website requests passwords, one-time security codes, or access to your personal accounts.
- They ask you to install remote-access software or give control of your computer without a clear, verified business reason.
- The website has misspellings, broken pages, an unusual domain, or contact details that cannot be independently confirmed.

Before you apply or accept: verify independently

Check	What to do
Company website	Type the company's known website address yourself. Find the opening on its official careers page; don't rely only on a link in a message.

Check	What to do
Recruiter identity	Contact the company using contact information published on its official website to confirm the recruiter and vacancy.
Job details	Compare the title, duties, location eligibility, pay, and application process with the official listing.
Your information	Share sensitive details only when the employer and hiring process are verified and the information is reasonably required.

If something feels wrong: Stop responding, do not click more links or send money, save messages and screenshots, and verify the company through an independently found contact method. If you already shared financial information, contact your bank promptly. In the U.S., report suspected job scams to the FTC at **ReportFraud.ftc.gov**; if identity information was exposed, visit **IdentityTheft.gov** for recovery steps.

Remember: A single red flag does not prove fraud, and a legitimate-looking process is not a guarantee of safety. Use the full context and verify independently before proceeding.

HomeHireHub • Remote job search resources • homehirehub.com