



Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention для электронной коммерции и ритейла

Современные потребители привыкли принимать удобство и доступность электронных сервисов как нечто само собой разумеющееся, и задача эффективной защиты этих сервисов от онлайн-мошенничества стоит остро как никогда. Отличными инструментами для увеличения дохода являются инвестиции в маркетинговые кампании, стимулирующие новые покупки и поощряющие лояльность потребителей, однако если эти инвестиции не оправдывают себя, причина, вероятнее всего, кроется в действиях кибермошенников.

Факты и статистика

В 2019 году FTC зарегистрировали **1,4 миллиона** сообщений о мошенничестве в электронной торговле, **25%** из которых были связаны с потерей денег. В общей сложности сумма убытков составила **\$1,48 млрд.**¹

В III и IV кварталах 2019 года почти половина случаев мошенничества (**43%**), обнаруженных Kaspersky Fraud Prevention, были связаны с мошеннической активностью ботов.



Взгляд на индустрию

Частые утечки данных пользователей и информации, позволяющей установить личность, создают основу для мошенничества, открывают возможность доступа к учётным записям пользователей, кражи бонусных баллов и покупок, совершаемых с использованием украденных кредитных карт. Мошенники всегда ищут простые способы получения прибыли, многих из них привлекает кажущееся отсутствие наказания за этот вид преступления и доступность инструментов автоматизации, а также кражи пользовательских данных, которые доступны на Dark Web и других черных рынках в интернете.

С чем сталкиваются платформы электронной коммерции и ритейлеры?

Кража аккаунта (АТО) и боты. Кража учётной записи подразумевает получение несанкционированного доступа к одной или нескольким учётным записям для кражи бонусов или пользовательских данных. Во многих случаях мошенники получают нелегитимный доступ к учётной записи через украденные или купленные логины пользователей и пароли. Атака АТО может быть проведена как вручную, так и автоматически, с использованием ботов, которые просматривают социальные сети, банковские учётные записи, электронную почту и учётные записи в интернет-магазинах для проверки данных. А поскольку потребители обычно используют одни и те же пароли для многочисленных онлайн-сервисов, задача становится намного проще.

Мошеннические учётные записи. Нередко для эксплуатации в своих целях схем лояльности онлайн-магазинов, мошенники создают сети из тысяч поддельных учётных записей. Одним из случаев использования мошенничества с новыми учётными записями может быть получение бонусных баллов или миль, в которые были вложены деньги для постоянных клиентов. Преступники исследуют алгоритм, используемый для поощрения клиента, а затем создают новые учётные записи, с точностью настраивая свою атаку. Раскрутка маркетинговых кампаний также может стать весьма прибыльной целью для киберпреступников, при этом значительные расходы идут на бесплатные рекламные акции, такие как «получи бонус в 1000 рублей на наши услуги при регистрации». Мошенники находят лазейки в схеме продвижения и перепродают эти товары, создавая высокодоходную маржу для себя. По данным Kaspersky Fraud Prevention, более половины (57%) кибератак, совершенных на вендоров электронной коммерции в III и IV кварталах 2019 года, были попытками использовать новые мошеннические учётные записи.

¹ FTC's 2019 Report – Consumer Sentinel Network Data Book https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Предотвращение мошенничества в электронной коммерции и ритейле

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

© АО «Лаборатория Касперского», 2020. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.



Kaspersky
Fraud
Prevention

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

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

@KasperskyFP