

Deepfakes – deception with the help of artificial intelligence (AI)

With the help of Artificial intelligence (AI), it is now possible to create deceptively realistic videos, voices or images. These so-called “deepfakes” are also used for scamming attempts in the financial sector.

The most important points to remember:

- **Check the source:** If you are concerned, ring contact persons you know well via official telephone numbers before you act.
- **Distrust urgency:** Financial institutions and reputable business partners will never put you under massive time pressure.
- **Multichannel confirmation:** Always make sure to verify any payment instructions via a second, independent channel of communication.

Risk in a financial context

Deepfakes are used in the financial sector to **abuse trust** and entice victims into financial dealings.

Some examples:

- **Faked influencer or banker videos:** On social media like Facebook, purportedly well-known celebrities promote investments with a “guaranteed return” (please also read our article on [“investment fraud \(https://www.ebas.ch/en/investment-fraud/\)](https://www.ebas.ch/en/investment-fraud/)” on this topic.)
- **Faked phone or video calls by a “manager”:** Via a phone call (using a faked voice) or video call (using a faked live video), employees are ordered to execute an urgent bank transfer (please also read our article on [“CEO fraud \(https://www.ebas.ch/en/ceo-fraud/\)](https://www.ebas.ch/en/ceo-fraud/)” on this topic.)

Why deepfakes are so dangerous

- **Deceptively realistic:** Even to the trained eye or ear, it is difficult to expose faked videos or voices.
- **Rapid spread:** Social media and messaging services can spread fakes in a matter of seconds.
- **High level of credibility:** The human brain tends to strongly trust visual and auditory impressions.

How to spot deepfakes

Even if technology is continuously improving, there are some clues:

- **Unnatural facial expressions:** They look stiff or do not seem to agree with what is being said.
- **Asynchronous lip movements:** Voice and lip movements do not match properly.
- **Sound and image effects:** Blurring, strange light effects or distorted voices.

- **Unusual contact channels:** A person you know suddenly starts to communicate via new channels.
- **Striking choice of topic:** A person you know is discussing topics out of character for them or tries to put you under pressure.

Deepfakes are a serious threat – especially in the world of digital financial business. Don't just blindly trust what you see or hear. Remain vigilant, critically check requests and obtain a second opinion if in doubt.

In the worst case: **Contact your bank (<https://www.ebas.ch/en/partners/>) and the police immediately**

The term “deepfake” is a combination of “deep learning” (a type of artificial intelligence) and “fake”. In the process, image, audio and video content is manipulated in such a way that they look real.

Some typical examples:

Face manipulation: *A person is speaking or acting in a video although he or she has never actually done so.*

Voice imitation: *AI imitates a person's voice in a deceptively realistic fashion.*

