

The Candidate in Front of You Might Not Be **Real**.

AI did not just change how people apply. It changed who is applying, and whether you can trust what you see. Here is what the data shows, and what still works.

For two decades, two things did most of the early filtering in hiring: the resume, and a short screen to confirm the person matched it. Both just stopped being reliable, and not at the margins. The tools candidates now use, and in a growing number of cases the people posing as candidates, have turned the front of the funnel into something you cannot take at face value.

THE FLOOD IS REAL, AND MOST OF IT IS MACHINE-MADE

11,000/min

APPLICATIONS ON LINKEDIN

Up 45% in a year. Hiring managers open the inbox to hundreds of resumes that read like one person wrote all of them. (NYT / LinkedIn, 2025)

39%

USED AI TO APPLY

Of candidates, with many generating resume text, cover letters, and work samples. Auto-apply bots send hundreds at a click. (Gartner, 2025)

28%

FAKED WORK SAMPLES

Admitted using AI to produce fake work samples, and 32% claimed AI skills they do not actually have. (Greenhouse, 2025)

The instinct is to call this a candidate problem. It is not. If your process leaned on the resume to do the filtering, AI just proved the resume was never a strong filter to begin with.

THE FAKES ARE NO LONGER RARE, AND SOME ARE NOT EVEN PEOPLE

By 2028, Gartner projects **1 in 4 candidate profiles worldwide will be fake**. In a 2025 survey, 6% of candidates already admitted to interview fraud, posing as someone else or having someone pose for them.

Gartner, July 2025. The 1-in-4 figure is a forecast, not a current count.

This is where it stops being about polished resumes and starts being about identity. The FBI has warned since 2022 that applicants are using deepfake video, voice, and stolen personal data to land remote roles, especially in IT, engineering, and software. Security firm KnowBe4 hired one such person in 2024. The photo was AI-altered, the stolen identity cleared a background check, and four video interviews raised no alarm. Malware showed up on the laptop on day one.

THIS IS NOT HYPOTHETICAL. IT IS A FEDERAL CASE.

The U.S. Department of Justice has spent 2024 and 2025 dismantling a scheme in which North Korean operatives, using stolen American identities, were hired as remote workers at more than 300 U.S. companies, including many in the Fortune 500. One facilitator in Arizona ran a "laptop farm" out of her home, helped place workers at over 300 businesses, and was sentenced in July 2025. The scheme tied to her generated more than 17 million dollars. The prosecutor's summary was blunt: "The call is coming from inside the house."

A fraudulent hire is not just a bad hire. **It is an open door.**

The average malicious-insider incident reached 4.99 million dollars, the most expensive attack type IBM tracks, a real risk for anyone hiring for access to systems, data, or customers. (IBM Cost of a Data Breach, 2024)

WHY THE OLD FILTERS STOPPED WORKING

A resume can be generated in seconds. An automated screen reads keywords, not people, and cannot confirm an identity. A quick video call can be deepfaked. A take-home assignment can be completed by a model, and real-time tools now feed candidates answers during live interviews, one of which raised 15 million dollars in venture funding in 2025. Every shortcut the last decade added to hiring is now the exact surface AI exploits.

WHAT ACTUALLY WORKS

The fix is not better fraud detection software. It is the thing the shortcuts replaced: a real person, talking to a real person, early, in a way that is hard to fake. The research has been consistent for 25 years. A structured live interview is the single strongest predictor of whether someone will perform, ahead of cognitive testing and far ahead of the resume.

- **Move a live human conversation earlier**, before the formal rounds. Ask for a specific account of a decision the person actually made, and why. A model and a confident faker both come apart when the question is "walk me through what you did."
- **Verify identity and history directly**. The FBI's own guidance: confirm prior employment with the businesses, cross-check photos and contact details, and watch for reused phone numbers and shifting bank details.
- **Use live, harder-to-fake interaction for sensitive roles**. Google, McKinsey, and Cisco have all brought back an in-person or verified round in 2025 for exactly this reason.

A 15-MINUTE SCREEN THAT IS HARD TO FAKE: THREE QUESTIONS

- 1 Walk me through a call you got wrong, and what you changed afterward.
- 2 Why did you make that tradeoff the way you did, and not the other way?
- 3 Tell me about a decision you owned that did not work out.

WARNING SIGNS WORTH A SECOND LOOK

- Reluctance to turn the camera on, or audio that lags the lips
- A resume and answers that are fluent but never specific
- Work quality that does not match the interview
- Reused or VoIP phone numbers, and shifting bank details
- Asking to ship equipment to a different address
- Holding several full-time roles at once

You are not going to out-sort the flood, and you are not going to win a detection arms race against tools that improve every month. What you can control is how early a real, skilled human enters your process, and how hard your screening is to fake. That is the part of hiring we have run for more than 20 years.

Right now, what is the first real filter in your process, a document, or a person?