

The Evolution of online banking fraud

And why traditional defences can't keep up

A panic economy

Anti-fraud-tech has become a shouting match



Every vendor claims to be "AI-powered," "real-time," or "autonomous." Same promises. Different logos.

The result

Panic-based marketing and blind-spot detection.



Cleafy isn't part of the panic economy.

A better way

Cyber-fraud fusion defence



A continuous detection fabric that unites:



It sees what others miss. Not another alert engine. A live map of digital trust.

Years of shifting fraud tactics

2000s Phishing & credential theft



Criminals stole logins through fake emails.



Banks countered with two-factor authentication.

2010s Malware & automation



Malware like Zeus and Gozi hijacked sessions and drained accounts.



Defences shifted to device fingerprinting and risk scoring.

2020s Mobile trojans and hybrid fraud



The boundary between cyberattacks and fraud collapsed.

Cleafy LABS uncovered multiple **zero-day mobile malware families**, built to bypass authentication and operate inside live sessions.



Attackers merged automation, social engineering, and deepfakes to scale deception.



Legacy systems, tuned for static signals, couldn't see the live manipulation inside sessions.

And now AI steps in

AI-driven fraud tactics



Attackers use lightweight, task-specific AI.



They simulate legitimate activity.



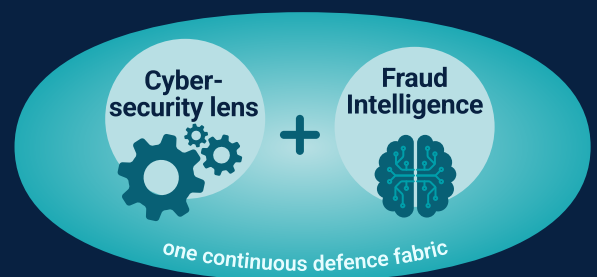
They replay real sessions so they slip past controls.



Fraud no longer starts with the transaction; it starts before login, long before money moves. This is fraud in rehearsal.

Cyber-fraud fusion defence

Cleafy extends detection beyond transactions and sessions into the pre-login phase.



From reconnaissance to takeover, Cleafy sees every stage in motion to stop it before impact.