



Kaspersky<sup>®</sup>  
Fraud Prevention

# Kaspersky Fraud Prevention x Gaming

Fraudsters regard gaming industry as their own personal golden mine where stolen accounts and virtual treasures turn into pure profit for them. Identity theft and account takeover are big targets for fraudsters because of the financial rewards on offer.

[www.kaspersky.com/fraudprevention](http://www.kaspersky.com/fraudprevention)

#truecybersecurity

# Overview of the field

**Mobile gaming leads** the industry in **global revenues with 51%**, while PC and Console gaming are following with 24 and 25% respectively.

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**.

The gaming industry is flourishing with millions of players all over the globe. Online gaming is big business, revenues are at an all-time high and fraudsters want their piece of the pie.

Users are obsessed with their digital personalities and the growth of their characters, are emotionally attached to their digital alter ego, and are willing to spend big money on it. This phenomenon of modern age gaming allows for the creation of numerous market places where luxurious accounts, skins, virtual currencies and other in-game features are products in high demand.

Identity theft and account takeover are affecting the industry. In one case, a major global multiplayer game developer reported 35 cases of fraud in a very short-space of time, through web-injects, quickly losing thousands of pounds. Players followed web-links and filled-in their digital account information to receive in-game currency, and fraudsters simply harvested the gathered data to take over players' accounts.

## 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 gaming industry

### New Account Fraud

- Global entity linking and mapping
- 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

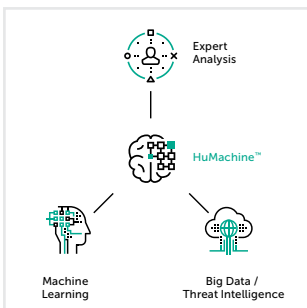
### DEVICE ENVIRONMENT ANALYSIS

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 [kfp@kaspersky.com](mailto:kfp@kaspersky.com)



Kaspersky Lab  
Enterprise Cybersecurity: [www.kaspersky.com/enterprise](http://www.kaspersky.com/enterprise)  
Cyber Threats News: [www.securelist.com](http://www.securelist.com)  
IT Security News: [business.kaspersky.com/](http://business.kaspersky.com/)

#truecybersecurity  
#HuMachine

[www.kaspersky.com/fraudprevention](http://www.kaspersky.com/fraudprevention)

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.