Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x Telecom

While telecom enterprises provide millions of users with internet, mobile and satellite services, Kaspersky Lab has the technology and know-how to provide them with industry-leading fraud prevention and data protection.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

Our age is synonymous with digital infrastructure, and the telecom industry leads the way in ensuring that consumers receive mobile, data and satellite communications. Now that data is so valuable, it is no wonder that fraudsters are continually coming up with new ways of acquiring it.

Some facts and statistics

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.

During the last five years, telecom providers witnessed around 50 million user's records being stolen.

According to analysis by FICO, 81% of telecom companies say they expect that cyberattacks will increase in the coming year – the highest of any industry surveyed.

The amount of personal information that telecom providers possess is overwhelming: from contacts and addresses to payments and customer banking credentials.

The main attraction of the telecom industry is the resource at the heart of its operations : data – the most precious asset for criminals. It can be easily stolen, altered and modified, multiplied endlessly, used for blackmailing, and the list goes on and on. An argument can be made that data in the modern era of digital transformation is the new money and fraudsters want it.

The telecommunications industry cannot afford to ignore the tools and opportunities that going digital present. Telecom providers need to team up with a proven cybersecurity provider in order to defend themselves from fraudsters and ensure their customer experience is smooth, all while being up to date, and beyond.

Major fraud issues that the telecom industry faces include:

• Verifying identities – identifying users and increasing conversion rates.

• Detecting stolen identities that are used for defaulting on premium handset contracts.

• Detecting fraudulent behavior, such as subscription fraud.

• Visual terrorism is also a looming threat: criminals are learning to interfere with AR/VR technology to manipulate user behavior.
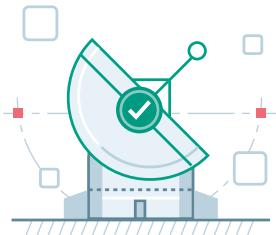
Preventing Account Takeover

• 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

Preventing New Account Fraud

• Immediate recognition of synthetic accounts

• Detection of new unknown devices

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

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.

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

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence