kaspersky BRING ON THE FUTURE

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention for e-commerce and retail

With the modern consumer used to having everything at their fingertips, there's now more need than ever for services to ensure seamless protection from online fraud. Investing in marketing campaigns to boost new purchases and reward customer loyalty is great for building revenue, but when a company fails to understand why the revenue numbers don't add up, cyberfraud could well be at the heart of the problem.

Some facts and statistics

In 2019, the FTC registered **1.4 million** reports on fraud in e-commerce, **25%** of which involved financial losses totaling **$1.48 billion**.[1]

Almost half **(43%)** of fraud cases detected by Kaspersky Fraud Prevention in Q3 and Q4 of 2019 were related to malicious bot activity.

Overview of the field

Large data leaks of user credentials and personally identifiable information create a convenient pathway for accessing user accounts, stealing bonus points and making purchases with stolen credit cards, creating a fraud-friendly environment for cybercriminals. Fraudsters are always looking for easy ways to make a profit, many of them attracted by the seeming lack of retribution for this type of crime, plus the ready availability of automation tools, device fingerprints and user data on the dark web and other digital black markets.

What are the main areas of concern for e-commerce and retail providers?

Account takeover (ATO) and bots. Account takeover implies gaining unauthorized access to one or several accounts in order to steal bonuses or user data, purchase items with stolen card information and perform card-not-present fraud. In many cases, fraudsters gain unauthorized access to an account through stolen or bought usernames and passwords. An ATO attack can be carried out both manually and automatically, for example, by using bots that skim social media, banking accounts, emails and e-commerce accounts in order to validate the data. The fact that consumers tend to use the same passwords for numerous online services makes the task much easier.

After performing credential stuffing or brute-force attacks and gaining access to the account, cybercriminals make fraudulent transactions from the compromised accounts. Fraudsters can then launch automated attacks on website login pages, steal bonus points accumulated by real users and empty out your stock. In Q3 and Q4 of 2019, almost half of fraudulent incidents (43%) detected by Kaspersky Fraud Prevention were connected to suspicious bot activity.

New account fraud. Oftentimes, in order to abuse the loyalty schemes offered by businesses, fraudsters set up networks of thousands of fake accounts using stolen and bought credentials. One of the aims of new account fraud can be reaping reward points, money or miles that you've invested in for loyal customers. Criminals figure out the algorithm used to create rewards and then create new accounts hitting all the right points. Fraud actors cash incospicuous amounts from each account and use unclaimed rewards. Promotions for marketing campaigns can also become a highly attractive target for cybercriminals, with considerable spending on promotions that offer a cash sign-up bonus. Fraudsters find loopholes in the promo scheme and make use of cashable goods, creating a healthy profit for themselves. More than half (57%) of cyberattacks on e-commerce vendors in Q3 and Q4 of 2019 were attempts to commit new account fraud, according to Kaspersky Fraud Prevention data.

1 FTC's 2019 Report – Consumer Sentinel Network Data Book https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Preventing fraud in e-commerce and retail

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