bambooHR®

UNCOVER AND STOP
AI Fraud in Hiring

"Your avatar is kind of weird. Can you take your hand and put it in front of your face?"

Dawid Moczadło, cybersecurity expert and self-described "ex-ethical hacker," is conducting a virtual interview for a developer role at his San Francisco-based LLM-powered security startup, Vidoc Security Lab, and there is something…off about the interviewee's video display.

"Is this a joke?" says the individual on the other end of the virtual meeting. Their lips barely move.

"No, it's not a joke," states Dawid calmly. "I can see you're using some kind of software."

"This is unprofessional," protested the candidate. "I won't do this."

"If you don't do it, we will end the conversation right now," says Dawid. Again, he's calm, and he seems to be holding back a smile of either amusement or amazement. Perhaps both.

"No," they say.

"Okay, thank you," replies Dawid, but before he can click End Meeting—

"Wait! Ok, I'm raising my hand. See?"

The candidate swiftly raises and lowers a glitching, but five-fingered hand. It's clear their background is a static image, but that's nothing to raise an eyebrow at in this age of remote work and sometimes impromptu workspaces.

However, their face is nearly expressionless, and they've tellingly not followed Dawid's simple direction. They lifted their hand carefully to the side of their face.

"No, like this," says Dawid, "in front." He puts his open palm in front of his face, and though his background—what looks to be a living room—is slightly blurred, Dawid's hand and face do not glitch.

The candidate shifts uncomfortably in their seat and says nothing. They do not comply. Dawid ends the meeting.

The video of Dawid's interaction with a deepfaked job candidate swept across **LinkedIn** toward the beginning of 2025. In his post, Dawid wrote that this was the second time this had happened to him in two months.

Gone are the days when "candidate fraud" meant resume embellishment and falsified credentials. Before the **1970s**, the threats facing hiring teams today were still the stuff of science fiction, and basic candidate background checks hadn't even entered the private sector yet.

Fast-forward nearly sixty years and **one in four online candidate profiles worldwide will be fake** by 2028, says Gartner. A 2025 survey of cybersecurity leaders also revealed that **62% of organizations** had experienced at least one deepfake attack in the previous 12 months.

Today, you almost have to be a cybersecurity expert like Dawid to avoid being duped by AI-wielding bad actors. Almost. Anyone is capable of side-stepping attempted fraud as deftly as Dawid did, when they know what to look for and how to act.

This guide will help you do just that—while preserving a smooth and positive candidate experience. Read on to learn how to:

- Spot real-world red flags recruiters are seeing right now in the hiring space.
- Implement simple, effective strategies at every stage of the hiring process to catch AI fraud.
- Balance your people-first values with necessary fraud-resistant hiring practices.

Hiring strategy action plan

Use this template to take stock of your current hiring approach, explore new paths to fresh talent, and give your recruiting strategy a boost.

GET THE ACTION PLAN →

"We've been seeing interesting developments as candidates use AI when they apply for jobs. AI can be used in less-than-positive ways, with AI bots applying to jobs and posing as candidates. Recruiting is actually becoming more in-person and interactive as a result, just for the sake of confirming our candidates are real people."

BEKAH WILKERSON | HR BUSINESS PARTNER | BAMBOOHR

The new faces of candidate fraud

AI has elevated the scale, speed, and sophistication of fraud into something out of a Mission Impossible script—how many times did the plot call for Ethan Hunt wearing another person's face throughout the series? (Google says "6 to 8 times.")

In the real world, convincing deepfakes have been used to con millions out of established professionals, when they're not being used to trick unsuspecting retirees, that is.

But deepfakes aren't the only bit of AI trickery showing up in hiring fraud today. Here's everything to be aware of:

AI-GENERATED APPLICATIONS

AI tools can now generate tailored resumes and cover letters in seconds. In many cases, candidates use these tools responsibly—to improve clarity or grammar. But increasingly, bots and bad actors are using AI to:

- Mass-apply to hundreds of roles automatically
- Mirror job descriptions almost word-for-word

PROXY INTERVIEWS

The person interviewing is not the person who would actually do the job. This can look like:

- A highly polished stand-in completes interviews on behalf of someone else
- AI-generated video or audio is used to mask a candidate's real identity
- Real-time coaching via chat or earpieces during interviews

RESUME AND CREDENTIAL FRAUD

Traditional resume fraud has evolved, too. AI makes it easier to fabricate:

- Degrees or certifications from institutions that don't exist
- Inflated job titles or responsibilities
- Employment histories that can't be verified

IDENTITY FRAUD

In some cases, fraudulent candidates are using stolen or AI-synthetized identities.

REFERENCE AND INTERVIEW FRAUD

Scammers can weasel into roles on false pretenses using:

- Fake references
- Burner phone numbers
- AI-voice generators
- Scripted interview answers

THE "BAIT AND SWITCH"

A different person shows up on day one, or no one shows up at all.

What scammers stand to gain

Sometimes it's not just about pilfering a few paychecks. It's about access to sensitive customer information, trade secrets and intellectual property, and proprietary systems and data.

If hired, fraudulent candidates can:

- Learn and exploit a company's digital and physical security gaps
- Target your customer and employee base for further fraudulent activity
- Syphon company resources
- Sell proprietary data or information to competitors

Until they're caught, fake hires often operate with the same access and authority as real employees. The damage can be significantly destabilizing and long-lasting.

Red flags to watch for

Fraud rarely shows up as a single blaring alarm bell like a candidate refusing to put a hand in front of their face during a video interview. More often, it's a pattern of small inconsistencies that don't quite add up.

One or two of the following red flags don't constitute fraud, but if you're considering a candidate and checking off multiple boxes in each of the following categories, it may be time to cut and run (after documenting and reporting the incident as appropriate, of course).

- [ ] **GET YOUR COMPANY GLOBAL-READY**
  - [ ] The resume matches the job description too perfectly
  - [ ] Experience reads generically, without concrete examples
  - [ ] Credentials or degrees can't be verified
  - [ ] Employment gaps that are vague or inconsistent
  - [ ] Previous employers are either very small and lack a legitimate or established internet presence, or very large, making it harder to corroborate employment

- [ ] **LINKEDIN AND ONLINE PRESENCE**
  - [ ] Brand-new profiles claiming extensive experience
  - [ ] No profile photo or profile photos that:
    - [ ] Appear AI-generated
    - [ ] Obscures the candidate's face (e.g., it's blurry or the subject of the photo is far away)
  - [ ] The candidate's name matches another person on LinkedIn with very similar work experience
  - [ ] No online evidence generated by an established third-party source that corroborates details from their resume (e.g., high school or community news article, college competition results)
  - [ ] Minimal digital footprint for senior-level roles
  - [ ] Inconsistencies between resume and online profiles

- [ ] **INTERVIEW BEHAVIOR**
  - [ ] Avoids video calls
  - [ ] Difficulty explaining past work in their own words
  - [ ] Delayed or unnatural responses during live calls
  - [ ] Answers sound polished but lack depth
  - [ ] Background noises suggest candidate is in a call center
  - [ ] Candidate is unwilling to unblur or unmask their background

- [ ] **YELLOW FLAGS**
  - [ ] Different names, phone numbers, email addresses, or physical addresses across resume or background check reports or at different points in the process, such as for official communications and to receive work equipment
  - [ ] Immediate acceptance of below-market compensation
  - [ ] Hesitation around basic identity or employment verification
  - [ ] Has recently experienced a medical injury or family crisis that doesn't prevent them from working, but does prevent them from attending in-person training or being on camera, while declining or unable to provide documentation for a legal accommodation
  - [ ] LinkedIn picture, driver's license, and/or other profile photos look like they could have been taken on the same day
  - [ ] Requests without a legitimate explanation that no taxes or deductions be taken from pay

WHAT'S NOT A RED FLAG

It's critical for HR and hiring managers to draw clear boundaries around what is due diligence and what is over-vigilance, so fraud prevention doesn't turn into a case study of subjectivity and bias.

Protecting your hiring process must go hand in hand with compliance, fairness, inclusion, empathy.

The following circumstances or characteristics are not indicators of candidate fraud, and weighing them against a candidate's eligibility or legitimacy can lead to credible allegations of discrimination:

- Speaking with an accent
- Requesting a legal accommodation
- Having lived, studied, or worked internationally
- Appearing younger or older than expected
- Having a legal name change

How AI and remote work create the perfect conditions for hiring fraud

AI didn't invent hiring fraud, but it dramatically lowered the barrier to entry.

AI automation allows bad actors to scale deceptive operations quickly, and remote hiring reduces in-person signals many recruiters have relied on for years. The combination creates a fruitful playing ground for scammers, and high-salaried remote

But technology isn't the villain, and neither is remote work. HR also uses AI tools to streamline hiring processes, and remote work has opened up manifold opportunities for individual and organizational growth and success.

The important thing to remember is for humans to remain meaningfully involved at each stage of hiring, so threats don't slip through the cracks and lead to real consequences for the company:

- Security breaches and legal exposure
- Wasted recruiter time and hiring resources
- Wasted salary and benefits investment
- Reputational and brand damage
- Burdensome remedial and administrative costs

Strategies to protect each stage of the hiring funnel

Stage	Threat	What to do
Application	Application	• Use role-specific application questions. • Add short async video responses with custom prompts. • Look for thoughtful, human answers over perfect ones.
Resume padding and fake credentials	Resume padding and fake credentials	• Cross-check experience and timelines. • Validate credentials where appropriate. • Use structured screening criteria.
Interview	Deepfake, proxy, or live coaching	• Require live video interviews when possible. • Ask context-based follow-up questions. • Ask the candidate to remove their digital background and to wave a hand in front of their face.
Offer	Identity mismatch	• Ask location-based questions. • (Re)check references.
Onboarding	Bait-and-switch or ghosting	• Use onboarding checklists to ensure consistency across new hires. • Organize a welcome call from a manager, and schedule other early manager touchpoints.

Free hiring metrics checklist

Fraud prevention takes time. As you make targeted improvements to the way you recruit and welcome new hires, this checklist covers the 9 metrics you need to track to keep your process as efficient as possible.

SEE THE METRICS →

The vital importance of human-in-the-loop AI use

In the age of AI, keeping a human in the loop during the hiring process is not only a crucial layer of fraud prevention, it's a vital part of an organization's **culture and employer brand strategies**.

"A big misconception about recruiting is that you're just filtering resumes," says Bekah Wilkerson, **HR business partner at BambooHR**. "That type of task can be sped up by AI, but there are so many other strategic aspects of talent acquisition that I think human recruiters will always be needed in some form. For example, candidate experience is huge to us at BambooHR. Finding people that align with our mission and values is huge to us. And that due diligence is best done by a human."

- **Over-automation** can make hiring feel cold and impersonal.
- AI can replicate biases or create the opportunity for unscrutinized confidence in hiring decisions.
- Artificial intelligence cannot replace the strategic value of informed **emotional intelligence**.

For these reasons, each and every hiring decision should ultimately be made by a human.

"For every candidate that applies to one of my roles at BambooHR, I look at their application," says Bekah. "Time-to-fill is important, but at the end of the day, what matters most is that we're making hiring decisions that will be positive long-term."

Need to recenter your onboarding strategy?

The Definitive Guide to Onboarding is a great place to start if you're looking to revisit and refresh the way you bring new talent into your organization.

GET THE GUIDE →

AI regulation now and in the future

From the **New York City law** regulating the use of Automated Employment Decision Tools (AEDT) to Illinois' **AI Video Interview Act**, which oversees how AI is used to analyze video interviews, AI regulation is mostly starting local, while the **EEOC** has reaffirmed that federal anti-discrimination laws apply to AI and other emerging technologies just as they do traditional employment practices.

As the future trends toward more defined regulation around AI use in the workplace, the measures you take now to protect yourself from AI fraud are also an investment in future-proofing your organization's compliance efforts.

For example, investing in AI-savvy HR software like BambooHR® helps you ensure compliance now and in the future by:

- Enabling a structured, consistent hiring process
- Creating a well-organized, secure documentation trail
- Keeping humans in the loop at every stage

> "The discussion our recruiting team has a lot right now is how do we use AI in smart ways that don't sacrifice things that are really important to us as a company."
>
> **BEKAH WILKERSON | HR BUSINESS PARTNER | BAMBOOHR**

Your 5-step AI fraud action plan

We covered what you can do to mitigate AI fraud at each stage of the hiring process, but what can you do as immediate next steps?

1. **Audit your hiring funnel**. Where are you most vulnerable?
2. **Train your team**. Can your people confidently spot AI red flags? Do they know what to do when there's a reason to suspect fraud?
3. **Add specific, fraud-preventative checkpoints**. Is fraud prevention baked into your processes?
4. **Track consistency**. How well does every department adhere to precautionary hiring protocols?
5. **Keep it human**. How aligned are your hiring practices with your company values and culture initiatives?

AI fraud in hiring is an exhausting variable in an already high-stakes effort, and as Sarah Brinton points out, "We at BambooHR are in the thick of it, too. We're working hard to hire great people who will help our customers have what they need to hire great people, too. It's all a part of our mission to set people free to do great work."

With the right structure, training, and tools, HR teams can protect their hiring process without sacrificing the quality of their candidate experience.

The future of hiring doesn't have to be colder in response to sophisticated bad actors. Even in the age of AI, hiring can be smarter, smoother, and still deeply human.

> "Candidate experience is huge to us at BambooHR. Finding people that align with our mission and values is huge to us. And that due diligence is best done by a human."
>
> **BEKAH WILKERSON | HR BUSINESS PARTNER | BAMBOOHR**

Human-first hiring doesn't mean unprotected

You're just trying to find the right people for your org—you didn't sign up to be an interrogator! But this new type of candidate fraud can have you questioning your reality, as well as the very human connections you're striving to build.

So how do you protect your organization without making your hiring process feel like a gauntlet? After all, it's talent acquisition not talent inquisition.

Sarah Brinton, Associate General Counsel at BambooHR, shares how she likes to approach candidate verification: "I like to go for a Where in the World Is Carmen San Diego? vibe versus Spanish Inquisition vibes. As I tell my kids all the time, 'Curiosity before distress.'"

You don't have to choose between a people-first candidate experience and a fraud-resistant **hiring process**, or give up kindness to stay protected. When your **processes** are structured and consistent, and your **people are well-trained**, you can feel confident that your kindness cannot be mistaken for opportunity or vulnerability to social engineers with bad intent.

"Taking care to verify that your candidates really are who they say they are is a kindness to your colleagues and your future self," says Sarah. "Companies need HR professionals to be watchful and discerning gatekeepers. Now more than ever we need them to be 'wise as serpents and peaceful as doves.'"

START CREATING A STRUCTURED HIRING PROCESS WITH THESE FREE RESOURCES

- **Interview guides**

  These keep interviews consistent and fair and make it easier to spot red flags or off-script answers.

- **Candidate scorecard**

  This helps interviewers take meaningful notes and spot patterns, which can be especially useful when something feels off but you need supporting documentation.

- **Onboarding checklists**

  These ensure early touchpoints, like manager and team intros, actually happen, which can surface issues quickly if a new hire isn't who they said they were during the interview process.