kaspersky BRING ON THE FUTURE

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention for telecom

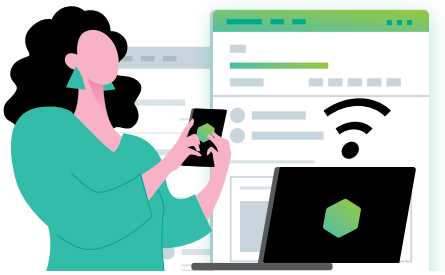
Deeply ingrained in the operation of businesses and the evolution of modern society, the telecom industry has become an integral part of digital transformation. Considering how essential telecommunications are to everyday activities of the modern world, it's imperative for providers to ensure the utmost reliability and security of telecom networks. While telecom enterprises provide millions of users with internet, mobile and satellite services, Kaspersky has the technology and know-how to provide them with industry-leading fraud prevention and data protection.

Some facts and statistics

In the second half of 2019, telecommunications experienced a **295%** increase in the frequency cyberattacks.[1]

According to CFCA, the annual cost of telecom subscription fraud reaches over **$12 billion**.[2]

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



Telecommunications and cyberfraud

Websites and mobile applications offering customer self-management are secured through the customer side, meaning any personally identifiable information found online or on the Dark Web can be used to manipulate the account. Through hijacking the account, the fraudster is granted access to SIM-card bills, as well as debt, which can be used as a pathway for access to money. As well as that, access to the user's SIM-card management account can help redirect authentication SMS and data traffic, meaning that a fraudster may gain access to a customer's banking account through stealing the authentication code and proceeding to launder money and commit more fraud. That way, SIM card fraud can also become a pathway for credit card fraud.

The amount of personal information that telecom providers possess is overwhelming: from contacts and addresses to payment details and 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. It could be said that data in the modern era of digital transformation is the new money and fraudsters want to get their hands on it. More often than not, fraudsters aim for the weakest security link between the telecom provider and the app – the end customer.

Using a tactic known as social engineering, fraudsters may call customers and introduce themselves as a representative from a telecom company's security department. By manipulating the customer into providing their data the fraudsters can gain access to user accounts. A stolen account can be resold or used to make free calls for further fraud. User-based fraud can be just as simple as using a lost or stolen mobile device or SIM card. However, with the right user behavior analysis tools, telecom companies can prevent cyberattacks in real time.

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 keeping up to date with the latest technology.

1 Netscout Threat Intelligence Report H2 2019
https://www.netscout.com/threatreport

2 The Paypers
https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807

Preventing fraud in telecom

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