kaspersky BRING ON THE FUTURE

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention for gaming

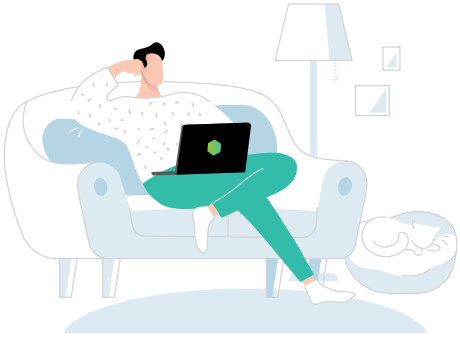
The fact that fraud in the gaming industry has proliferated in recent years clearly shows that cybercriminals also want to play in the booming online gaming industry. Fraudsters regard the gaming industry as their own personal gold mine, where stolen accounts and virtual treasures are turned into pure profit. Identity theft and account takeover are very popular with fraudsters because of the financial rewards on offer.

Some facts and statistics

The number of online gamers increases by **50 million** annually and is expected to reach 877.3 million in 2020.[2]

Analysts estimate that up to **77%** of mobile users are mobile phone gamers.[3]

A study has found that over **25%** of potential gaming customers refused to complete the account opening process due to lengthy and complex authentication.[4]



Big new market

There are currently more than 2 billion gamers worldwide and almost 50% of them make in-game transactions.[1] The fact that fraud in the gaming industry has surged in the recent years shows that cybercriminals want their share of the expanding online gaming field.

Users are obsessed with their digital personalities and the growth of their characters, are emotionally attached to their digital alter egos, and are willing to spend big money on them. This phenomenon of modern-age gaming has spawned numerous marketplaces where luxurious accounts, skins, virtual currencies and other in-game features are in high demand.

In game currency has value for fraudsters

Identity theft and account takeover are affecting the industry. Players can become victims of social engineering, happily giving away their data, expecting to receive bonuses and in-game items for free or very little cost. Tempted by an offer of in-game currency, players follow web links and enter their digital account information, which is then harvested and used by fraudsters to take over the players' accounts.

Identity verification is also crucial to the gaming industry given that certain in-game content may be age restricted or if automated credit card payments are used and need to be protected from unauthorized purchases or manipulations. Therefore, fool-proof user authentication is also extremely useful in these instances, as well as the ability to recognize whether the user behind the screen is a legitimate player or a cheater.

Cases of account takeover, for instance, have flooded industry platforms, with groups of hackers stealing and then putting up for sale thousands of real user accounts. With streaming services, the popularity of some users can be enormous, and the consequences of their accounts being stolen can be devastating for game developers. As well as suffering severe reputational damage, they are likely to lose lots of fans if their more popular users end up shunning the platform.

1 Statista Number of active video gamers worldwide from 2014 to 2021
https://www.statista.com/statistics/748044/number-video-gamers-world/
2 League of Betting Number of Online Gamers to Hit 1 Billion by 2024
https://leagueofbetting.com/number-of-online-gamers-to-hit-1-billion-by-2024/
3 IAB Digital Trends 2016: Consumer Usage, Ad Revenue and Impact
https://www.wepc.com/news/video-game-statistics/#mobile-gaming
4 Jumio Online Gaming Report 2018
https://www.jumio.com/about/press-releases/online-gambling-report/

Preventing fraud in gaming

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