Infographic

Cleafy

Online fraud through the years

How attack tactics have changed and why traditional defences are no longer enough

2000s

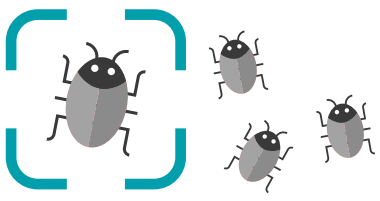
Credential theft & phishing?

Fraudsters send fake emails to **steal login credentials.**

Banks introduce 2FA (Two-Factor Authentication) to mitigate risks.

2010s

Malware & automated attacks



Attackers deploy banking malware such as Zeus, Gozi, and Carberp to steal credentials and manipulate transactions.

Banks start using **Device fingerprinting & risk scoring.**

2020s

Mobile banking trojans & hybrid fraud

The emergence of mobile banking trojans like Cerberus and Alien has revolutionised the threat landscape.

Hybrid fraud combines social engineering, real-time session hijacking, and AI-generated deepfakes.

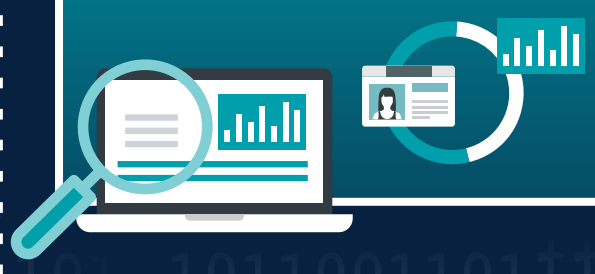
The as-a-service economy enables access to attack tools via Malware-as-a-Service, allowing less skilled groups to carry out sophisticated campaigns.

Legacy fraud detection struggles, as these attacks don't trigger traditional alerts.

Today

The need for real-time FxDR

Proactive detection based on behavioural analytics, AI, and continuous monitoring is now essential.



Banks must **stop fraud before transactions happen** rather than reacting after the fact.

To learn more about how we can help you, visit cleafy.com or email us at info@cleafy.com.
Trusted by leading Europeans and LATAM banks, boasting a 4.2 score on Gartner Peer reviews.

Cleafy - Italy | UK | Spain | Netherlands | Brazil | Colombia

Cleafy