Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x Loyalty Programs

Fraud is the unknown competitor that every business faces. Making sure that customer's benefits, bonuses and points are protected is key to expressing loyalty.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

In this day and age of digital transformation, loyalty programs are highly profitable for fraudsters.

Some facts and statistics

Kaspersky Fraud Prevention Team recently discovered over 3,000 fake accounts in the loyalty program of just one major retailer. These accounts were used to acquire welcome bonuses for newly registered users, and were then sold on the dark web at a reduced fee.

Statistics show that while a physical bank robbery may bring rewards estimated at $5,000 – 7,000, selling 100-150 gift cards, at $50 each, brings the same rewards but a much reduced risk of being caught.

Making sure that the organization will not suffer financial and reputational consequences requires strong yet seamless authentication and analysis of both identities and the sessional data. Striking the balance between the protection of customers from new account fraud and account takeover, while ensuring that the user experience is seamless and smooth remains a balance that is difficult to strike.

Organizations with loyalty programs face tough consequences when they encounter fraud:

- Restoring stolen points and loyalty program benefits to victims

- Recovering their brand reputation

- Keeping the consumer within the loyalty program

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

© AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence