

15.01.2026

Identity fraud when digital banking: Vigilance is king

Modern attempts at fraud are increasingly boosted by artificial intelligence – for instance via AI-generated identities or deepfake techniques able to bypass traditional defences. In consequence, it is not just technical security which is important, but also your ability to properly recognise such fakes and react to them correctly in everyday life.

Cases of identity fraud in digital banking are increasing in Switzerland, too. Criminals abuse stolen or manipulated personal data to try and open accounts, trigger payments or apply for credits – frequently without victims even noticing this straight away.

This makes it increasingly difficult for end customers to differentiate fake from real news, calls or websites. Particularly perfidious: With artificial intelligence, fraud attempts nowadays appear deceptively realistic and professional.

To protect yourself, vigilance is king:

- Don't click any links in e-mails or text messages received unexpectedly
- Never pass on log-in or card details
- Make sure to check senders, URLs and prompts particularly thoroughly
- Report suspicious processes to your bank immediately

You can find out how modern deceptions using AI work and why deepfakes pose an increasing risk in our article on [“Deepfakes – deception with the help of artificial intelligence \(AI\) \(https://www.ebas.ch/en/deepfakes-deception-with-the-help-of-artificial-intelligence-ai/\)”](https://www.ebas.ch/en/deepfakes-deception-with-the-help-of-artificial-intelligence-ai/).