

# Job and Employment Scams

The fake-job playbook, including 'task' scams, and how to tell a real offer apart.

**\$501M**

losses to job and employment-agency  
scams in 2024

FTC, 2025

**~4x**

rise in gamified 'task scam'  
reports in 2024

FTC, 2024

**\$0**

a real job never asks you to pay to  
start

rule of thumb

## SIGNS THE JOB IS FAKE

### 01 Hired with no real interview

An offer over chat or text after a few questions, often for 'easy' remote work.

### 03 'Task' jobs that pay you, then ask for deposits

Gamified apps that show earnings, then require you to add money to keep going.

### 02 You are asked to pay to start

Fees for training, equipment, or a 'starter kit' for your own job.

## PAYMENT AND IDENTITY RED FLAGS

### 04 A check to deposit and forward

Overpayment by check, then asked to buy gift cards or wire back the difference.

### 05 Sensitive details up front

Bank logins, SSN, or ID demanded before any genuine hiring step.

## WHERE FAKE JOBS REACH YOU

### 06 Unsolicited offers by text or chat

A recruiter messaging out of the blue with an easy, high-pay role.

### 07 Spoofed company names

A real brand's name on a free-mail address or a look-alike domain.

### 08 Reshipping and 'task' work

Jobs that have you receive and resend packages, or apps paying for repetitive tasks.

## DO / DON'T

### DO

- Apply through the company's official website and verify the recruiter there.
- Search the company name together with words like 'scam' or 'review'.
- Keep your bank logins and ID private until a verified, signed offer.
- Treat any request to pay, or to deposit and forward money, as a scam.

### DON'T

- Do not pay for training, equipment, or a 'starter kit' for a job.
- Do not deposit a check and send part of it back. The check will bounce.
- Do not add your own money to 'unlock' tasks or earnings.
- Do not hand over your SSN or bank logins before a legitimate hire.

## THE ONE MOVE

A real employer never asks you to pay to work, to deposit a check and send money back, or to hand over bank logins before day one. Verify the company through its official site and apply there directly.

## IF IT HAPPENS

- 1 Stop sending money and cut off contact.
- 2 If you deposited a check, tell your bank now. You are liable when it bounces.
- 3 Change any passwords or revoke any access you shared.
- 4 Report to [reportfraud.ftc.gov](https://reportfraud.ftc.gov) and, for reshipping, to the FBI at [ic3.gov](https://ic3.gov).

Get a briefing like this every week, free.

[threatlevelhuman.substack.com](https://threatlevelhuman.substack.com)

[youtube.com/@threatlevelhuman](https://youtube.com/@threatlevelhuman)

Sources: U.S. FTC Consumer Sentinel (2024, 2025). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.