Решения для бизнеса

KASPERSKY lab

Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

для финансового сектора

Финансовые организации служат основной мишенью для мошеннических атак, которые причиняют им значительный ущерб. Учитывая стремительное развитие технологий, какие действия по защите от мошенничества необходимо предпринять на уровне отрасли? Ответ прост: нужно не реагировать на атаки, а предотвращать их.

www.kaspersky.ru/enterprise-security/fraud-prevention

#truecybersecurity

Взгляд на индустрию

Среди всех вертикалей финансовая отрасль несет наибольший ущерб от действий онлайн-мошенников, которые постоянно совершенствуют свои инструменты и методы атак. Кража личных данных и учетных записей клиентов позволяет им создавать фальшивые учетные записи и подавать заявки на кредиты, что приводит к серьезным финансовым потерям для организаций. Мошенники используют учетные записи для совершения покупок в кредит, использования «денежных мулов» и даже для отмывания денег.

Факты и статистика

По данным опросов, более 70% крупных компаний ищут защитные решения, которые оказывают минимальное влияние на взаимодействие пользователей с сервисом.

Объем транзакций, связанных с отмыванием денег, оценивается в 2-5% глобального ВВП, что примерно соответствует $1-2 трлн в год.

Согласно статистике Experian, данные логин и пароль для платежных систем могут продаваться в Dark Web за $20 и дороже.

Что нужно киберпреступникам?

- Финансовая выгода от нелегетимных транзакций
- Кража информации (для рыночных манипуляций и получения инсайдерской информации)
- Нарушение работы сервисов
- Подрыв репутации конкурентов

Что ожидают пользователи от сервиса?

- Четкой и удобной работы с учетной записью без затруднений и задержек
- Надежной защиты своих личных данных
- Быстрого доступа к учетной записи онлайн банкинга в любое время с различных устройств

Несмотря на широкое распространение случаев мошенничества, использование онлайн-банкинга остается второй по частоте (88%) активностью на устройствах пользователей. Для финансовых организаций это означает дополнительную ответственность.

Чтобы защитить себя и своих клиентов от нелегальных транзакций, предприятия финансовой отрасли широко применяют практику «знай своего клиента», основанную на электронной верификации пользователей. Это делает финансовые организации уязвимыми для таких угроз кибербезопасности, как отмывание денег, создание мошеннических учетных записей и кража учетных записей клиентов.

В рамках системы Open Banking финансовые учреждения могут использовать открытые API, дающие возможность сторонним приложениям и сервисам работать с их системами. Экосистема FinTech переполнена, и развитие Open Banking значительно усложняет обеспечение безопасности всех взаимодействий. Сложность и разнообразие способов доступа к цифровым учетным записям создают новые уязвимые точки, которые могут эксплуатировать мошенники. С этой точки зрения для финансовых учреждений технологии – обоюдоострый меч: использовать их необходимо, но это подвергает организации дополнительному риску кибератак.

Как сообщили 1 из 6 опрошенных организаций в Азиатско-Тихоокеанском регионе, их предприятия откладывают цифровую трансформацию из-за опасений, связанных с кибер-рисками. Это сдерживает развитие рынка и мешает таким организациям в полной мере использовать безграничные возможности, которые дает цифровая трансформация. Сотрудничество с проверенным поставщиком услуг кибербезопасности – вот что необходимо каждой компании, стремящейся обеспечить бесперебойное цифровое обслуживание клиентов и надежную защиту их данных.

Предотвращение мошенничества в финансовом секторе

Мошеннические учетные записи

- Обнаружение аккаунтов, использующихся для злоупотребления возможностями сервиса
- Распознавание новых устройств или тех, которые используются для различных учетных записей

Отмывание денег

- Анализ уникального идентификатора устройства
- Кросс-канальное обнаружение случаев отмывания
- Построение и сопоставление связей между аккаунтами организациями

Кража учетной записи

- Выявление кражи учетной 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 учетных записей, отмывания денег и кражи учетных записей пользователей
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Группа 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

Реальное машинное обучение

Экспертиза и расследование мошенничества

Снижение операционных издержек

Automated Fraud Analytics

- Мониторинг всех данных и активности во время пользовательской сессии
- Выявление мошеннических учетных записей, кражи аккаунтов пользователей и случаев отмывания денежных средств
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Advanced Authentication

- Аутентификация на основе рисков (RBA)
- Непрерывный анализ биометрических, поведенческих показателей и данных окружения в режиме реального времени
- Сокращение расходов на второй фактор аутентификации

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

Kaspersky Lab
Enterprise Cybersecurity:
www.kaspersky.com/enterprise
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com**

#ИстиннаяБезопасность
#HuMachine

www.kaspersky.com/fraudprevention
www.kaspersky.ru/enterprise-security/fraud-prevention