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

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.

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

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 in protection. All this with flexible case management & forensic capabilities that significantly reduce the operational costs for enterprises.

Finding the perfect balance between seamless interaction and secure design is key to providing digital services at the highest level. Kaspersky Fraud Prevention strives to help providers achieve the golden standard of data and service protection.

Kaspersky Advanced Authentication

- Prioritizing legitimate users and detecting suspicious ones
- Risk Based Authentication continuously monitors numerous unique parameters
- Real-time analysis of biometrical, behavioral and environmental data
- Legitimate users proceed to their digital accounts without any unnecessary verification steps, which means reduced second factor costs for providers

Kaspersky Automated Fraud Analytics

- Advanced machine learning makes sure that 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

Kaspersky Fraud Prevention

Advanced Authentication

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

Automated Fraud Analytics

Thoroughly analyzes events happening during the whole session and transforms them into valuable pieces of data. Events and incidents provided allow to make accurate and timely decisions and uncover complicated fraud cases.

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.

Key use cases for loyalty programs

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 ANALYSYS
Building patterns of legitimate and fraudulent behavior

BEHAVIORAL BIOMETRICS
Building user profiles based on mouse, keyboard, and mobile phone usage
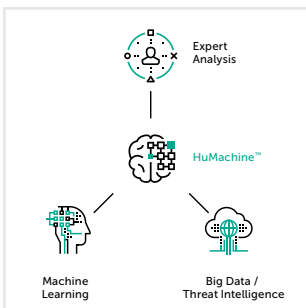
DEVICE ENVIRONMENT ANALYSIS
Analysis of session events happening around users and their devices

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

Order your demo by contacting us at <u>kfp@kaspersky.com</u>

Expert
Analysis

HuMachine™

Machine
Learning

Big Data /
Threat Intelligence

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine
www.kaspersky.com/fraudprevention