

24.04.2026

# Fraud industrialised: How AI is revolutionising financial crime

**Those days of obviously flawed phishing mails and clumsy scamming attempts are gone for good. In 2026, we are witnessing a true watershed: Artificial intelligence (AI) has transformed cyber criminality from tedious, manual work into a highly automated industry with global scalability.**

If the norm used to be individual attackers with a limited range, nowadays organised networks using specialised AI tools, data-driven strategies and almost unlimited scalability have taken over. In case you are using e-banking and digital financial services, this means: Conventional warning signals, such as spelling errors, impersonal forms of address or strange senders are increasingly losing in significance.

While financial institutions continuously improve their technical protection mechanisms, attackers are consistently shifting their focus to the biggest vulnerability in the system: humans. And AI acts as a range extender, precision tool and deception genius at the same time.

## **Deepfakes and voice cloning: Identity turned precious loot**

The probably most dangerous development is so-called deepfakes – the ability to imitate voices and videos in a deceptively real manner. While in the past, extensive audio materials were necessary, just a few seconds of social media clips or voice messages are sufficient to create a convincing digital twin.

- **CEO fraud 2.0:**

During the course of a seemingly legitimate video conference, a “managing partner” requests an urgent remittance. Voice, face and behaviour are correct – only this person is not currently taking part in that video conference.

- **A shocking phone call:**

Victims receive telephone calls from purported family members in distress. AI doesn't just simulate their voice, but also a complete acoustic scenario including stress, emotion and environment.

## **Mass personalisation using LLMs**

A Large Language Model (LLM) is an AI system which – employing training using gigantic volumes of data to learn statistical patterns in language – can then autonomously generate logically-sounding texts and solve tasks. These models include ChatGPT, Gemini or Claude. Such LLMs allow for fraud of a totally new quality, characterised by individualisation, context awareness and real-time capability. Instead of relying on generic mass e-mails, attackers use AI to create deceptively real and highly personalised scenarios. To do so, these systems analyse publicly accessible information such as social media profiles, company websites or press releases and link them to credible stories. This is how payment reminders or project references for instance are created, which actually exist in real life and therefore hardly ever raise suspicions.

Also, language barriers are practically no longer existent. Modern-day AI isn't just able to translate correctly, but can also adjust content both in a cultural and linguistic manner. Thus scammers can act using High German, Swiss German or even regional dialects, and appear significantly more authentic than in the past.

Another decisive difference is interactivity: While classic phishing mails were of a static nature, AI-supported systems can act more dynamically in case of further enquiry. They lead convincing dialogues, provide plausible explanations, respond to objections and adapt their argumentation in line with victim reactions in real time. This creates a form of communication now hard to distinguish from authentic human interaction, significantly increasing the risk of a successful deception.

### **Automation and scaling: Fraud as a business model**

One central difference to the past is industrialisation:

- **Crime-as-a-Service:**

Criminals offer ready-made AI tools, deepfake services or complete fraud campaigns on the Darknet – complete with support and updates.

- **A/B testing scams:**

Attacks are optimised just like marketing campaigns, including tests of a number of variations, success quote analyses and strategies which are continuously adjusted.

- **24/7 operating models:**

AI systems work around the clock, without breaks or tiring, drastically increasing their efficiency.

### **The psychological trap: Social engineering in perfection**

Despite all technological advances, the core of all fraud attempts remains unchanged: the deliberate manipulation of human behaviour. In this, artificial intelligence is used to reinforce psychological levers, employing them in a more precise manner than ever before. It is particularly a sense of urgency being generated, making victims believe they have to act immediately to prevent any damage. At the same time, some sort of authority is introduced, for instance citing purported instructions by superiors, banks or authorities, which are hardly ever questioned. A principle of scarcity is also employed in a targeted way, by implying allegedly once-in-a-lifetime opportunities or a limited timeframe to act. This is supplemented by building trust, for instance by simulating famous people or personal relations.

### **Potential protection strategies**

Technical solutions alone are not enough. The crucial factor is a reinforced “human firewall” – meaning every individual person’s security awareness. AI can also be used for detection, but such processes are not as yet reliable.

- Two-factor authentication (2FA), biometric protection and transaction confirmations offer an important level of protection and should always be used.
- With unusual payment reminders, always use a second channel. Make return calls only via known phone numbers or alternative channels of communication.
- Time pressure is a classic means of manipulation. Reputable institutions will not apply any unrealistic deadlines.
- When in doubt, use the “four eyes principle”.
- Fewer publicly available personal data (on social media) will considerably reduce the attack surface.