

# 5 Ways to **detect a Deepfake** in the workplace

**Deepfakes pose a significant threat to workplaces** worldwide, especially in regulated industries like **finance, insurance, and technology.**

The spread of realistic fake audio, video, and images undermines trust, disrupts operations, and damages company reputation. It can lead to fraud and security breaches.



By combining **technology with human expertise**, organisations can **safeguard your workplace** and maintain trust, compliance, and security in today's digital landscape.



## Use live video interviews with spontaneous prompts

Asking candidates to perform random actions with spontaneous requests helps reveal deepfake overlays or video filters that can't adapt in real time.



## Implement biometric authentication

Biometric checks such as facial recognition or fingerprint scans are hard to fake and add extra layers of security to your hiring process.



## Cross-check official documents in person

Where possible, verify education, credentials, and ID documents in person to uncover inconsistencies or forgeries that digital submissions may hide.



## Employ AI tools to detect deepfake artifacts

Advanced AI solutions can spot telltale signs of deepfake media, such as unnatural facial movements, mismatched audio, or image artifacts.



## Trust human intuition and oversight

Empower teams to look for subtle cues and inconsistencies that tech might miss. Human judgment remains irreplaceable in ensuring authenticity.

## Why it matters?

- Protect your organisation from fraud and financial loss
- Safeguard public trust, company reputation and regulatory compliance
- Maintain secure interaction and collaboration between onsite and remote teams.

Take the next step in reducing workplace risk and ensuring authenticity within your organisation.

**Contact Guidant Global today.**