KASPERSKY lab

Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x Gambling

The online gambling sector attracts fraudsters like good odds attract bet-makers. This is where the money is. Literally. This industry has always been a desired target for criminals. Nothing has changed, so when platforms moved online, so did the fraudsters. The virtual space is the new battlefield and Kaspersky Fraud Prevention can be your ace up the sleeve.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

Statistics show that more and more users turn to their mobile devices when accessing digital gambling platforms. To protect sensitive information, such as billing and payment data, contact information and addresses, players may go through laborious authentication methods to access their accounts, including biometrics, devices or stringent password rules.

Some facts and statistics

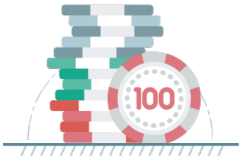
Attackers seek new ways to exploit the ever-growing market that is expected to soar to around $1 trillion by 2021.

Players expect:

- Easy and frictionless access
- Being able to play from multiple devices and different locations
- Protection of their personal Information

The data stored presents a great deal of value to fraudsters however, and they are constantly evolving in their methods and means of acquiring it. Account takeover and abuse of promotions are big targets for fraudsters due to the financial rewards on offer. Furthermore, money laundering is a looming concern, especially with the prevalence of cryptocurrency as payouts becoming an exploitable innovation.

Fraudsters perform their attacks from multiple devices and different locations, which makes such crimes incredibly difficult to fight.



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

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

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