

6 Ways HR Teams Can Stay Ahead of AI Scams



Artificial intelligence (AI) is transforming HR, but it's also powering more convincing, scalable scams. From deepfake candidates to impersonated executives, today's threats look more real than ever.

The following tips can be used to avoid HR-related AI scams.



1. Learn how to spot AI scams.

Watch for these emerging AI-driven red flags:

- Polished phishing emails with internal details
- Fake audio/video from leadership
- AI-generated resumes or profiles
- Mass personalized outreach



4. Build processes that make scams harder to execute.

Put these safeguards in place to reduce risk:

- Multistep approvals for sensitive changes
- Secure platforms (not email) for data sharing
- Standardized workflows for hiring and onboarding
- Role-based access to sensitive info



2. Strengthen verification during the hiring process.

Build these verification steps into your hiring process:

- Use secure identity verification tools.
- Watch for video glitches.
- Ask deeper follow-up questions.



5. Train regularly on AI threat awareness.

Reinforce awareness with these training strategies:

- Quarterly trainings
- Realistic phishing simulations
- Examples of deepfakes and fake candidates



3. Validate communications claiming to be from leadership.

Use these practices to verify leadership communications:

- Confirm via a second channel.
- Never approve changes based on one message.
- Check tone and phrasing.
- Be cautious of urgent requests that bypass normal processes.
- Report suspicious activity immediately.



6. Use technology as support, not the sole defense.

Leverage technology effectively with these approaches:

- Use tools to flag anomalies.
- Verify images and documents.
- Pair automation with human review.
- Use secure systems for approvals.

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.

Contact us today for additional resources.