



Kaspersky Fraud Prevention и игровая индустрия

Благодаря миллионам игроков по всему миру, игровая индустрия неуклонно набирает обороты. Сегодня онлайн-игры – это крупный бизнес с огромными доходами. Неудивительно, что мошенники проявляют к нему повышенный интерес. Для мошенников игровая индустрия – это золотая жила, ведь украденные учётные записи и виртуальные ценности оборачиваются чистой прибылью. Кража персональных данных и перехват аккаунтов особенно выгодны и поэтому очень распространены.

Факты и статистика

Количество онлайн-игроков ежегодно увеличивается на **50 млн**; ожидается, что в 2020 г. оно достигнет **877,3 млн**.²

Исследования показывают, что около **77%** пользователей мобильных устройств играют в мобильные игры.³

Исследование показало, что более **25%** потенциальных геймеров не доводят до конца процесс создания учётной записи из-за длительной и сложной процедуры аутентификации.⁴

Новый большой рынок

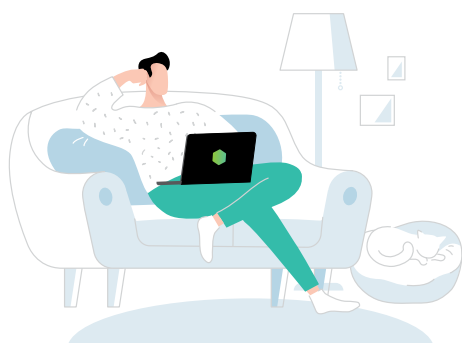
Сейчас в мире насчитывается более 2 млрд геймеров, и почти 50% из них совершают внутриигровые транзакции.¹ Естественно, киберпреступники хотят урвать свою долю с этого развивающегося рынка, поэтому их активность в последние годы выросла. Тот факт, что активность мошенников последние годы увеличилась, говорит о том, что они хотят заполучить свою долю этого развивающегося рынка.

Для игровой индустрии кража личных данных и учётных записей пользователей представляет серьёзную проблему. Так, в одном случае крупный глобальный разработчик игр сообщил о 35 случаях мошенничества с использованием веб-инъектов за короткий период времени. Игроки переходили по предлагаемым ссылкам и вводили данные своих учётных записей, чтобы получить игровую валюту. Мошенники затем использовали собранные данные для кражи аккаунтов, что привело к финансовому ущербу, исчисляемому тысячами фунтов.

Мошенникам нужна внутриигровая валюта

Внутриигровая валюта представляет ценность для преступников. Кража персональных данных и перехват учётных записей – все это затронуло и игровую индустрию. Геймеры нередко попадают на приёмы социальной инженерии и с готовностью предоставляют свои личные данные в надежде получить бонусы и внутриигровые предметы бесплатно или по очень низкой цене. Соблазняясь предложениями получить игровую валюту, игроки переходят по мошенническим ссылкам и вводят свои учётные данные. Затем злоумышленники их собирают и используют для перехвата аккаунтов.

Случаи перехвата учётных записей на игровых платформах бесчисленны. Группы киберпреступников крадут тысячи аккаунтов реальных пользователей и выставляют их на продажу. Благодаря стримингу некоторые геймеры обретают невероятную популярность в игровом сообществе, и кража их учётных записей может иметь катастрофические последствия для разработчиков игр. Из-за репутационного ущерба последние рискуют потерять многих своих фанатов, если популярные игроки перестанут доверять их платформе.



1 Statista Number of active video gamers worldwide from 2014 to 2021
<https://www.statista.com/statistics/748044/number-video-gamers-world/>

2 League of Betting Number of Online Gamers to Hit 1 Billion by 2024
<https://leagueofbetting.com/number-of-online-gamers-to-hit-1-billion-by-2024/>

3 IAB Digital Trends 2016: Consumer Usage, Ad Revenue and Impact
<https://www.wepc.com/news/video-game-statistics/#mobile-gaming>

4 Jumio Online Gaming Report 2018
<https://www.jumio.com/about/press-releases/online-gambling-report/>

Предотвращение мошенничества в игровой индустрии

Мошеннические учётные записи

Обнаружение аккаунтов, используемых 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