BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Deepfakes & KI-Betrug - Stimme, Video, Stil

KI-generierte Stimmen und Videos sind 2026 reif für Betrug im Alltag. Wir zeigen, was technisch möglich ist, woran Sie es trotzdem erkennen - und welche Prozesse gegen Stimme-zu-Stimme-Angriffe wirklich helfen.

min Lesezeit: 8 min **Aktualisiert:** 14. März 2026 **Risiko:** Hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/deepfakes-ai

Was ist KI-basierter Betrug mit Deepfakes?

Deepfakes sind KI-generierte Audio-, Video- oder Textinhalte, die eine reale Person imitieren. Die Technologie war bis vor wenigen Jahren nur für spezialisierte Labore zugänglich; seit 2024 sind qualitativ hochwertige Stimmen- und Video-Fakes mit kommerziellen SaaS-Werkzeugen in Minuten produzierbar - aus wenigen Sekunden öffentlich verfügbaren Audiomaterials.

Für Unternehmen ist vor allem **Voice Cloning** relevant: Angreifer können die Stimme eines CEOs, CFOs oder Vorstandsmitglieds aus öffentlichen Interviews, Webinaren oder Podcast-Auftritten klonen und für betrügerische Anrufe nutzen. 2026 sind solche Stimmen in Echtzeit generierbar - das Gespräch klingt natürlich, mit Pausen, Fülllauten und Betonung.

KI-generierte E-Mails sind die zweite Flanke: Sprachmodelle formulieren überzeugende Texte in Stil und Tonalität der imitierten Person - ohne Rechtschreibfehler, ohne ungewöhnliche Formulierungen, die früher als Phishing-Indikator galten.

Auf einen Blick

01

Echtzeit-Voice-Cloning ist 2026 Realität

Angreifer können in einem Live-Telefonat die Stimme einer anderen Person nutzen - aus Trainingsdaten, die öffentlich abrufbar sind (YouTube, Podcasts, Pressekonferenzen).

02

Der Perimeter der Erkennung verschiebt sich

Klassische Erkennungsmerkmale (Rechtschreibfehler, holpriger Stil) gelten für KI-generierte Inhalte nicht mehr. Prozessuale Kontrollen gewinnen gegenüber inhaltlicher Analyse an Bedeutung.

03

Authentifizierung schlägt Vertrauen

Ob jemand klingt wie die Geschäftsführerin, ist irrelevant - wenn der Prozess eine Out-of-band-Bestätigung verlangt. Prozesse schützen, wo Sinne versagen.

Woran erkennen Sie Deepfakes & KI-Betrug?

Leichte Lippen-Asynchronität
Bei Video-Deepfakes stimmt die Lippenbewegung nicht immer exakt mit dem Ton überein - besonders bei schnellem Sprechen oder Konsonanten.

Audio-Artefakte bei Fülllauten
"Ähm", "öhm" und spontane Sprechpausen klingen in geklonten Stimmen oft leicht künstlich oder fehlen ganz.

Ungewöhnliche Augenbewegungen oder Blinzeln
Frühere Video-Deepfakes blinzelten kaum. Aktuelle Modelle haben das verbessert - aber unnatürliche Blickbewegungen und Gesichtsrandunschärfen bleiben Hinweise.

Fehlende Kenntnis geteilter Erlebnisse
Ein echter Vorgesetzter kennt das gemeinsame Projekt, das letzte Meeting, den Witz vom Betriebsausflug. Ein Deepfake-Anruf weicht solchen Fragen aus oder bleibt vage.

Inhaltlich unerwartete Anfrage
Eine Stimme klingt wie der CEO - aber der CEO würde niemals anrufen, um direkt eine Überweisung anzuweisen. Der Inhalt widerspricht dem bekannten Verhaltensmuster.

Videoanruf ohne Video oder mit technischen "Problemen"
Wenn jemand behauptet, eine Videokamera gehe nicht, könnte das ein Versuch sein, Video-Verifikation zu umgehen.

So schützen Sie sich

Für Mitarbeitende

- **Inhalt vor Stimme prüfen:** Klingt die Anfrage typisch für diese Person? Passt sie zu bekannten Prozessen? Eine vertraute Stimme ersetzt keine prozessuale Kontrolle.
- **Geheimwort-Protokoll vereinbaren:** Mit engen Kollegen und der eigenen Führungskraft ein persönliches Codewort vereinbaren, das im Zweifelsfall Identität bestätigt.
- **Bei Video-Calls zweifeln:** Ruckeliges Bild, weigerliche Kamera, schlechte Verbindung - das sind Signale, die Verifikation über einen zweiten Kanal rechtfertigen.
- **Nie unter Zeitdruck entscheiden:** Deepfake-Anrufe sind häufig mit Dringlichkeit kombiniert. Nachfragen, zurückrufen, einen Kollegen hinzuziehen - das ist legitim und professionell.

Für Administratoren

- **Out-of-band-Verifikation als Prozessstandard** für alle Transaktionen oder Änderungen, die per Anruf oder Video angewiesen werden.
- **Deepfake-Detection-Tools** für kritische Video-Meetings in Betracht ziehen (noch reifend, aber als ergänzende Maßnahme nützlich).
- **Schulung zu KI-Täuschung** in Security-Awareness-Programm aufnehmen - viele Mitarbeitende unterschätzen, was 2026 technisch möglich ist.
- **Social-Media-Monitoring:** Wer viel in öffentlichen Videos spricht (Management, Pressesprecher), schafft ungewollt Trainingsdaten. Bewusstsein für diesen Aspekt schärfen.
- **Prozesse für Bankkontenänderungen und Großüberweisungen** so gestalten, dass sie niemals auf Basis eines einzigen Kanals ausgelöst werden können.

Echte Beispiele

FALL 01 · BANK · DE · Q3/2025

Ein Finanzinstitut erhielt einen Videoanruf, der scheinbar vom CFO eines Unternehmenskunden kam und eine dringende Überweisung über EUR 2,8 Mio. autorisierte. Das Gesicht des CFOs war überzeugend nachgebildet, die Stimme nahezu perfekt. Zwei Mitarbeitende der Bank genehmigten die Transaktion.

Schaden: EUR 2,8 Mio. · **Erkennung:** CFO meldete sich zwei Stunden später wegen einer anderen Transaktion · **Lehre:** Videokonferenz-Identität reicht nicht für Großtransaktionen. Out-of-band-Bestätigung über separate Telefonleitung oder persönlich ist Pflicht.

FALL 02 · MASCHINENBAUER · CH · Q4/2025

Angreifer klonten die Stimme eines Geschäftsführers aus einem auf YouTube verfügbaren Messeinterview. Der CEO-Fraud-Anruf an die Buchhaltungsleiterin war inhaltlich präzise (aktuelle Projektnamen, Lieferantenbeziehungen). Die Buchhaltungsleiterin überwies CHF 125.000, bevor der echte Geschäftsführer erreichbar war.

Schaden: CHF 125.000, Rückbuchung gescheitert · **Erkennung:** Geschäftsführer rief 90 Minuten später selbst an · **Lehre:** Öffentliche Video-Auftritte von Führungskräften schaffen Deepfake-Trainingsdaten. Awareness und Prozesse müssen Schritt halten.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Transaktion stoppen**, wenn möglich - Bank sofort anrufen (Überweisungs-Recall).
2. **Verdacht dokumentieren:** Aufnahme des Anrufs (falls vorhanden), Zeitstempel, Inhaltsprotokoll.
3. **IT-Security und Geschäftsleitung informieren** - Deepfake-Vorfälle sind oft Teil koordinierter Angriffe.
4. **Keine Öffentlichkeitskommunikation** vor Abstimmung mit Rechtsabteilung - Deepfake-Vorwürfe gegen Externe haben rechtliche Konsequenzen.
5. **Strafanzeige:** Deepfake-Betrug ist in DE und CH strafbar; Strafverfolgungsbehörden haben zunehmend Expertise.
6. **Präventionsmassnahmen sofort schärfen:** Out-of-band-Prozesse überprüfen und kommunizieren.

Häufige Fragen

Kann ich mit blossem Ohr eine geklonte Stimme erkennen?

In vielen Fällen nicht mehr zuverlässig. Aktuelle Voice-Cloning-Modelle erreichen eine Qualität, bei der selbst nahestehende Personen unsicher sind. Das Gehör ist kein verlässliches Erkennungsinstrument - Prozesse müssen das kompensieren.

Wie viel Audiomaterial braucht ein Angreifer für Voice Cloning?

Aktuelle Modelle benötigen wenige Minuten qualitatives Audiomaterial. Führungskräfte, die regelmäßig in Podcasts, Webinaren oder Pressekonferenzen sprechen, liefern de facto öffentlich zugängliche Trainingsdaten.

Gibt es technische Erkennungslösungen?

Ja - aber sie sind ein Wettbewerb zwischen Angriff und Abwehr. Deepfake-Detektoren erkennen aktuelle Modelle oft, werden aber durch neue Modelle überholt. Sie sind ein ergänzendes Werkzeug, kein verlässlicher Primärschutz.

Sind KI-generierte E-Mails an Stil erkennbar?

Kaum noch - und das ist die eigentliche Herausforderung. Frühere Phishing-Mails hatten Rechtschreibfehler und schlechten Stil als Erkennungsmerkmale. KI-generierte Texte sind grammatikalisch korrekt und stilistisch angepasst. Der Fokus muss auf Inhalt und Kontext liegen, nicht auf Sprache.

Weitere Themen

Deepfakes machen CEO-Fraud überzeugender und Vishing-Angriffe schwerer erkennbar. Die Kombination aus Social Engineering und KI ist die wichtigste Bedrohungsentwicklung der kommenden Jahre.

© JULITH GmbH · awareness-as-a-service.com · deepfakes-ai