



Hiring with Confidence in the AI Era: 3 Trends to Spot and 7 Ways to Safeguard Your Process

Insights

10.24.25

Rapid advancements in AI technology are reshaping nearly every stage of the hiring process, from how employers source talent to how candidates present themselves. Artificial intelligence can streamline staffing activities and help job seekers polish their resumes and prepare for interviews. But an emerging concern for employers is whether applicants are using AI to game the system rather than genuinely showcase their skills. How can employers embrace these new tools while still ensuring authenticity in the hiring process? Here are three deceptive practices that could lead to bad hires and seven ways to protect your business.

3 Trends to Spot

As AI tools become more sophisticated, employers face growing concerns about deepfakes, embellished work samples, and AI-generated interview responses. The first step to protect your business from these deceptive practices is to stay on top of the latest trends in this area:

1. Falsifying Job Search Materials with AI. Many job candidates use AI to help fine-tune their resumes and cover letters, and it's generally fine if an applicant uses ChatGPT to help them to speed up the process and polish their documents before sending. It becomes a problem when work samples, writing capabilities, or experience and skills are fabricated through AI, and candidates are misleading about their actual knowledge, skills, and abilities. While job seekers could fake their qualifications before the rise of GenAI, new technology makes it easier and more prevalent. Employers should be aware of this emerging issue, even if it involves only a small subset of the candidate pool.

2. Using AI to Answer Interview Questions. You may have seen this on social media: Viral videos show job candidates in remote interviews using AI on their computers or nearby phones to feed them model answers that make them sound like the perfect fit. There are even videos on how to ensure eye contact while reading the responses and what tools to use to best deceive the interviewer. *You should recognize, however, that social media influencers may actually be promoting or selling these AI tools, so their real prevalence in job interviews may also be embellished.* Still, this is an alarming trend for hiring manager who takes the time to ensure they hire who they believe to be the best candidate for the job, particularly when the cost of turnover and hiring can be exorbitant.

3. Creating Deep Fakes for Nefarious Reasons. Some job seekers are altering their appearance and voice in online interviews to look and sound more professional in so-called “synthetic interviews.” But an even scarier trend we’ve seen in the headlines recently involves criminals posing as job candidates. In particular, North Korean scammers are posing as IT workers and targeting freelance contracts at US businesses and beyond. Scammers might steal personal information and pretend to be job candidates in the hopes of getting hired, accessing trade secrets and sensitive data, installing malware, or committing financial crimes. Indeed, even a prominent cybersecurity training company fell victim to this type of scam last year.

HIRING IN THE AI ERA

3 WORKPLACE TRENDS

1

Falsifying Job Search Materials with AI

Many job candidates use AI to help fine-tune their resumes and cover letters. It becomes a problem when skills are fabricated through AI.

2

Using AI to Answer Interview Questions

Candidates in remote interviews may use AI to feed them model answers, making them sound like the perfect fit.

3

Creating Deepfakes for Nefarious Reasons

During "synthetic interviews" candidates may change their appearance and voice to be more professional, or more alarmingly, as part of a scam.



7 Ways to Safeguard Your Hiring Process

Although these deceptive practices are concerning, employers shouldn't abandon new AI tools altogether. When used correctly, artificial intelligence can help improve the hiring process and the

candidate experience. Consider taking these steps to protect your processes and benefit from the latest technology.

1. Conduct video interviews with the camera on so your hiring team can observe potential issues. When it comes to AI-fed interview answers, pay attention to whether the candidate appears to be reading or giving unusual answers. But avoid knee-jerk reactions. Candidates may simply be nervous or facing distractions or challenges that have nothing to do with AI misuse.

To spot deepfakes, look for blurry details, irregular lighting, unnatural eye or facial movements, mismatched audio, or the absence of emotion. As technology improves, you should also consider investing in threat-detection tools that can identify and flag potential deepfakes.

2. Foster a culture of awareness when it comes to hiring remote workers, similar to the way that employees are now on guard for phishing emails. Be sure they are aware of social engineering tactics that are being employed by malicious cyberattackers.

3. Consider the feasibility of conducting in-person interviews, even for remote positions. This can help you verify how candidates interact without technology. Moreover, mentioning that the process includes an in-person interview may dissuade scammers from continuing with the interview process.

4. Conduct skills assessments in a secure environment. We all use technology in our day-to-day jobs, but you may want to see how candidates perform without these tools. You could arrange for an assessment in a secure environment, such as a testing center or your corporate headquarters. Just be sure to treat all applicants consistently and fairly – and ensure your assessment and screening procedures don't run afoul of employment laws, such as the Americans with Disabilities Act, Title VII of the Civil Rights Act, state biometric data privacy laws, and wage and hour laws.

5. Audit your hiring practices to ensure your hiring team is consistently following best practices on background checks, references, resume review, interviews, and more. Be sure to verify a candidate's identity and credentials when appropriate or necessary. You'll also need to comply with the federal Fair Credit Reporting Act (FCRA) and applicable state laws when conducting background investigations.

6. Ensure your IT security monitoring systems are robust and up to date and trained to look for attempts to access unauthorized systems or download improper files.

7. Develop a robust workplace AI policy, and make sure job candidates and employees are aware of it. [Click here for the 10 things all employers must include in any workplace AI policy.](#)

HIRING IN THE AI ERA

7 WAYS TO SAFEGUARD HIRING

- 1 Conduct Video Interviews with Camera On
- 2 Foster a Culture of Awareness
- 3 Consider Conducting In-Person Interviews
- 4 Conduct Skills Assessments in a Secure Environment
- 5 Audit Your Hiring Practices
- 6 Ensure Your IT Security Monitoring Systems Are Up to Date
- 7 Develop a Robust Workplace AI Policy

The logo for Fisher Phillips, featuring the company name in white text on a red, stylized banner.

Conclusion

The AI revolution has added value to the workplace in many ways, and savvy employers can take proactive steps to address the risks while also reaping the benefits of exciting new technology. We will continue to provide the most up-to-date information on workplace data security and AI-related developments, so make sure you are subscribed to [Fisher Phillips' Insight System](#). If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our [AI, Data, and Analytics Practice Group](#) or [Privacy and Cyber Group](#).

Related People



Lisa Nagele-Piazza
Lead Content Counsel
404.760.7943
[Email](#)



David J. Walton, AIGP, CIPP/US
Partner
610.230.6105
[Email](#)

Service Focus

AI, Data, and Analytics

Privacy and Cyber