

Deepfake – inganno con l'intelligenza artificiale (IA)

L'intelligenza artificiale (IA) permette di creare video, audio o immagini con un livello di realismo ingannevole. Questi cosiddetti deepfake vengono sfruttati anche per realizzare tentativi di frode in ambito finanziario.

Punti principali:

- **Verificate la fonte:** in caso di dubbi, prima di fare nulla ritelefonate alle persone di contatto che conoscete usando numeri ufficiali.
- **Diffidate del senso d'urgenza:** gli istituti finanziari e i partner commerciali seri non vi mettono mai sotto forte pressione.
- **Conferma multicanale:** verificate sempre gli ordini di pagamento attraverso un secondo canale di comunicazione slegato dal primo.

Pericoli nel contesto finanziario

Nel campo delle transazioni finanziarie digitali, i deepfake vengono utilizzati per abusare della fiducia e spingere le vittime a compiere operazioni finanziarie.

Esempi:

- **Contraffazione di video di influencer o banchieri:** sui social media come Facebook si trovano personalità famose che pubblicizzano investimenti «a rendimento garantito» (leggete anche il nostro articolo sul tema «[Investment Fraud](https://www.ebas.ch/it/investment-fraud/) (https://www.ebas.ch/it/investment-fraud/) »).
- **Contraffazione di telefonate o videochiamate dei «superiori»:** tramite telefonata (con voce contraffatta) o videochiamata (con video in diretta contraffatto) viene impartito a una collaboratrice o un collaboratore l'ordine di eseguire un trasferimento di denaro urgente (leggete anche il nostro articolo sul tema «[CEO Fraud](https://www.ebas.ch/it/ceo-fraud/) (https://www.ebas.ch/it/ceo-fraud/) »).

Perché i deepfake sono così pericolosi

- **Realismo ingannevole:** anche l'occhio e l'orecchio più allenato ha difficoltà a smascherare i video o le voci contraffatte.
- **Diffusione rapida:** i social media e i servizi di messaggistica diffondono le contraffazioni in pochi secondi.
- **Alta credibilità:** il cervello umano si fida molto delle percezioni visive e uditive.

Come riconoscere i deepfake

Anche se la tecnologia migliora continuamente, ci sono alcuni indizi cui si può fare attenzione:

- **Espressioni facciali innaturali:** le espressioni del viso appaiono rigide o inadatte a ciò che viene detto.

- **Labiale asincrono:** le parole e il movimento delle labbra non coincidono del tutto.
- **Artefatti sonori e visivi:** sfocature, strani riflessi di luce o voci distorte.
- **Modalità di contatto inconsuete:** una persona che conoscete usa all'improvviso un canale nuovo per comunicare.
- **Argomenti che sorprendono:** una persona che conoscete parla di argomenti che di solito non tocca o cerca di mettervi sotto pressione.

I deepfake sono una minaccia seria, soprattutto nel mondo delle transazioni finanziarie digitali. Non fidatevi ciecamente di ciò che vedete o sentite. Fate sempre attenzione, esaminate criticamente le richieste che ricevete e in caso di dubbio chiedete un secondo parere.

Se la questione si fa seria, **contattate immediatamente [la banca \(https://www.ebas.ch/it/partner/\)](https://www.ebas.ch/it/partner/) e la polizia.**

Il termine «deepfake» è un composto di «deep learning» (una forma di intelligenza artificiale) e «fake» (contraffazione). I contenuti grafici, audio e video vengono manipolati in modo tale da sembrare veramente reali.

Esempi tipici:

Manipolazione del volto: in un video si vede una persona che dice o fa cose che in realtà non ha mai detto o fatto.

Imitazione della voce: l'IA imita in modo ingannevole la voce di una persona.

