Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x e-Commerce and Retail

It is time for retail and e-commerce sector to team up with a proven cybersecurity provider to be able to reach the happy medium between seamless user experience and high protection of data.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

Moving to the digital world means elevating cybersecurity for e-commerce and retail enterprises. It is essential to provide security for consumers during the entire session, including registration, login and transactions, but not limited to this.

Some facts and statistics

Given the rise of technologies, customers have high expectations regarding the service:

- Seamless access to the digital account
- High level of personal data protection
- Being able to access accounts from multiple devices anywhere anytime

In the past year, almost 7% of digital services users were subject to various kinds of identity fraud, while account takeover losses tripled and reached more than $5 billion globally.

Meanwhile fraudsters are constantly evolving in their methods and means. For example, fraudsters are now utilizing triangulation fraud, which is in effect a sophisticated three-step plan:

- Offer low priced products of high demand through a fake ecommerce store, where payments can only be made with credit cards. This enables fraudsters to collect data.

- Fraudsters are then able to purchase the requested product from the legitimate store and deliver it to the victim as would be expected.

- The fraudster is then able to use the stolen credit card data for their own purchases.

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

Breakdown of the solution

Advanced Authentication

Created for frictionless and continuous authentication, cutting the costs of two-factor authentication for legitimate users while ensuring high fraud detection rates in real-time.

Automated Fraud Analytics

Thoroughly analyzes events occurring during the whole session, transforming them into valuable pieces of data. Events and incidents allow accurate, timely decisions to be made and help uncover complex fraud cases.

Fraud Research and Analysis Team

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

Key Use Cases

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

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