kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention для государственных услуг онлайн

Государственные электронные службы хранят огромное количество информации о гражданах. Более того, некоторые приложения также работают с конфиденциальными данными, такими как данные паспорта, водительских прав. Поскольку многие воспринимают различные государственные службы как единое целое, любой ущерб от мошенничества, связанного с электронными госуслугами, негативно влияет на имидж всего государственного аппарата. Это как раз тот случай, когда лучше предотвратить атаку, нежели чем разбираться с её последствиями.

Факты и статистика

Более половины государственных и общественных организаций увеличили свои расходы на кибербезопасность в 2019 году, при этом **66%** планируют повторить это и в 2020 году.[1]

В 2018 г. через одну из самых крупных брешей в государственной базе данных произошла утечка учётных записей более **1,1 млрд** граждан Индии. Затем эти данные продавались в Сети по цене всего **US$7,32**.[2]

Многие пользователи сервисов электронных госуслуг активно используют для этой цели свои смартфоны и компьютеры. При этом пользователи ожидают от сервиса полной защиты своих данных и удобства взаимодействия с сервисом, который позволяет избежать бюрократии.

Взаимодействие с государственными сервисами включает в себя:
Транзакции (налоги, пенсии, штрафы и оплату за услуги)
Регистрационные процедуры (подача документов в школы, детские сады, получение паспорта, пособий)
Предоставление информации

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

Во что могут вылиться утечки данных граждан?

В поисках очередной наживы мошенники обратили внимание на государственный сектор, который стал уязвим вследствие того, что для взаимодействия с гражданами начали использоваться цифровые каналы. Злоумышленники могут нанести государственным организациям финансовый, правовой и репутационный ущерб. Так, следствием мошеннических действий может стать снижение эффективности работы государственных служб, утечка данных и ресурсов граждан и, следовательно, потеря доверия граждан к госаппарату.

Борьба с мошенничеством в сфере электронных госуслуг

При обращении с личными данными граждан государство должно демонстрировать открытость и компетентность. В то же время взаимодействие с государственными электронными сервисами не должно быть для пользователя в тягость, иначе эти сервисы не будут востребованы у населения. Достичь баланса между безопасностью данных и удобством пользования –одна из основных задач государственного сектора.

Строго необходимо внедрение систем предотвращения мошенничества, поскольку злоумышленники непременно будут пытаться атаковать госучреждения. Чтобы противостоять угрозам, государству следует действовать в двух направлениях. Во-первых, тщательнее расследовать и анализировать выявленные случаи мошенничества, а во-вторых, внедрять технологии обнаружения, чтобы быстро фиксировать события и инциденты, свидетельствующие о мошенничестве.

Успешно предотвращать мошенничество в сфере электронных госуслуг можно, только моментально обнаруживая преступную активность на основе предиктивных моделей и используя передовые методы сбора данных для выявления новых мошеннических схем.

С опорой на обширную базу поведенческих шаблонов граждан можно выявлять подозрительное поведение в электронных службах, предотвращая реальный финансовый и репутационный ущерб.

Предотвращение мошенничества в сервисах государственных услуг онлайн

Мошеннические учётные записи
Обнаружение аккаунтов, использующихся для злоупотребления возможностями сервиса
Распознавание новых устройств или тех, которые используются для различных учётных записей
Кража учётной записи
Выявление кражи учётной записи, как на этапе логина, так и на протяжении всей сессии
Обнаружение подозрительной активности в режиме реального времени
Возможность предотвращения потенциальных потерь

Kaspersky Fraud Prevention

Благодаря обширному экспертному опыту «Лаборатории Касперского» в сфере кибербезопасности и высочайшему качеству предоставляемой защиты Kaspersky Fraud Prevention помогает поставщикам цифровых услуг добиться оптимального баланса между уровнем безопасности и удобством для клиентов. Гибкое управление инцидентами и возможности цифровой криминалистики позволяют значительно снизить операционные расходы крупных компаний.

Kaspersky Advanced Authentication

- Приоритизация легитимных пользователей
- Аутентификация на основе рисков
- Анализ биометрии, поведения и данных окружения в режиме реального времени
- Легитимные пользователи получают доступ к своим аккаунтам без дополнительной верификации, что позволяет сократить расходы на второй фактор аутентификации

Kaspersky Automated Fraud Analytics

- Мониторинг всех данных и активности во время сессии с использованием передовых технологий машинного обучения
- Выявление мошеннических учётных записей, отмывания денег и кражи учётных записей пользователей
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Команда исследования и анализа мошеннических инцидентов

Обширный экспертный опыт аналитиков «Лаборатории Касперского», передовые технологии и глобальная база знаний об угрозах помогут вам развивать свой бизнес, не беспокоясь о проблемах с безопасностью и удобством использования ваших сервисов.

Защита от мошенничества для вас – быстрый и удобный сервис для ваших клиентов. Kaspersky Fraud Prevention

Реальное машинное обучение

Экспертиза и расследование мошенничества

Сокращение операционных расходов

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.ru

Kaspersky Fraud Prevention

Чтобы заказать демо-версию, отправьте заявку на kfp@kaspersky.com

Подробнее на www.kfp.kaspersky.com/ru/

@KasperskyFP