27.03.2025

Deepfake fraud with banks

According to a recent study, banks, insurance companies and fintech companies in Europe have noticed a 2'137 per cent increase in fraud cases involving deepfake technologies.

Deepfakes involve image, video or audio content created by Artificial Intelligence. Amongst others, such technologies enable criminals to impersonate legitimate bank customers and therefore access their accounts or apply for credit.

They use two main methods to do so: presentation attacks and injection attacks. With presentation attacks, an identity is faked with the help of masks, make-up or by playing a deepfake video in real time, to circumvent security checks this way. With injection attacks on the other hand, non-trustworthy content such as deepfake videos are injected into a program. This often involves onboarding programs by banks or fintech companies.

Banks and financial service providers are continuously working on new security measures to hamper deepfake fraud. At the same time, there are some measures customers can take themselves:

- Using multifactor authentification: Entering several security factors during a log-in process, for instance a password and code via text.
- Regularly checking your account activities: You should immediately notify your bank of any unusual transactions or log-in attempts.
- Stay up to date: Information pertaining to current security measures and fraud attempts will help recognise any risks early.

You can find the original article here (https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year) .