27.03.2025

Deepfake-Betrug bei Banken

Laut einer aktuellen Untersuchung haben Banken, Versicherungen und Fintech-Unternehmen in Europa in den letzten drei Jahren einen Anstieg von 2´137 Prozent bei Betrugsversuchen mit Deepfake-Technologie festgestellt.

Deepfakes sind durch Künstliche Intelligenz erstellte Bild-, Video- oder Audioinhalte, die täuschend echt wirken. Diese Technologie ermöglicht es Kriminellen beispielsweise, sich als legitime Bankkunden auszugeben und somit auf deren Konten zuzugreifen oder Kredite zu beantragen.

Dabei kommen zwei Hauptmethoden zum Einsatz: Präsentationsangriffe und Injektionsangriffe. Bei Präsentationsangriffen wird eine Identität mithilfe von Masken, Make-up oder dem Abspielen von Deepfake-Videos in Echtzeit vorgetäuscht, um Sicherheitsprüfungen zu umgehen. Bei Injektionsangriffe hingegen wird nicht vertrauenswürdiger Inhalt, z.B. Deepfake Videos, in ein Programm eingeschleust. Dies betrifft häufig On-Boarding Programme von Banken oder Fintech-Unternehmen.

Banken und Finanzdienstleister arbeiten kontinuierlich an neuen Sicherheitsmassnahmen, um Deepfake-Betrug zu erschweren. Gleichzeitig gibt es einige Massnahmen, die Kunden selbst ergreifen können:

- Mehrstufige Authentifizierung nutzen: Die Angabe von mehreren Sicherheitsfaktoren bei einem Login Prozess, z.B. Passwort und Code via SMS.
- Kontoaktivitäten regelmässig überprüfen: Ungewöhnliche Transaktionen oder Anmeldeversuche sollten umgehend der Bank gemeldet werden.
- Auf dem Laufenden bleiben: Informationen über aktuelle Sicherheitsmassnahmen und Betrugsversuche helfen, Risiken frühzeitig zu erkennen.

Den Originalartikel finden Sie hier (https://www.signicat.com/de/pressemitteilungen/betrugsversuche-mit-deepfakes-nehmen-in-den-letzten-drei-jahren-um-2137-zu) .