

Deepfakes – Täuschung mit künstlicher Intelligenz (KI)

Künstliche Intelligenz (KI) ermöglicht es, täuschend echte Videos, Stimmen oder Bilder zu erzeugen. Diese sogenannten Deepfakes werden auch für Betrugsversuche im Finanzbereich eingesetzt.

Wichtigste Merkmale:

- **Prüfen Sie die Quelle:** Rufen Sie bei Bedenken bekannte Kontaktpersonen über offizielle Nummern zurück, bevor Sie handeln.
- **Misstrauen Sie Dringlichkeit:** Finanzinstitute und seriöse Geschäftspartner setzen Sie nie unter massiven Zeitdruck.
- **Mehrkanal-Bestätigung:** Verifizieren Sie Zahlungsanweisungen stets über einen zweiten, unabhängigen Kommunikationskanal.

Gefahr im Finanzkontext

Im Bereich digitaler Finanzgeschäfte werden Deepfakes genutzt, um **Vertrauen zu missbrauchen** und Opfer zu finanziellen Handlungen zu bewegen.

Beispiele:

- **Gefälschte Influencer- oder Banker-Videos:** In sozialen Medien wie z. B. Facebook werben angeblich bekannte Persönlichkeiten für Investments mit «garantierter Rendite». (lesen Sie hierzu auch unseren Artikel zu «[Investment Fraud](https://www.ebas.ch/investment-fraud/) (<https://www.ebas.ch/investment-fraud/>) »)
- **Gefälschte Telefon- oder Videoanrufe von «Vorgesetzten»:** Mitarbeitende werden in einem Telefonanruf (mit gefälschter Stimme) oder Video-Call (mit gefälschtem Live-Video) angewiesen, dringende Überweisungen vorzunehmen. (lesen Sie hierzu auch unseren Artikel zu «[CEO Fraud](https://www.ebas.ch/ceo-fraud/) (<https://www.ebas.ch/ceo-fraud/>) »)

Warum Deepfakes so gefährlich sind

- **Täuschend echt:** Selbst geschulte Augen können gefälschte Videos oder Stimmen nur schwer entlarven.
- **Schnelle Verbreitung:** Social Media und Messaging-Dienste verbreiten Fälschungen in Sekunden.
- **Hohe Glaubwürdigkeit:** Das menschliche Gehirn vertraut visuellen und auditiven Eindrücken stark.

Woran Sie Deepfakes erkennen können

Auch wenn die Technologie immer besser wird, gibt es Hinweise:

- **Unnatürliche Mimik:** Gesichtsausdrücke wirken steif oder unpassend zum Gesagten.
- **Asynchrone Lippenbewegungen:** Sprache und Lippenbewegung passen nicht exakt zusammen.
- **Ton- und Bildartefakte:** Unschärfen, seltsame Lichtreflexe oder verzerrte Stimmen.

- **Ungewöhnliche Kontaktwege:** Wenn eine bekannte Person plötzlich über neue Kanäle kommuniziert.
- **Auffallende Themenwahl:** Eine bekannte Person spricht über für sie untypische Themen oder versucht Sie unter Druck zu setzen.

Deepfakes sind eine ernsthafte Bedrohung – gerade in der Welt digitaler Finanzgeschäfte. Vertrauen Sie nicht blind dem, was Sie sehen oder hören. Bleiben Sie wachsam, prüfen Sie Aufforderungen kritisch und holen Sie sich im Zweifel eine zweite Meinung ein.

Im Ernstfall: **Kontaktieren Sie sofort Ihre Bank (<https://www.ebas.ch/partner/>) und die Polizei.**

Der Begriff Deepfake setzt sich aus «Deep Learning» (eine Form der künstlichen Intelligenz) und «Fake» (Fälschung) zusammen. Dabei werden Bild-, Audio- und Videoinhalte so manipuliert, dass sie wirken, als wären sie echt.

Typische Beispiele:

Gesichts-Manipulation: *Eine Person spricht oder handelt in einem Video, obwohl sie dies nie getan hat.*

Stimmen-Nachahmung: *KI imitiert täuschend echt die Stimme einer Person.*

