Something's Off in *Tech Hiring*

A Founder's Guide to Spotting Fake Candidates

WHAT'S HAPPENING

If you've been hiring engineers recently, you've probably noticed something feels off. More applications coming in, but fewer that actually hold up. Resumes that look polished on paper but fall apart the moment you start asking real questions.

It's not your imagination. **AI-generated resumes, fake LinkedIn profiles, and proxy candidates** — people interviewing on behalf of someone else entirely — are a real problem in technical hiring. And even experienced recruiters are getting fooled.

The problem is more widespread than most founders realize. Fraud rings are now organized and well-funded, and the tools used to fake identities are improving faster than most hiring processes can adapt. Whether you're running your first technical hire or your twentieth, knowing what to look for is the best defense you have.

1 in 4

Candidate profiles globally are projected to be fake by 2028, according to Gartner

41%

Of organizations have unknowingly hired a fraudulent candidate, according to GetReal Security

1,300%

Increase in deepfake fraud attempts in 2024, according to Pindrop's Voice Intelligence Report

Continued on next page →

Here's *What to Watch For*

BEFORE THE INTERVIEW

- Resume bullet points that are oddly uniform — identical structure, round-number metrics, zero company-specific detail
- Claimed employers that have little to no web presence
- LinkedIn profile that's either brand new or missing entirely — despite years of claimed experience
- Location on the resume doesn't match their LinkedIn
- Run a reverse image search on their LinkedIn photo — stock photos and recycled images are more common than you'd think

DURING THE INTERVIEW

- Slight but consistent delays before answering — even simple questions
- Answers that sound polished at a high level but go vague the moment you ask for specifics
- Camera off, or odd video behavior — lighting shifts, background inconsistencies, lip sync that feels slightly off
- Can't speak with any real depth about what they personally built or what tradeoffs they made
- Claims to be local but won't accommodate an in-person or same-timezone request

AFTER THE INTERVIEW

- Their thank-you note or follow-up email reads like it was written by a completely different person
- GitHub portfolio looks recycled, sparse, or inconsistent with their claimed experience
- References that can't be reached or verified at all
- If you had more than one conversation, compare them — different energy, different depth, or a noticeably different presence across stages is a signal worth taking seriously

What Actually Works

1. **Cross-reference before you get on a call**
   Compare every employer, title, and date on their resume against their LinkedIn. Mismatched titles and shifted dates are the most common tells — and it only takes a few minutes.

2. **Ask something spontaneous**
   Fraudulent candidates prepare for predictable questions. Go off-script. Context, motivation, and how they talk about their own work are much harder to fake than a polished answer.

3. **Give them something real to solve**
   Live problem-solving reveals more than any prepared answer will. It doesn't need to be elaborate — even a simple, role-relevant scenario will tell you a lot.

4. **Add light friction to the process**
   A short camera-on moment, a spontaneous follow-up question, or a quick skills check creates enough friction to deter most fraud without slowing down legitimate candidates.