Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x Finance

The financial services industry is a prime target for fraudsters and bears the brunt of their cyberattacks. But how should the industry react in a world where technology is constantly evolving? The answer is to prevent attacks before they occur, rather than just reacting to them.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

The finance industry suffers more damage from online fraud than any other vertical, and it shows no sign of abating as fraudulent activity continues to evolve. By gaining access to customers' personal data, fraudsters are able to take over accounts, open new ones, and even apply for credit, resulting in severe financial losses. Fraudsters use accounts to make purchases on credit, create money mules, and even launder money.

Some facts and statistics

Surveys show that more than 70% of enterprises are looking for security solutions that do not significantly affect user interaction with the digital service.

Money laundering transactions are estimated at 2 to 5% of global GDP. That's roughly $1-2 trillion USD annually.

According to Experian, online payment services logins (such as PayPal) can sell on the Dark Web for as little as $20.

What do cyber-criminals want?

- Financial gain from fraudulent transactions
- Information theft (for market intelligence and insider trading)
- Malicious service disruption
- Damage to competitors' reputation

What do clients want?

- Seamless interaction with the digital account without any additional friction
- Having their personal data protected
- Being able to access digital banking accounts from multiple devices anywhere anytime

While the realities of fraud are all-consuming, online banking remains the second most performed activity (88%) from users' devices. That means elevated responsibility for financial institutions.

Financial institutions rely on the practice of 'know your customer' in order to protect themselves and their customers from illegal transactions. Given that KYC relies heavily on electronic identity verification, financial institutions face many cybersecurity threats such as money laundering, new account fraud and account takeover.

Open banking lets financial institutions use open APIs that enable third-party applications and services to be built around their systems. The FinTech ecosystem is crowded and the rise of open banking makes it much more difficult to keep all interactions safe. The complexity and diversity of means for accessing digital accounts are opening new points of vulnerability for fraudsters to exploit. From this perspective, technology is a double-edged sword for financial institutions – something that they must use, but which also leaves them vulnerable to attack.

For instance, one in six respondents among Asia Pacific organizations state that their enterprise has put off digital transformation efforts due to the fear of cyber-risks. This affects the development of the market and makes it impossible for such ventures to take advantage of the limitless possibilities that going digital presents. This is a major barrier that stops many enterprises from taking the next step towards the market of the future. Teaming up with a proven cybersecurity provider is something that every business should aim for in order to provide a smooth digital service while keeping customer data protected.

Preventing fraud in finance

Money Laundering

- Global entity linking and mapping
- Ready to use incidents, based on the gathered data

New Account Fraud

- Immediate recognition of synthetic accounts
- Detection of new unknown devices

Account Takeover

- Uncovering signs of ATO at the stage of a login and throughout the session
- Detecting anomalies & suspicious behavior in real-time
- Accuracy and speed of detection
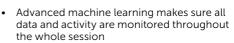
Kaspersky Fraud Prevention

Kaspersky Fraud Prevention helps organizations achieve that happy medium between usability and security of digital services. Backed by Kaspersky Lab's 21 years of experience in cybersecurity, Kaspersky Fraud Prevention takes pride in helping service providers reach the pinnacle of protection. All this comes with flexible case management and forensic capabilities that significantly reduce operational costs for enterprises.

Kaspersky Advanced Authentication

- Prioritizing legitimate users and detecting suspicious ones

- Risk-based authentication continuously monitors numerous unique parameters

- Real-time analysis of biometric, behavioral and environmental data

- Legitimate users proceed to their digital accounts without any unnecessary verification steps, which means reduced two-factor authentication costs for providers

Kaspersky Automated Fraud Analytics

- Advanced machine learning makes sure all data and activity are monitored throughout the whole session

- Continuous detection and analysis of in-session events like bots, malware, remote administration tools, new unknown devices, web injects, and more

- Identification of new account fraud and account takeover incidents

- Global mapping, link building and device identification

Fraud Research and Analysis Team

Continue the conversation with our Analysts to learn how global threat intelligence and cutting-edge technologies combined will help you grow your business without security concerns and usability issues.

Technologies

BEHAVIORAL ANALYSIS
Building patterns of legitimate and fraudulent behavior

BEHAVIORAL BIOMETRICS
Building user profiles based on mouse, keyboard, and mobile phone usage

DEVICE ENVIRONMENT ANALYSIS
Analysis of session events happening around users and their devices

MALWARE DETECTION
Accurate detection of various kinds of malware in both web and mobile channels

Beat fraud and ensure seamless digital experience for your clients

True Machine Learning

Forensic Capabilities

Reduced Operational Costs

Automated Fraud Analytics

- Real-time detection and analysis of in-session events
- Identification of new account fraud, money laundering and account takeover incidents
- Global entity linking and mapping

Advanced Authentication

- RBA functionality
- Continuous authentication
- Reduced second factor costs

Order your demo by contacting us at **kfp@kaspersky.com**

Kaspersky Lab
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.com/fraudprevention

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence