6 Tips for HR Teams to Avoid AI Scams

Artificial intelligence (AI) is transforming how organizations recruit, communicate and operate. Unfortunately, the same tools that are streamlining HR workflows are also fueling a new wave of sophisticated scams. From deepfakes of CEO voices to fake job applicants submitting AI-generated resumes, threat actors are exploiting AI to create more believable, personalized and scalable attacks. For HR teams, often the first line of communication with external candidates and vendors, understanding how these scams work can help offer a first line of defense against common, preventable scams.

This article offers six tips to avoid AI scams.

1. **Recognize How AI Is Changing Scam Tactics**
   AI tools now allow scammers to create communications and identities that look and sound increasingly real, making traditional "look for typos" advice outdated. Research shows the threat is accelerating. According to research and advisory firm Gartner, 1 in 4 job candidates could be fake by 2028, and real-world incidents already confirm the trend, including deepfake applicants who use AI-generated faces, voices and fabricated histories during live interviews. These techniques eliminate old warning signs and make deception highly scalable and personalized, putting new pressure on HR teams to rely on process rather than instinct alone.

The following are common risks to watch for:

- Highly polished phishing emails referencing real internal details
- Deepfaked audio or video claims from leadership
- AI-generated applicant profiles or resumes
- Mass-personalized scams targeting HR inboxes
- Communications that mimic internal tone or job-related language

2. **Strengthen Verification During Hiring Processes**
   Because scammers increasingly pose as applicants, contractors or potential remote workers, HR teams can build in safeguards for verification at every stage of the hiring and onboarding process. AI-generated candidates may use synthetic faces, fabricated credentials or coached responses that sound polished but lack depth. Identity checks that combine document verification; cross-checked employment history from trusted sources; and spontaneous, scenario-based interview questions can help confirm a candidate's authenticity by validating real-world experience and prompting answers that AI tools struggle to replicate convincingly.

Consider the following hiring safeguards:

- Conduct identity verification through secure, official HR platforms.
- Look for video interview red flags such as lip sync issues or visual artifacts.
- Ask follow-up questions that require sophistication or timelines.
- Verify digital documents through secure channels; never email attachments.

3. **Validate Communications Claiming to Be From Leadership**
   AI now enables scammers to impersonate executives via email, text or even live voice calls, often pressuring HR to bypass standard payroll, benefits or hiring processes. By paying close attention to message tone, timing and context, HR staff can help detect impersonators.

The following are practices for preventing executive impersonation scams:

- Always confirm unusual requests through a different communication channel.
- Never approve payroll or data changes based solely on email or chat instructions.
- Watch for tone or phrasing that doesn't match the leader's typical style.
- Question any urgent requests that bypass normal steps.
- Report impersonation attempts immediately to IT or security teams.

4. **Build Processes That Make Scams Harder to Execute**
   Even the most convincing AI scam is far less effective when strong internal processes require multiple checks and approvals. By standardizing how HR shares data, communicates with candidates and processes sensitive changes, organizations can reduce the likelihood that a single convincing message or a single rushed moment leads to a serious breach. Clear workflows also give HR teams confidence to slow down and follow protocol, even when a message feels legitimate.

The following tips can help create safeguards against AI scams:

- Require multistep approvals for payroll, benefits and access changes.
- Restrict sensitive data sharing to approved platforms only.
- Use secure systems rather than email for document exchange.
- Maintain a verification checklist for onboarding and offboarding.
- Limit access to confidential information based on role and necessity.

5. **Train Regularly on AI Threat Awareness**
   Because AI threats evolve rapidly, HR teams need frequent, targeted training rather than annual cybersecurity refreshers. Training should include real examples of AI-generated scams, simulated phishing attempts tailored to HR scenarios and practical exercises that build confidence in spotting red flags.

Consider the following training strategies:

- Offer quarterly micro-trainings on AI scam trends.
- Run realistic phishing simulations with polished AI-generated content.
- Include examples of AI deepfakes and synthetic applicants.
- Reinforce reporting expectations and a nonpunitive response culture.
- Encourage “verify first” as a normalized practice, not a hesitation.

6. **Use Technology as Support, Not the Sole Defense**
   AI-detection and cybersecurity tools can help HR teams spot anomalies, such as manipulated images or automated resume patterns, but they shouldn’t replace human judgment. Technology is best used as a first filter, with HR teams applying behavioral analysis, structured verification steps and internal process knowledge to confirm legitimacy. A blended approach ensures no single weakness becomes a failure point.

Smart ways to leverage technology:

- Use image and document verification tools when reviewing candidates.
- Flag email tone anomalies with communication-scanning software.
- Combine automated resume screening with behavioral interviewing.
- Use secure systems for data transfers and approvals.
- Pair AI-detection tools with strong human review processes.

Conclusion
As AI-driven fraud becomes more sophisticated and widespread, HR teams are among the most targeted entry points for scammers. By staying informed, alert and proactive, HR can transform from a vulnerable doorway into a powerful first line of defense, helping the organization remain resilient in an evolving landscape of AI-enabled threats.