Why Deepfakes in Virtual Meetings Are a Growing Risk For Every Business

Discover how deepfakes are infiltrating virtual meetings on platforms like Zoom and Microsoft Teams, and how liveness detection is key in the battle against these fraud attacks.

53.7%

of humans can accurately detect if AI-generated images, videos, audio, and audiovisual stimuli.[1]

Nearly

40%

of cybercriminals use Microsoft Teams and Zoom as a second step for contacting victims.[2]

30%

of enterprises may consider their standalone identity verification solutions unreliable by 2026 due to the impact of deepfakes.[3]

The growing threat of deepfakes in virtual meetings

In 2024, a finance worker at a multinational firm was tricked into paying $25 million to fraudsters after attending a virtual call with deepfakes of company executives.[4]

This isn't a single instance; it indicates a greater issue across online meetings, interviews, conferences, and virtual online sessions. Due to the rise of AI, fraudsters can create deepfakes with relative ease and use them nefariously on virtual calls. This is a dangerous, insidious form of social engineering, and we expect the problem to increase as we continue to live and work in a remote-friendly world.

Key takeaways:

- Be aware of the proliferation of deepfakes, as infiltration of virtual meetings lends false credibility to fraudulent schemes
- Implement advanced liveness detection to spot deepfakes in virtual meetings
- Stay informed on the latest fraud tactics to help protect your organization from financial losses and reputational damage
- Pindrop® Pulse for virtual meetings integrates with meeting software to notify organizers when deepfake participants are detected

[1] As Good As A Coin Toss: Human detection of AI-generated images, videos, audio, and audiovisual stimuli

[2] Egress: Phishing Threat Trends Report, April 2024, Vol. 3

[3] Gartner: Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026

[4] CNN: Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

In multichannel attacks, nearly 40% of cybercriminals use Microsoft Teams and Zoom as a second step for contacting victims.[5] Yearly, organizations advocate for greater awareness around phishing emails to help detect and stop fraudulent attacks. But, when someone looks and sounds like a company executive, it's much harder to spot—especially when humans are only 53.7% accurate at detecting AI-generated images, videos, audio, and audiovisual stimuli.[6]

That's why advanced technology, like liveness detection, is vital in catching and stopping deepfakes—before they cause serious damage.

Common tactics fraudsters use

Fraudsters are evolving their strategies quickly. From spoofed identities to advanced video simulation to audio manipulation, fraudsters are perfecting tactics that attack weaknesses in security protocols.

Spoofed identities

Armed with personal details from data breaches and information freely available on social media, fraudsters can convincingly spoof individuals' identities.

Spoofing individuals can harm organizations, especially when fraudsters impersonate public figures or executives.

Advanced video simulation

AI-generated videos manipulate or alter facial expressions, actions, and more to mimic individuals and create fabricated scenarios.

These videos can deceive stakeholders or employees by portraying false statements or actions. For example, fraudsters used AI-generated deepfakes to impersonate Arup's CFO and other employees during a video conference, convincing a staff member to transfer $25 million to Hong Kong bank accounts.[7]

Audio manipulation

Deepfake audio is often created using text-to-speech (TTS) engines and advanced AI. For example, fraudsters targeted WPP, the world's largest advertising group, by creating a deepfake voice clone and fake WhatsApp account to impersonate CEO Mark Read. The attack involved using YouTube footage to deceive employees during a virtual meeting.

---

[5] Egress: Phishing Threat Trends Report, April 2024, Vol. 3
[6] As Good As A Coin Toss: Human detection of AI-generated images, videos, audio, and audiovisual stimuli
[7] CFO Dive: Scammers siphon $25M from engineering firm Arup via AI deepfake 'CFO'

The importance of combatting deepfakes in virtual meetings

In our remote-friendly world, meeting software like Zoom and Microsoft Teams is often the location for significant interactions. When deepfakes invade these spaces, individuals and organizations risk falling victim to fraudulent schemes. Protecting these spaces is vital–and advanced detection technology is key to keeping fraudulent actors out.[8]

4 Key methods of deepfake detection

Deepfakes are hyperrealistic and difficult for humans to detect alone. Different detection technologies can expose different forms of deepfakes, including audio, still images, videos, and more.

1. Audio deepfake detection

Audio deepfake detection is the ability to analyze subtle acoustic and behavioral traits that may seem normal to the human ear but reveal mechanical signatures of synthetic generation. Deepfake audio is difficult to detect with the human ear alone. Instead, deepfake detection analysis takes a precise look at the audio, including frequency, voice variance, spectral distortions, and pauses, to identify patterns distinctly different from natural human speech.

2. Detection in still images

AI-generated images sometimes have visible clues that humans can see, like unusual lighting, misplaced features, or strange backgrounds. However, there are hidden clues that only detection technology can detect, like repeated patterns over a frequency spectrum. Data making up digital content is spread across different frequencies, and hidden patterns typically appear when AI generates synthetic content.

3. Changes over time (temporal analysis)

Temporal analysis includes examining how things change from frame-to-frame and looking for signs that a video features synthetic impersonations. Similar to audio, when video frames are analyzed over time, detection technology can identify inconsistencies in the sequence of changes from frame-to-frame.

Facial feature drift is one pattern that deepfake detection technology looks for—this includes identifying inconsistencies in the facial organs between adjacent forgery images. Additionally, AI models look for lip inconsistencies, specifically how the lips move during speech, examining differences in the speaker's mouth region.

4. Audio-visual deepfake detection

When looking at media that includes audio and video, detection technology performs additional checks for patterns that may indicate the media is synthetic. This includes lip-syncing, which compares lip movements with speech sounds to determine if they match perfectly.

[8] The Guardian: CEO of world's biggest ad firm targeted by deepfake scam

How Pindrop® Pulse for virtual meetings works

Pindrop® Pulse brings liveness detection to your most important virtual communications, including hiring interviews, business calls, and more. By capturing media through a configurable security assistant in your existing virtual meeting software, Pindrop® Pulse can alert organizers when deepfake participants are detected.

Media capture and analysis

Media capture involves inviting a security assistant to important, high-stakes virtual meetings. In beta, Pindrop® Pulse will analyze the meeting audio for deepfakes—and video deepfake analysis is expected soon. The combination of audio-visual analysis will allow for a robust, real-time examination of virtual meetings, catching deepfake participants early in the interaction.

Notification and alert mechanisms

Pindrop® Pulse works in the background of virtual meetings. The security assistant joins via calendar integration, email invitation, a companion app, or the web app, and alerts organizers when AI-generated media is detected. This real-time analysis allows for organizers to investigate and stop the call before it proceeds—helping you identify deepfakes to keep them out of important conversations.

Secure your virtual meetings with Pindrop® Pulse

High-stakes conversations about hiring, finances, and more occur on virtual meeting platforms daily–and these interactions must be safeguarded against deepfake attacks. Pindrop® Pulse for virtual meetings brings highly reliable deepfake detection, proven by independent, third-party analysis from NPR.org,[9] to these vital interactions.

Request early access to our Pindrop® Pulse for meetings beta.

[9] Pindrop: Pindrop® Pulse Excels in NPR Deepfake Detection Study