THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Deepfakes & AI fraud — voice, video, style

AI-generated voices and videos are production-ready for everyday fraud in 2026. We show what is technically possible, how to recognise it despite that — and which processes genuinely protect against voice-to-voice attacks.

min read: 8 min **Updated:** 14 March 2026 **Risk:** High risk
Source: awareness-as-a-service.com/en/resources/threats/deepfakes-ai

What is AI-based fraud and deepfakes?

Deepfakes are AI-generated audio, video, or text content that imitates a real person. Until a few years ago this technology was accessible only to specialist labs; since 2024, high-quality voice and video fakes have been producible in minutes with commercial SaaS tools — using just a few seconds of publicly available audio.

For organisations, **voice cloning** is the most immediately relevant threat: attackers can clone the voice of a CEO, CFO, or board member from public interviews, webinars, or podcast appearances and use it for fraudulent calls. In 2026, such voices can be generated in real time — the conversation sounds natural, with pauses, filler sounds, and emphasis.

AI-generated emails are the second front: language models craft convincing text in the style and tone of the impersonated person — without spelling mistakes, without the unusual phrasing that used to serve as a phishing indicator.

At a glance

01
Real-time voice cloning is reality in 2026
Attackers can use someone else's voice in a live phone call — built from training data that is publicly accessible (YouTube, podcasts, press conferences).

02
The detection boundary has shifted
Classic detection markers (spelling errors, clunky phrasing) no longer apply to AI-generated content. Procedural controls gain importance over content analysis.

03
Authentication beats trust
Whether someone sounds like the CEO is irrelevant — if the process demands out-of-band confirmation. Process protects where the senses fail.

How to recognise deepfakes and AI fraud

! **Subtle lip-sync issues**
In video deepfakes, lip movement does not always precisely match the audio — especially during fast speech or consonants.

! **Audio artefacts on filler sounds**
"Um", "er", and spontaneous speech pauses often sound slightly artificial in cloned voices, or are absent entirely.

Unusual eye movement or blinking
Earlier video deepfakes barely blinked. Current models have improved this, but unnatural gaze patterns and facial-edge blur remain indicators.

Lack of shared-experience knowledge
A genuine manager knows the joint project, the last meeting, the joke from the team away day. A deepfake call deflects such questions or stays vague.

Unexpected request in familiar voice
The voice sounds like the CEO — but the CEO would never call to directly instruct a transfer. The content contradicts the known behavioural pattern.

Video call without video or "technical problems"
If someone claims their camera is broken, that may be an attempt to avoid video verification.

How to protect yourself

For employees

- **Evaluate content before trusting the voice:** Does the request sound typical for this person? Does it fit known processes? A familiar voice does not replace procedural controls.
- **Agree a code word:** With close colleagues and your own manager, agree a personal code word that can confirm identity in a genuine emergency.
- **Be sceptical of video calls:** Stuttering image, camera refusal, poor connection — these are signals that justify verification through a second channel.
- **Never decide under time pressure:** Deepfake calls often combine impersonation with urgency. Asking follow-up questions, calling back, or looping in a colleague is legitimate and professional.

For administrators

- **Out-of-band verification as a process standard** for all transactions or changes instructed by call or video.
- **Deepfake detection tools** for critical video meetings are worth evaluating — still maturing, but useful as a supplementary layer.
- **Deepfake awareness training** in the security awareness programme — many employees still underestimate what is technically possible in 2026.
- **Social media monitoring:** Executives who speak frequently in public videos (management, PR leads) inadvertently create training data. Raise awareness of this risk dimension.
- **Bank account change and large-transfer processes** must be designed so they can never be triggered on the basis of a single channel.

Real cases

CASE 01 · BANK · DE · Q3/2025

A financial institution received a video call apparently from the CFO of a corporate client, authorising an urgent transfer of EUR 2.8 million. The face was convincingly reproduced; the voice nearly perfect. Two bank employees approved the transaction.

Damage: EUR 2.8 million · **Detection:** the real CFO called two hours later about a separate matter · **Lesson:** Video conference identity is not sufficient for large transactions. Out-of-band confirmation via a separate phone line or in person is mandatory.

CASE 02 · MACHINE MANUFACTURER · CH · Q4/2025

Attackers cloned the CEO's voice from a trade-fair presentation available on YouTube. The CEO fraud call to the head of accounting was content-precise (current project names, supplier relationships). She transferred CHF 125,000 before the real CEO was reachable.

Damage: CHF 125,000, reversal failed · **Detection:** the CEO called 90 minutes later · **Lesson:** Public video appearances create deepfake training data. Awareness and processes must keep pace.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Stop the transaction** if possible — call your bank immediately (transfer recall).
2. **Document the incident:** Recording of the call (if available), timestamp, content log.
3. **Inform IT Security and management** — deepfake incidents are often part of coordinated attacks.
4. **No public communications** before alignment with legal — deepfake allegations against external parties have legal consequences.
5. **File a police report:** Deepfake fraud is criminal in both Germany and Switzerland; law enforcement is developing increasing expertise.
6. **Sharpen prevention measures immediately:** Review and communicate out-of-band processes.

Frequently asked questions

Can I detect a cloned voice with my own ears?

In many cases, no longer reliably. Current voice cloning models achieve a quality at which even close associates are uncertain. Hearing is not a reliable detection instrument — processes must compensate.

How much audio material does an attacker need for voice cloning?

Current models require only a few minutes of quality audio. Executives who speak regularly in podcasts, webinars, or press conferences are effectively providing publicly accessible training data.

Are there technical detection solutions?

Yes — but they represent an ongoing race between attack and defence. Deepfake detectors recognise current models but are overtaken by new ones. They are a supplementary tool, not a reliable primary protection.

Can AI-generated emails be identified by style?

Barely any more — and that is the core challenge. Earlier phishing emails had spelling errors and poor style as detection markers. AI-generated text is grammatically correct and stylistically adapted. The focus must be on content and context, not language quality.

Related topics

Deepfakes make CEO fraud more convincing and vishing attacks harder to detect. The combination of social engineering and AI is the most important threat development of the coming years.