

FREE PRACTICAL CHECKLIST

The Work From Home Scam Red Flag Checklist

A fast, practical screen before you apply, reply, pay, download software, cash a check, or send personal information.

60-SECOND SCREEN	10 VERIFICATION QUESTIONS
Spot the patterns that deserve an immediate pause.	Confirm the opening and recruiter using sources you find yourself.
SAFE APPLICATION RULES	DAMAGE-CONTROL STEPS
Know what not to send, pay, cash, install, or reveal.	Use official resources if money or personal information already moved.

STAY AT HOME MOM LAB

Practical tools for better work and business decisions

Educational information only. This checklist cannot prove that an offer is safe, and it is not legal, financial, employment, cybersecurity, or identity-theft advice.

The 60-second first screen

Check every statement that applies. One red flag is enough to pause. Several common scams use multiple signs at once.

[] The recruiter contacted me unexpectedly by text, WhatsApp, Telegram, or social message.
Unexpected contact is not proof of fraud, but it means you should verify the person and opening independently.

[] The company, role, duties, or hiring process stay vague.
A real name or logo can be copied. Ask for specific facts and confirm them on the official company website.

[] The pay is unusually high for simple work or little experience.
Compare the offer with credible listings for similar work, location, and experience.

[] I must pay for training, equipment, software, certification, or a background check.
Do not send money merely to receive a job.

[] They sent a check and told me to buy equipment or send money elsewhere.
Stop. A fake check may appear available before the bank discovers it is fraudulent.

[] They want bank details, identification, or a Social Security number before a verified hiring process.
Sensitive information belongs only in a legitimate, necessary onboarding process you have independently verified.

[] The email domain is free, misspelled, or different from the company's real domain.
Read the entire address. A familiar display name proves nothing.

[] They use urgency, secrecy, threats, or an immediate offer to push the next step.
Pressure is a reason to slow down, save evidence, and verify.

[] I cannot find the same opening on the official careers page.
Contact the company using a public phone number or careers address you found independently.

[] The entire interview happens by chat with no credible human conversation.
Chat-only hiring combined with vague duties, instant approval, or money requests is a serious warning sign.

USE THE RESULT **0 flags:** Continue verification. **1 flag:** Pause and verify. **2 or more:** Stop and investigate. **Any check, payment, gift card, crypto, or money transfer:** Stop immediately.

Ten questions to verify before you trust

Write down the answer and where you confirmed it. A claim repeated by the same recruiter is not independent verification.

01	What is the company's full legal or public business name? Record the exact name, location, industry, and official website you found yourself.
02	Does the website domain match the email domain? Check spelling, extra words, country endings, and the full sender address.
03	Is the same job on the official careers page? Compare the title, duties, location, pay information, and application process.
04	Can the company confirm the recruiter and opening? Use a public phone number or careers contact from the official site, not the message.
05	What work will I do and who will manage it? Ask for specific duties, tools, schedule, reporting line, and performance expectations.
06	How is pay calculated and delivered? Confirm rate, hours, commission, fees, payment timing, employee or contractor status, and taxes.
07	What is the interview and onboarding process? Legitimate processes vary, but vague chat interviews plus instant offers deserve scrutiny.
08	Why is any money, check, or purchase involved? You should not pay merely to get hired or move employer money through your own account.
09	Why is each piece of personal information needed now? Delay sensitive data until the employer, role, purpose, and secure process are verified.
10	What happens when I slow the process down? A legitimate contact can answer reasonable questions. Pressure, anger, or threats are evidence to stop.

Verification note: Search results, reviews, and complaint posts can provide clues, but none proves legitimacy by itself. Confirm the opening through the company's official channels.

A 20-minute verification routine

Do this in a new browser tab. Do not begin with the links or phone numbers the recruiter supplied.

1 Save the original evidence

Capture the listing, messages, email address, phone number, profile, promised pay, and any file or payment request. Do not open unfamiliar attachments merely to preserve them.

2 Find the official website yourself

Type the company name into search, compare multiple credible results, and inspect the domain carefully. Avoid sponsored lookalikes.

3 Find the official careers page

Search within the official site. Compare the role, location, duties, and hiring instructions with what you received.

4 Contact the company through a public channel

Use a number, careers address, or contact form from the official site. Ask whether the recruiter and opening are legitimate.

5 Search for the specific pattern

Search the company name, recruiter name, email, phone number, exact message text, and words such as scam, fake recruiter, complaint, check, equipment, and reshipping.

6 Compare the offer with normal hiring behavior

Look at similar roles from credible employers. Compare pay, experience, interviews, training, equipment, and requested information.

7 Decide from evidence, not urgency

Continue only when the employer, role, process, and purpose of each request make sense. If important facts remain unclear, stop.

COMPANY	
ROLE	
OFFICIAL WEBSITE	
VERIFIED CONTACT	
DECISION AND REASON	

Safe application rules

A legitimate job can eventually require sensitive information. The question is whether the employer, role, purpose, timing, and method are all verified first.

- [] Money to receive the job**
Do not pay a recruiter for access to ordinary employment, and do not use gift cards, crypto, wire transfers, or money-transfer apps because someone promises reimbursement.
- [] Money from a deposited check**
Do not buy equipment, send a refund, forward funds, or pay a vendor from a check sent by a new employer.
- [] Sensitive identity data too early**
Delay Social Security numbers, banking details, tax forms, driver's-license images, and similar data until a legitimate employer and necessary onboarding process are verified.
- [] Remote access to your device**
Do not install unfamiliar software or let a stranger control your phone or computer to complete an interview, deposit money, or set up equipment.
- [] Passwords or one-time codes**
No legitimate recruiter needs your email, banking, marketplace, or social-account password or security code.
- [] Private family details**
Do not send children's names, schools, schedules, birthdates, medical information, or documents that expose unrelated household details.

SAFER HABITS

Use a dedicated job-search email	Create a separate address, use a unique password, and turn on multifactor authentication.
Type official addresses yourself	Use independently found websites, phone numbers, and careers contacts when verifying.
Keep a written record	Save the original source, dates, names, claims, files requested, and your verification steps.
Review the actual work terms	Confirm schedule, pay, classification, training, equipment, privacy, and childcare expectations.

If you already replied, paid, or sent information

Act quickly, preserve evidence, and use official contacts. The right steps depend on what was shared and where you live.

01 Stop contact and stop moving money

Do not send another payment to unlock, recover, refund, or verify anything. Do not confront the person if doing so may increase risk.

02 Contact the financial provider

Call the bank, card issuer, payment app, exchange, or wire service using its official number. Explain that the transaction may involve fraud and ask what can still be stopped or disputed.

03 Protect affected accounts

Change reused passwords from a safe device, turn on multifactor authentication, review sessions and recovery details, and contact the provider if someone gained access.

04 Use IdentityTheft.gov

If identity information was exposed, visit <https://www.identitytheft.gov/> for a recovery plan based on what happened.

05 Consider a credit freeze

Use the official Equifax, Experian, and TransUnion websites. A freeze can make it harder for someone to open new credit in your name.

06 Report the scam

Report to the Federal Trade Commission at <https://reportfraud.ftc.gov/>. Also report the account, listing, message, or payment through the platform where it appeared.

07 Preserve evidence

Save messages, profiles, listings, email headers, receipts, check images, transaction identifiers, phone numbers, dates, and the steps you took.

08 Ask for qualified help when needed

Contact local law enforcement, an attorney, an identity-theft professional, or another qualified adviser if money, identity, threats, or complex legal issues are involved.

**RECOVERY SCAM
WARNING**

Someone who promises to recover your money for an upfront fee may be targeting you again. Verify every recovery contact independently.

Printable job-lead verification tracker

Use one row for each opportunity. If you need more room, copy this page before writing on it.

Company / role	Source	On official site?	Email matches?	Money requested?	Verified contact?	Decision

OFFICIAL SOURCES TO KEEP

Federal Trade Commission job-scam guidance	https://consumer.ftc.gov/articles/job-scams
Report fraud to the FTC	https://reportfraud.ftc.gov/
Identity-theft recovery plan	https://www.identitytheft.gov/

WANT THE COMPLETE WORK-FROM-HOME PLANNING SYSTEM?	The Work From Home Starter Bundle helps you compare realistic paths, plan around your actual schedule, prepare truthful applications, track leads, and screen opportunities without pretending any tool can guarantee a job. Visit stayathomemomlab.com/work-from-home-starter-bundle
--	--

Published by Stay At Home Mom Lab. You may print this checklist for your own personal use. Do not resell, redistribute, or present it as professional advice. Scam patterns, laws, platform rules, and recovery options change. Verify current information with official sources and qualified professionals.