kaspersky BRING ON THE FUTURE

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention for gambling and betting

The online gambling sector attracts fraudsters like good odds attract gamblers. This is where the money is. Literally. The industry has always been an attractive target for criminals. So when the platforms moved online, so did the fraudsters. The gambling industry is currently experiencing a period of exponential growth and fraudsters want to get in on the act. Cyberspace is the new battlefield and Kaspersky Fraud Prevention can be the ace up your sleeve.

Some facts and statistics

Massive data fraud and data theft have been named the fourth most important global risk of the next decade.[1]

Cybercriminals can make **$2.2 million per month** with just 10 stolen credit cards, which is why betting and gambling providers need to be more aware of cyberfraud.[2]

New era for gambling

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

The stored data is of great value to fraudsters however, and they are constantly evolving their methods and means of acquiring it. Account takeover and abuse of promotions are prime targets for fraudsters due to the financial rewards on offer.

Furthermore, money laundering is a looming concern, especially as cryptocurrency payouts become an exploitable innovation. Fraudsters perform their attacks from multiple devices and different locations, which makes tackling these crimes incredibly difficult.

For example, fraudsters may abuse bonus points and use collusion, as well as cryptocurrencies to redeem their "winnings". One of the most common fraudulent schemes in online gambling is collusion or, in other words, when multiple players work together to create a certain outcome. In such cases, they agree on the sum that each of them is going to get and abuse the system. Fraudsters frequently create networks of thousands of synthetic accounts, often using stolen personal data and credit card information to accumulate bonus points and redeem them. This particular type of fraud is extremely common in online poker and blackjack, where outcomes can be manipulated through game strategy, especially if it's been decided on beforehand. Rather than simply cheating other players, they will be playing a higher-stakes game to beat the online casino or betting platform.

Even before a user has started placing bets, the fraudsters may already be checking their bag of tricks to see which method better suits the situation at hand. This could be a basic identity theft scheme or the use of synthetic accounts to abuse promotional offers.

It's important not only to understand the threat but also to keep in my mind that, for online gambling providers, fraud prevention brings financial and reputation benefits.

What do players want?

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

[1] WEF Global Risks Report 2019 http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
[2] Symantec Internet Security Threat Report 2019 https://usa.ingrammicro.com/cms/media/Documents/vendors/s/symantec/istr_24_es.pdf

Preventing fraud in gambling and betting

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's 23 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.

Beat fraud and ensure seamless digital experience for your clients. **Kaspersky Fraud Prevention**

True machine learning

Forensic capabilities

Reduced operational costs

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Threat Intelligence Portal:
opentip.kaspersky.com

www.kaspersky.com

Kaspersky
Fraud
Prevention

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

More information at
https://kfp.kaspersky.com

@KasperskyFP