

CHECKLIST

Remote Job Scam *Red Flags*

Scams follow job seekers to wherever the jobs are, and remote and abroad roles are where they are. Twenty-two signals, in the order you will meet them, and a five-minute verification routine.

WHAT'S INSIDE

- The five scam shapes aimed at remote and abroad job seekers
- Red flags in the listing
- Red flags in the first message and the interview
- Red flags at the offer
- The five-minute verification routine
- If you have already paid or shared documents

Why remote and abroad job seekers are the target

A scam needs three things: a plausible reason you will never meet the employer in person, a plausible reason for money or documents to change hands, and a candidate under enough pressure not to check. Remote work supplies the first, visas and relocation supply the second, and a job search supplies the third.

That is why every listing on EnRoute is read by a person before it goes live, and why the site marks verification tiers. It is also why this checklist exists: most of your search happens beyond any one site, and the signals below work anywhere.

THE ONE RULE

A real employer never asks the candidate for money. Not for equipment, not for training, not for a visa, not for a background check, not for a "refundable deposit". Everything below is a refinement of that.

01

The five scam shapes

SHAPE	HOW IT WORKS	THE TELL
The equipment cheque	You are "hired" after a chat-only interview and sent a cheque to buy a laptop from their "vendor". The cheque bounces after you have paid the vendor.	A cheque, then a request to send money onward. Real companies ship equipment or reimburse.
The visa fee	A job abroad is offered; a "processing", "sponsorship" or "work permit" fee is required up front, often through an agent.	Any fee before a contract, or any fee at all for a sponsored visa. Employers pay sponsorship costs.
The reshipping or money mule	A "logistics" or "finance" remote role that involves receiving packages or funds and sending them on.	The job description is about moving things you did not buy or money you did not earn.
The impersonation	A real company's name, logo and even staff names used from a lookalike domain or a messaging app.	The email domain is not the company's; the interview is on Telegram or WhatsApp; the "recruiter" is not on the company's site or LinkedIn.
The identity harvest	A long application that collects passport scans, tax numbers and bank details "for onboarding" before any offer.	Sensitive documents requested before a signed contract, or by someone who is not HR at a verified domain.

02

Red flags, in the order you will meet them

Tick anything that applies. One flag is a question. Two is a pause. Three is a no.

In the listing

- ☐ Pay well above market for the role and level, with vague duties.
- ☐ No company name, or a name with no website, no registration, no staff anywhere.
- ☐ A free email domain (gmail, outlook) for a company that supposedly has hundreds of staff.
- ☐ Every requirement is soft ("motivated", "reliable") and nothing is specific.
- ☐ The listing says "no experience necessary" for a role that plainly needs it.
- ☐ The same text appears under several company names when you search a sentence of it.
- ☐ It says visa sponsorship or relocation is "guaranteed" with no process described.

In the first message

- ☐ Contact comes through a messaging app, or moves there immediately.
- ☐ You are hired, or nearly, before any interview.
- ☐ The recruiter's name and photo do not match anyone at the company.
- ☐ Pressure: "the position closes today", "reply within the hour".
- ☐ A link to "complete your profile" on a site you have never heard of.

In the interview

- ☐ Text-only "interview" on chat; no video, no voice, no camera when asked.
- ☐ They cannot describe the team, the manager, the tools or a normal week.
- ☐ You are asked for your date of birth, ID number or bank details "for the record".
- ☐ The interviewer is reading from a script and cannot answer a follow-up.

At the offer

- ☐ Any request for money: equipment, training, software, a deposit, a fee, a courier.
- ☐ A cheque or transfer you are asked to forward in part to someone else.
- ☐ A contract with no company registration number, address or signatory.
- ☐ Work that starts before the contract, "as a trial", unpaid.
- ☐ A visa or work permit that you must pay an "agent" for.
- ☐ Passport and bank details requested before the contract is signed by both sides.

03

The five-minute verification routine

Do this for every offer, from any source.

1

Find the company independently.

Search the name. Find the official website and its careers page without using any link the recruiter sent. Is the role there? Is the company registered where it says (most countries have a free company register)?

2

Check the domain.

The email you received should come from the domain on that official site. Look for one-letter changes, added words ("-careers", "-hr") and different endings.

3

Find the person.

Search the recruiter or hiring manager by name plus the company. A real recruiter exists on LinkedIn or the company site with a history longer than a month.

4

Ask for a video call.

Ten minutes with a camera on. A scam will not do this; a real employer will find it normal.

5

Ask for the company's legal name and address in writing.

And check them against the register from step one. A real employer has these on every contract anyway.

Company _____ Official site (found independently) _____

Registration number and country _____ Email domain matches? ☐ Yes ☐ No _____

Recruiter found independently? ☐ Yes ☐ No _____ Video call done? ☐ Yes ☐ No _____

Flags ticked (section 2) _____ Decision: ☐ Proceed ☐ Ask more ☐ Walk away _____

WHAT A REAL SPONSORED JOB LOOKS LIKE AT OFFER STAGE

A written offer on letterhead with the legal entity, a named signatory, the visa class they will sponsor, and a statement that the offer is conditional on visa approval. The employer or their immigration lawyer contacts you for documents after you have signed. Nobody asks you for money at any point. The Visa-Sponsored Job Playbook in this library walks through the real process step by step.

04

If you have already paid or shared documents

Money

- Contact your bank or card provider immediately; chargebacks and transfer recalls have time limits measured in hours.
- Report to your national fraud reporting service (in the US, reportfraud.ftc.gov and ic3.gov; in the UK, Action Fraud; most countries have an equivalent).
- Keep everything: messages, emails, receipts, the listing. Screenshot before it disappears.
- Do not pay anything more, including "recovery" services that contact you afterwards; those are the same people.

Documents and identity

- Passport scan shared: report to your passport authority; consider renewal.
- Bank details shared: tell the bank, watch the account, consider a new account number.
- Tax or social-security number shared: place a fraud alert or credit freeze where your country offers one.
- Login details shared: change them everywhere they were reused, and turn on two-factor authentication.
- Report the listing to the platform it appeared on so it comes down.

Being targeted is not a failure of judgement. Scams are designed by people who do this full time against people who are doing it once, under pressure. The routine above is how you stop being the easy case.

EnRoute Jobs

The work is out there. So is the world.

Remote roles, visa-sponsored positions, seasonal contracts and work exchange, every listing read by a person before it goes live. Free for job seekers.

BROWSE JOBS

enroutejobs.com/jobs

AI CAREER TOOLS

enroutejobs.com/tools

FOR EMPLOYERS

enroutejobs.com/employers

MORE FROM THE LIBRARY

- The Visa-Sponsored Job Playbook
- The Remote Job Search Tracker
- The Geo-Flex Score Field Guide
- The Work Exchange Starter Kit

All at enroutejobs.com/publications

Published by EnRoute Jobs, LLC. This document is general information, not legal, tax or immigration advice. Visa rules, income thresholds, fees and costs change; the figures here were current when this edition was prepared and should be confirmed with the relevant authority before you act on them.

You may print and share this document freely for personal or internal company use, unchanged and with attribution. It may not be resold.