Avoiding aviation job scams



aviationjobsearch

Aviation professionals are a well-suited target for job scams. Careers in this industry often involve international relocation, licence conversions, medical certificates, type ratings, and other genuine costs and paperwork — which gives scammers convincing cover. A fake fee or document request can look just like part of the normal process to someone unfamiliar with a particular operator or country.

When you factor in a competitive job market, long gaps between roles, and the pressure many pilots and engineers feel to secure command time, a type rating, or their first contract, and you have exactly the conditions scammers look for. They target people who are hopeful and under pressure, not just people who are careless.

The good news: these scams follow recognisable patterns. Once you know what to look for, most of them become easy to spot — often within the first message.

This guide walks through how these scams typically work, the specific patterns seen across pilot, cabin crew, and engineering recruitment, and how to verify whether an offer is genuine before you hand over money or personal information.



Inside

How the scam normally works 4

Scam patterns to look out for 5

Money red flags 7

Information red flags 8

How to verify a genuine offer 9

If you think you've been targeted 11

Anti-scam checklist 12

Upload your CV to Aviation Job Search and get found by hundreds of verified recruiters from airlines, MROs and aviation companies: aviationjobsearch.com/register



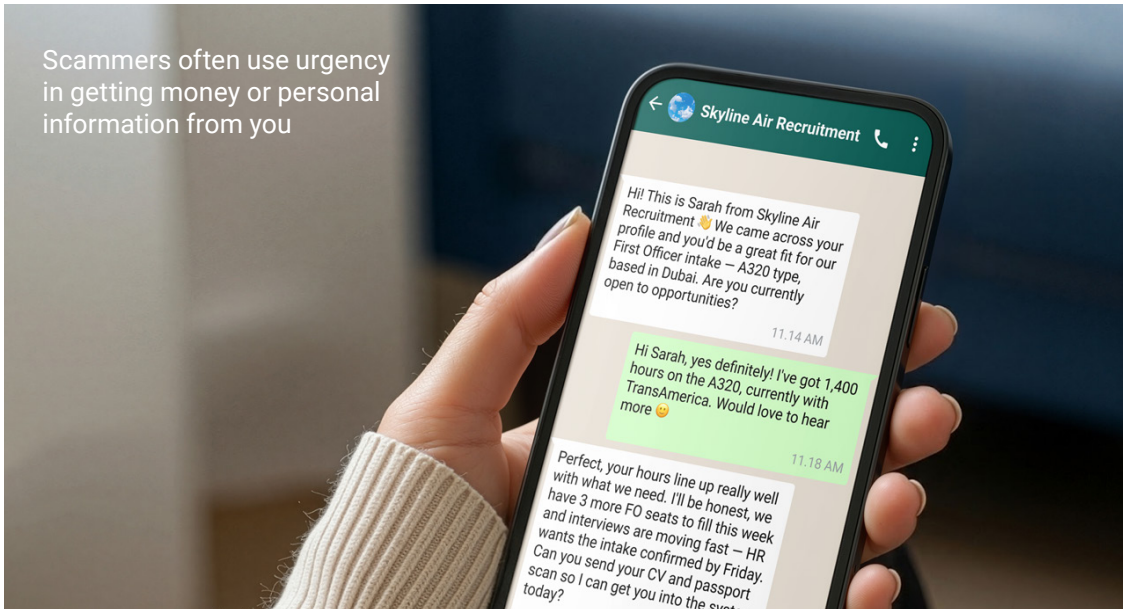
How the scam normally works

Most job scams follow a similar sequence, regardless of industry. It starts with an unsolicited message — usually on LinkedIn, Indeed, or WhatsApp — from someone claiming to be a recruiter for a well-known airline, MRO, or operator.

They reference your profile, your licence, or your aircraft type, and say you're a strong match for a role. The message is friendly, personalised but also has a sense of urgency. Next comes an official-looking document: a job briefing, an interview invitation, or an offer letter carrying the company's name and logo. The process might include a short video call.

Everything looks legitimate on the surface, but then comes the pivot. You're asked to pay for something — equipment, a background check, a training module — or to hand over sensitive personal details to "complete your paperwork." The company will reimburse you, they say. It never happens.

Genuine employers don't ask candidates to fund their own onboarding, and they don't need your bank details before you've signed a contract. Once you can recognise this shape, the aviation-specific versions become much easier to catch.



Upload your CV: www.aviationjobsearch.com/register

Scam patterns to look out for

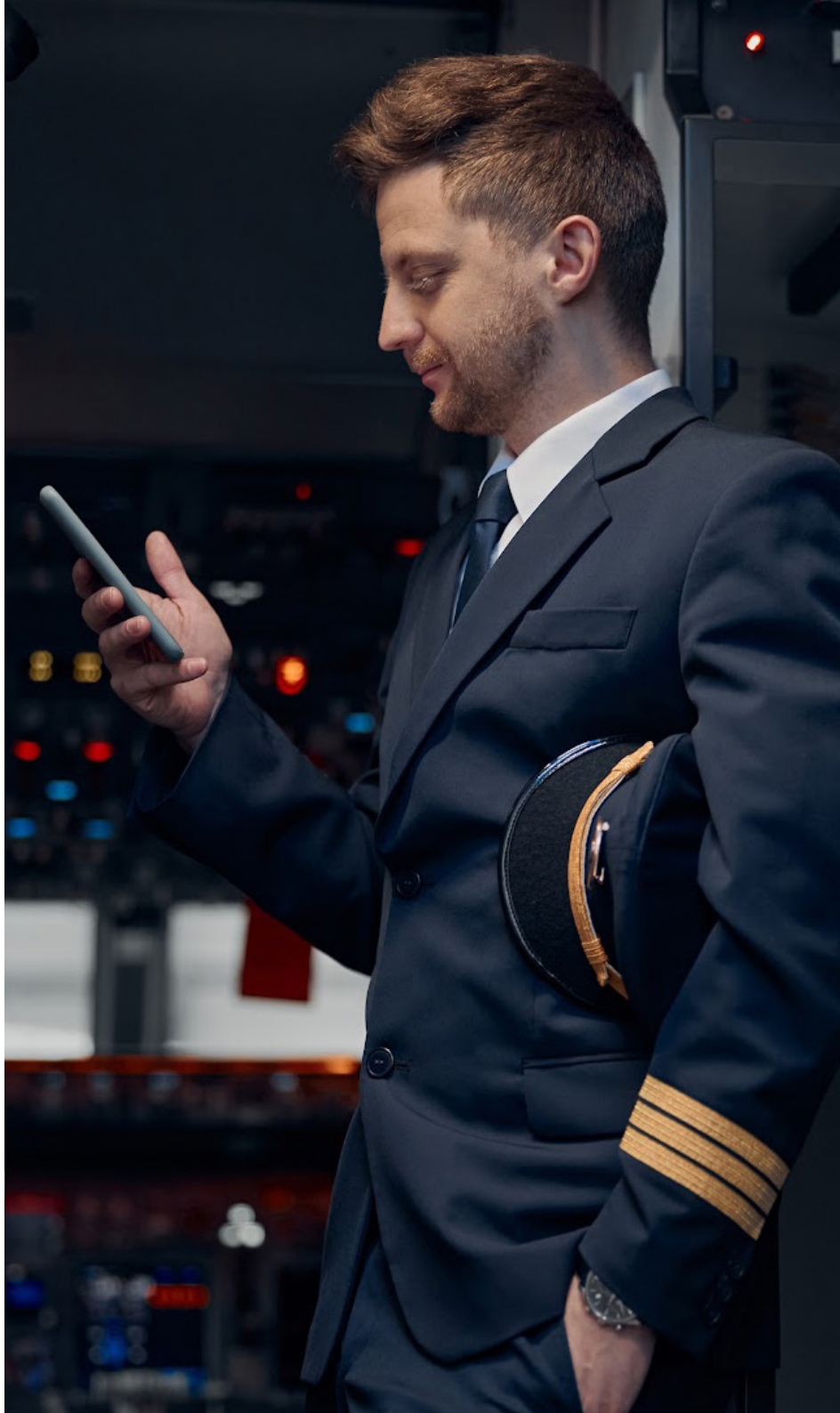
Aviation scams tend to dress themselves in language specific to the role being targeted. Here are just some of the scam patterns to look out for so you can identify them.

Targeting pilots and cabin crew

Fake type-rating and “pay to fly” schemes

A message offers a first officer role, contingent on completing a type rating or line training through a specific, unfamiliar provider — at your cost, often tens of thousands of dollars, with a promised contract waiting at the end.

Legitimate cadet and type-rating pathways exist, but they’re arranged directly with recognised training organisations, not brokered by a recruiter demanding payment to a personal account.



Fake cadet programmes

Aimed at those trying to enter the industry, these promise guaranteed jobs on completion of a paid course, often with no real airline attached to the "guarantee."

Fake cabin crew and ground staff academies

Promising placement in exchange for registration or security deposit fees — genuine airlines and ground handlers don't charge candidates to apply or interview.

Impersonated ACMI and charter operators

Urgent, high-paying contracts with real company names attached, but communication from personal email addresses (such as gmail.com) rather than the company's own domain (eg, etihad.com).

Targeting engineers and AMEs

Engineers and licensed AMEs face their own versions of these scams, often built around the genuine costs and technical language of the trade.

Fake licence conversion services

A message offers to fast-track an EASA Part-66, FAA, or other licence conversion for a fee, sometimes bundled with a "guaranteed" job offer once the conversion is "complete." Genuine licence conversions go through the relevant national authority, not a recruiter.

Mandatory toolkit or equipment purchases

You're told the role requires you to buy a specific toolkit, uniform, or software licence from a named supplier before starting — paid upfront, to be reimbursed later. This mirrors the equipment scam seen across the industry, but engineers are a particular target given the legitimately high cost of professional tooling.

Impersonated OEMs and MROs

Scammers have used the names of major manufacturers and defence contractors in fake engineering job offers, prompting several to publish dedicated fraud warnings on their careers pages. Always check a company's own site for an equivalent notice before engaging further.

Fake overseas contract offers

Attractive day-rate contracting roles requiring an upfront visa, medical, or relocation "processing fee" paid directly to the recruiter rather than a verified visa authority or employer payroll.

Upload your CV: www.aviationjobsearch.com/register

Money red flags

However it's dressed up, almost every job scam eventually asks for money. These are the patterns to watch for.

Any upfront payment at all

Legitimate employers do not ask candidates to pay for equipment, uniforms, training, background checks, or "processing" before employment begins. If the company genuinely needs you to have something, they buy it, provide it, or deduct it from salary — they don't ask you to front the cost.

Reimbursement promises

A common trick involves sending a cheque for "equipment" and asking you to deposit it and forward part of the funds elsewhere. The cheque bounces days later, after the money has already left your account — and you're liable for the shortfall.

Payment via personal apps, wire transfer, or crypto

Zelle, PayPal (friends and family), cash apps, gift cards, or cryptocurrency are the preferred methods for these



scams, since they're difficult to trace or reverse. No legitimate employer or training provider insists on these specifically.

Pressure to pay quickly

Urgency — "the seat closes today," "the visa deadline is tomorrow" — is designed to stop you pausing to check.

Upload your CV: www.aviationjobsearch.com/register

Information red flags

The second thing scammers want, alongside or instead of money, is your personal data — often for identity theft or resale.

Be cautious if you're asked for any of the following before a genuine offer and contract are in place:

- Passport or national ID details
- Medical certificate information
- Full licence number, in combination with other identifying details
- Bank account or card details, "for payroll setup," ahead of a signed contract
- Social Security, National Insurance, or equivalent tax numbers

A genuine employer will collect this information as part of a structured onboarding process, after a contract has been signed, usually through a secure HR system rather than over email or WhatsApp. Being asked for this before your questions about the role, salary, or reporting line have even been answered is a strong signal something is wrong.

If in doubt, share nothing until you've independently verified the recruiter and the role through a channel you found yourself — not one they gave you.



Upload your CV: www.aviationjobsearch.com/register

How to verify a genuine offer

A few checks, done before any money or data changes hands, will catch almost every version of this scam.

Go direct to the company

Search for the operator's official careers page yourself, rather than clicking a link in the recruiter's message. Genuine vacancies are usually listed there. If the role isn't listed and the recruiter can't explain why, be cautious.

Check the email domain

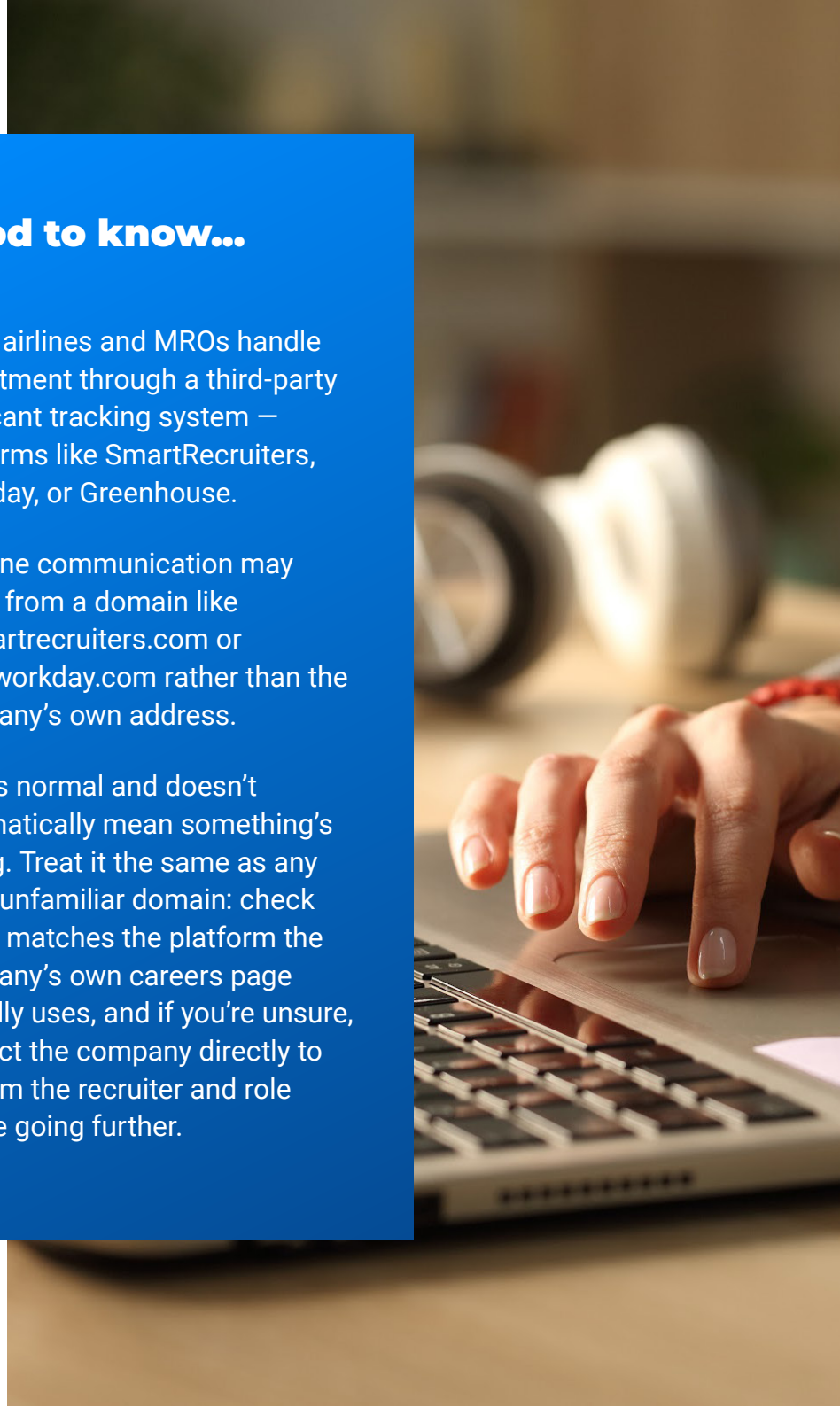
A recruiter emailing from a personal Gmail or Outlook address, rather than the company's own domain, is a major warning sign. Many airlines and manufacturers now state this explicitly in their own recruitment fraud notices.

Good to know...

Many airlines and MROs handle recruitment through a third-party applicant tracking system — platforms like SmartRecruiters, Workday, or Greenhouse.

Genuine communication may come from a domain like @smartrecruiters.com or @myworkday.com rather than the company's own address.

This is normal and doesn't automatically mean something's wrong. Treat it the same as any other unfamiliar domain: check that it matches the platform the company's own careers page actually uses, and if you're unsure, contact the company directly to confirm the recruiter and role before going further.



Call a number you sourced yourself

Not one provided by the recruiter. Use the number listed on the company's official website or LinkedIn page to confirm the role and the recruiter's identity.

Search the recruiter's name and photo

A reverse image search on a recruiter's profile photo sometimes reveals it's been lifted from a genuine employee elsewhere.

Trust the pattern, not the polish

Professional formatting and a real company logo don't rule out a scam — both are easy to copy.



If you think you've been targeted

If something feels off partway through a process, it's worth stopping and verifying before going any further, even if that means missing out on a role that turns out to be genuine. Acting quickly matters more than acting perfectly. Report first, then work through the details.

If you haven't paid or shared sensitive data

Stop responding, and report the account or message to the platform it came through (LinkedIn, Indeed, WhatsApp) and to the company being impersonated — most large employers have a dedicated recruitment fraud contact.

If you've shared personal information

Contact your bank to flag possible fraud risk, monitor your accounts and credit report, and consider a fraud alert or credit freeze where available in your country.

If you've already sent money

Contact your bank or payment provider immediately — some transfers can be recalled if reported quickly. Report the scam to your national fraud reporting body (such as Action Fraud in the UK, or the FTC/IC3 in the US), and file a report with local police if requested for insurance or bank purposes.

Upload your CV: www.aviationjobsearch.com/register

Your anti-scam checklist

Run through this before responding to any unsolicited aviation job offer.

Before you engage

- ☐ Every example in my CV and cover letter is genuinely mine
- ☐ The recruiter's email address matches the company's own domain
- ☐ I can find this vacancy listed on the company's official careers page
- ☐ I've searched the recruiter's name and photo for anything suspicious

Before you pay anything:

- ☐ I haven't been asked to pay for equipment, training, visas, or "processing" upfront
- ☐ No one has asked me to pay via Zelle, PayPal (friends and family), gift cards, or crypto
- ☐ I haven't been sent a cheque and asked to forward part of it elsewhere

Before you share information:

- ☐ I haven't shared passport, medical, licence, or bank details ahead of a signed contract
- ☐ I've verified the role and recruiter through a phone number or website I found myself, not one they gave me

If something feels wrong:

- ☐ I know where to report it (the platform, the impersonated company, and my national fraud reporting body)
- ☐ When in doubt, slow down and verify. A genuine opportunity will still be there once you've checked.

Upload your CV: www.aviationjobsearch.com/register



Helping support the careers of aviation professionals for 25 years

Make you upload your CV here
www.aviationjobsearch.com

Get the latest career advice
aviationjobsearch.com/career-hub