kaspersky BRING ON THE FUTURE

Kaspersky Fraud Prevention

Kaspersky Fraud Prevention for e-Government

The amount of citizens' information stored in e-government services is overwhelming. Furthermore, certain applications also manage highly personal information, such as ID cards, healthcare security numbers, passports or driver licenses. Given that citizens tend to view government as a single entity, any damage caused by fraud on e-government channels will be projected onto the image of the state body itself. This is a perfect example of where prevention is better than cure.

Some facts and statistics

Over half of all government and public sector organizations increased their spending on cybersecurity in 2019, with **66%** planning on spending more in 2020.[1]

In 2018, the accounts of over **1.1 billion** citizens in India were exposed in one of the biggest government data breaches, with the data later being sold online for just **US$7.30**.[2]

While striving for more efficient, productive and effective interaction with citizens, governments also open the door to fraudsters, inviting them to take advantage of vulnerabilities in e-government digital channels.

Interactions with public authorities include:
Transactions (taxes, pension, tickets, payments)
Registration procedures (applying to kindergarten, schools, benefits)
Informational services

How costly is the leakage of citizens' data?

In an effort to profit through deception, fraudsters are turning their attention to the public sector, which has become vulnerable as a result of interacting with citizens via digital channels. The specifics of this field imply certain economical, legal and reputational repercussions for government bodies. In particular, e-government fraud can lead to reduced efficiency, an outflow of data and resources from their rightful owners and a loss of trust and confidence in government institutions.

Fraud-related issues in the field of e-government pose a particular threat because citizens tend to view government bodies as a single entity and do not differentiate between online services and the state. So any reputational damage to the e-service will harm the image of the government itself.

Approaching the issue of fraud and G2C services

In government-to-citizen interactions, the state has to display integrity and competence when handling citizens' personal identifiable data. At the same time, the user experience shouldn't be too onerous or people won't engage. Finding the right balance between data security and a service that's easy to use is one of the key challenges facing state bodies.

Implementation of anti-fraud prevention systems is mandatory, so that when the inevitable attacks are launched they will be blocked. In order to do this, a government has to implement two major defense techniques:

1. Thorough investigation and analysis of detected fraud cases.
2. Detection technologies that quickly identify events and incidents that signal fraudulent activities.

Successful fraud prevention in the e-government sector means immediate detection of fraudulent activities based on prediction models and the utilization of data mining methods, which are necessary for uncovering new types of fraud.

Collecting large datasets of citizens' non-personal behavioral patterns makes it possible to detect suspicious behavior in an e-government digital channel before any real financial or reputational damage is inflicted.

[1] EY Global Information Security Survey 2018-19 https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019

[2] WEF Global Risks Report 2019 http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Preventing fraud in e-Government

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