kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention и телекоммуникации

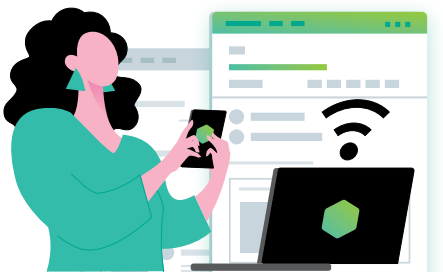
Управление бизнесом, как и вообще развитие современного общества, немыслимо без телекоммуникаций, они стали неотъемлемой частью цифровых преобразований. Учитывая, насколько телекоммуникации значимы практически для любой повседневной деятельности современного человека, крайне важно обеспечить безопасную и бесперебойную работу таких сетей. Телекоммуникационные компании предоставляют миллионам пользователей доступ к интернету, мобильной и спутниковой связи; «Лаборатория Касперского» со своей стороны предлагает таким компаниям передовые технологии защиты данных и предотвращения мошенничества.

Факты и статистика

Во второй половине 2019 г. частота кибератак в сфере телекоммуникаций выросла на **295%**.[1]

Согласно данным CFCA, ущерб от мошенничества с подписками на телекоммуникационные услуги составляет более **12 млрд долларов** в год.[2]

Телеком-провайдеры вынуждены решать следующие вопросы:
Проверка личных данных – идентификация пользователей и повышение коэффициента конверсии
Обнаружение мошеннического поведения, в том числе операций с подпиской



Телекоммуникации и кибермошенничество

Провайдеры телекоммуникационных услуг владеют невероятным количеством персональных данных: от контактной информации и адресов абонентов до банковских данных и деталей платежей. Самой большой ценностью в телекоммуникационных сервисах являются данные, с которыми они работают, – они же являются лакомым куском и для киберпреступников. Данные легко похитить, изменить, размножить, сделав сколь угодно много копий, использовать в целях шантажа и т. д. Можно с уверенностью заявить, что в эпоху цифровых преобразований информация стала валютой, и мошенники всеми силами стремятся завладеть ею. Чаще всего они направляют атаки на самое слабое звено в цепочке между провайдером телекоммуникационных услуг и приложением – на конечного пользователя.

Телекоммуникационная отрасль не может игнорировать новые инструменты и широкие возможности, которые предоставляет цифровая трансформация. Телеком-провайдеры должны объединиться с надёжным поставщиком услуг кибербезопасности, чтобы защитить себя от мошенников, обеспечить бесперебойное взаимодействие с клиентами и при этом идти в ногу со временем и даже опережать его.

Злоумышленники активно используют приёмы социальной инженерии. Так, они могут звонить клиентам и представляться сотрудниками отдела безопасности провайдера. Умело прибегая к обману, мошенники могут получить от клиента его личные данные, а с ними и доступ к учётной записи. Похищенный аккаунт можно перепродать или использовать для бесплатных звонков в преступных целях. Мошенничество путем обмана пользователей ничуть не сложнее, чем использование похищенного мобильного устройства или SIM-карты. Однако с помощью эффективных инструментов поведенческого анализа телекоммуникационные компании могут предотвращать кибератаки в режиме реального времени.

Телекоммуникационная отрасль не должна игнорировать новые технологии и возможности, которые открывают цифровые преобразования. Провайдерам телекоммуникационных услуг необходимо сотрудничать с поставщиками проверенных решений кибербезопасности, чтобы защитить себя от мошенничества и обеспечить своим клиентам стабильное и высокотехнологичное обслуживание.

1 Netscout Threat Intelligence Report H2 2019
https://www.netscout.com/threatreport

2 The Paypers
https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807

Предотвращение мошенничества в телекоммуникациях

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