Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

x Healthcare

Healthcare organizations continue to digitally transform their interactions with patients. Kaspersky Fraud Prevention strives to help companies achieve that perfect balance between protecting personal data and meeting customer expectations.

www.kaspersky.com/fraudprevention

#truecybersecurity

Overview of the field

Going digital for healthcare organizations means being able to focus on patients without all the cumbersome paperwork. However, technological progress is a two-way street where along with numerous benefits there is a greater chance of valuable data being stolen. Let's break down some looming cybersecurity concerns for medical organizations.

Some facts and statistics

In 2017 healthcare faced around 32,000 cyberattacks per day, twice as many as other industries.

Medical records are worth much more than stolen credit card details.

Bundles of stolen medical data from up to 140-million patients are currently for sale online.

Global healthcare cyber-security security spending is increasing by 4.1% annually and is set to exceed $56-billion cumulatively to 2021.

The global market for mobile healthcare applications is valued at $28.32-billion – and is expected to reach $102.35-billion by 2023.

While financial data can lose its value after passwords are changed or credit cards are blocked, the value of healthcare data does not change. Digital accounts now contain electronic medical records, health insurance ID, contact information, Social Security numbers (US), billing and payment information.

The opportunities that illegally obtained medical data presents to fraudsters are endless: taking advantage of insurance policies, receiving medical services illegally, selling information, purchasing subscription drugs, etc.

IT security is not a top priority for healthcare providers – their primary concern is to save lives, with all other matters considered secondary. Nevertheless, given the increasing use of mobile technology by doctors and other medical staff to access patient data, it is now crucial to protect it from increasingly sophisticated cybercriminals.

Patients who use mobile medical applications face the same dangers. Both parties need protection in this rapidly evolving field.

There are continual reports of incidents involving compromised medical data and they show no sign of abating. Around 1.13 million patient records were compromised in 110 healthcare data breaches in the first quarter of 2018 in the US alone. In July 2018 in Singapore, hackers breached the government's health database, accessing the data of approximately 1.5 million patients (including that of the Prime Minister) for almost a week. And in the UK, the National Health Service's NHS Digital suffered a data breach in which the confidential data of 150,000 patients was shared without their permission.

Healthcare providers are under massive pressure to prevent breaches, protect patients from doctored information, and to secure connected devices. Given the significance of the data and devices, prevention is crucial. At the same time, security cannot be at the expense of usability.

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

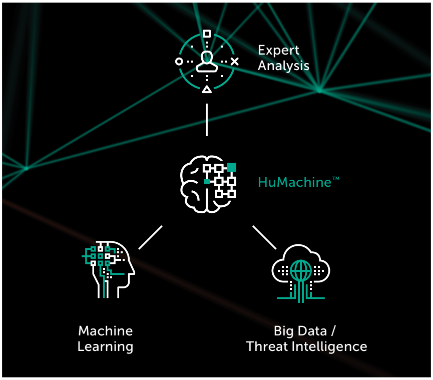
- RBA functionality
- Continuous authentication
- Reduced second factor costs

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