



Do be cautious if job offers come unsolicited or too easily.

Do not respond to calls, text messages or emails from unknown numbers or suspicious addresses.

Do not click any links in a text message from a number you do not recognize. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they weren't hacked.

Consider adding your number to the [National Do Not Call Registry](#) to prevent telemarketing calls.

File a report with local law enforcement if you have lost money or possessions due to a scam.

Do trust your intuition: offering an extremely high salary, incredible perks, or is above your qualifications.

Do verify the employer's location and their ability to conduct proper interviews.

Do watch for red flags. One major warning sign of a work from home scam is when the employer wants to urgently hire you.

Do look for mistakes in the communication. If words are misspelled or punctuation is off, this is a sign of a scam.

Scammers DO post fake work from home jobs on legitimate job sites.

Does use "What's App" vs. normal platforms to communicate.

Do ensure the job description is clear, and there is sufficient information online about the position.

Do opt for jobs with a thorough interview process, including video or in-person interviews.

Don't share sensitive personal or financial information over email, text messages or over the phone.

You don't have to pay to work. A common scam is when employers claim that you need to invest some money into your work to get started.

Don't apply if you read about warnings and bad reviews online about the company.

Don't apply if you can't find valid company information online: company website, LinkedIn, Indeed, Glassdoor.

Don't forget to look for employees on LinkedIn and company reviews online.

Avoid jobs with vague job descriptions and sparse or nonexistent online information.

Be cautious if the entire interview process takes place over a messaging app.

Be wary of employers who are out of the state or country and cannot conduct video or in-person interviews.

Be cautious if the company lacks credible information online.

Be wary if the recruiter uses a personal or unofficial email address.

Steer clear if communications are missing important details or contact information.

Refrain from providing personal information or banking details early in the process.

Be cautious if asked to pay for supplies, training, or certification.

Avoid jobs where you're sent a check and asked to cash it before even starting work.