Что такое скликивание контекстной рекламы и как его предотвратить. Полное руководство.

Ноябрь 2023 года. Редакция 2. Полная версия.

Подготовлено специалистами компании *https://clickfraud.ru/* — защита от скликивания рекламы.

В этой электронной книге вы узнаете, что именно понимается под «мошенническими кликами», как обнаружить скликивание самых распространенных типов и как определить, в каких отраслях и под-отраслях есть риск столкнуться со скликиванием. Кроме того, мы рассмотрим нормальные клики, влияющие на окупаемость затрат на рекламу, хотя это не основная тема данного руководства. Мы разберем причины, по которым со скликиванием трудно бороться, и расскажем о том, как оно влияет на индустрию цифровой рекламы. Мы покажем вам, что любая компания может сделать для защиты своих рекламных кампаний от мошеннических кликов даже без использования стороннего программного решения этой проблемы.

Наконец, мы обсудим, как найти правильный баланс между защитой своей рекламной учетной записи и запретом показа рекламы потенциальным покупателям.

Содержание книги

Проблема, из-за которой индустрия цифровой рекламы ежегодно теряет миллиарды долларов

Если вы подозреваете, что вашу рекламу скликивают, то вы не одиноки. Хотя поначалу большинство интернет-рекламодателей думают, что скликивание не повлияет на их рекламные кампании, в конечном итоге они замечают неточные данные по кликам в своих отчетах и начинают изучать эту обширную и сложную тему.

Даже если вы не следили за тем, как с 2004 года скликивание начало становиться всё более распространенным явлением, вы могли узнать о таких мошенниках из новостей, где о них часто рассказывали, например из этой статьи Forbes 2016 года о российской группе мошенников, которые управляли фермой ботов и получали пять миллионов долларов в день. И это только верхушка айсберга: по прогнозу Statista 2019 года общемировые потери, связанные с мошенничеством в области интернет-рекламы, «экспоненциально росли и предположительно будут расти с 2018 по 2022 год — с 19 миллиардов до 44 миллиардов долларов США».

И что самое неприятное — скликивание процветает в среде, которая должна давать маркетологам доступ к как никогда точным данным. При помощи кампаний интернет-рекламы удивительно легко охватывать аудиторию пользователей Интернета. Их довольно легко разрабатывать, они относительно дешевы и дают почти мгновенную обратную связь. Более того, они позволяют:

- Интегрировать программные решения, которые помогают отслеживать, редактировать и монетизировать кампании.
- Использовать различные форматы рекламы, начиная от текстов и баннеров и заканчивая нативной рекламой.
- Использовать разнообразные модели торгов за размещение рекламы, включая PPC, CPM, CPI и так далее.
- И что самое важное для маркетологов, полагающихся на данные, мгновенный доступ к количественным показателям.

К несчастью, сегодня уже нет оснований полагать, что каждый клик по рекламе делает реальный человек, заинтересованный в покупке ваших продуктов, товаров или услуг. Барри Левин утверждает: ... риск скликивания у полученного благодаря маркетингу трафика, например из кампании PPC-рекламы или других рекламных кампаний, в три раза больше по сравнению с трафиком, у которого нет единого источника».

Хотя некоторые утверждают, что не стоит беспокоиться о поддельных кликах, мы не считаем, что потерянные из-за мошенников деньги следует считать платой за размещение рекламных объявлений.

Основные признаки кликфрода:

1. Резкое увеличение расхода рекламного бюджета.

2. Количество конверсий, при этом, стоит на месте, а то и вовсе падает при растущих тратах.

3. CTR на Рекламных кампаниях вырастает в разы без видимых на то причин.

4. Ваши удивлённый глаза, которые не понимают, что происходит.

Яндекс.Директ утверждает, что их антифрод-программа сама умело справляется с фродом, используя для защиты систему, которая распознаёт скликивание по более чем 200-м метрикам. Как это работает на самом деле — мы вряд ли когда-нибудь узнаем.

Суть скликивания рекламы

В чем разница между «мошенническими» и «недействительными» кликами, и действительно ли она важна? Под «недействительными кликами» Google подразумевает непреднамеренные клики и мошеннические клики. Примеры недействительных кликов:

- Случайные клики, например, когда кто-то дважды нажимает на объявление.
- Клики и показы, реализованные с помощью автоматизированных инструментов, или ручные клики, направленные на увеличение затрат на рекламу или прекращение ее показа.
- Клики и показы, реализованные с помощью автоматизированных инструментов, или ручные клики, направленные на увеличение прибыли владельцев сайтов, размещающих вашу рекламу.

Последние два примера — скликивание. Оно представляет собой взаимодействие между пользователем и рекламным объявлением с оплатой за клик с целью извлечения прибыли из сборов, взимаемых с маркетологов за размещение рекламы.

Кто стоит за мошенническими кликами?

Иногда за скликиванием стоят люди, а не боты. В параграфах ниже описаны наиболее распространенные случаи мелкомасштабного скликивания. В таких случаях обнаружить злоумышленников обычно не составит труда, поскольку они, скорее всего, не очень хорошо скрываются — их можно выявить по поведению и/или IP-адресу.

Конкуренты, вручную кликающие по вашим объявлениям, чтобы срывать ваши маркетинговые кампании

Иногда, особенно в отраслях с высокой конкуренцией, к скликиванию прибегают, чтобы получить преимущество перед конкурентами. Многократно кликая по рекламным объявлениям, конкуренты опустошают выделенный на PPC-рекламу бюджет компании, выбранной в качестве жертвы, чтобы не дать потенциальным клиентам увидеть эти объявления.

Хуже всего то, что провернуть этот вид мошенничества не так уж сложно: если вы не организовали защиту от таких атак, рекламное объявление с оплатой за клик будет показываться до тех пор, пока не закончится его бюджет, выделенный на один день.

В этом случае конкуренты могут очень быстро исчерпать ваш рекламный бюджет. Для этого они могут либо многократно нажимать на ваши объявления с одного устройства, либо воспользоваться услугами третьих лиц для координации сотен кликов, выполняемых на нескольких устройствах (пример атаки типа «услуги по скликиванию» мы обсудим позже).

Иногда можно обнаружить клики конкурентов, отслеживая закономерности взаимодействия с рекламой в определенной нише. В простых случаях, когда конкуренты, не обладающие техническими навыками, пытаются срывать ваши кампании, вы можете распознавать клики конкурентов по их IP-адресам и запрещать им доступ к рекламе.

Издатели интернет-рекламы, которые вручную кликают по рекламе, чтобы увеличить доход от нее (отчасти с помощью своих друзей)

Некоторые издатели могут попытаться увеличить свой доход, кликая по рекламным объявлениям или получая прибыль от кликов своих друзей. Однако это незначительная угроза: если ручное, а значит, легко обнаруживаемое скликивание станет слишком интенсивным, то учетная запись AdSense будет приостановлена.

Часто скликиванием занимаются веб-мастера, на сайтах которых размещается реклама

Когда происходит клик по объявлению, веб-мастер получает свою прибыль с переходов по рекламе, размещенной на его сайте. Они заинтересованы в том, чтобы реклама на их сайте кликалась как можно чаще, а если этого не происходит, могут прибегнуть к искусственному увеличению кликов на своей площадке.

Ничего, кроме расхода рекламного бюджета, такие клики, конечно же, не принесут. Искусственная накрутка кликов на рекламных площадках наносит вред не только рекламодателям, но и поисковым системам. Ведь если реклама перестанет приносить

прибыль владельцам бизнеса, они просто перестанут рекламироваться в Яндекс и Google и станут искать качественный трафик через другие каналы.

Поисковые системы выдвигают ряд требований к площадкам, на которых размещаются их рекламные блоки. Эти требования касаются, в том числе, и качества трафика. Алгоритмы Яндекса прогнозируют конверсию по каждому клику, совершенному на площадке, и автоматически повышают или понижают ставку в зависимости от вероятности конверсии. Тем самым Яндекс мотивирует веб-мастеров повышать качество контента и привлекать живую платежеспособную аудиторию, вместо того чтобы заниматься скликиванием.

Алгоритмы Яндекса отсеивают большую часть недобросовестных площадок, но они не идеальны. Даже с пониженной ставкой за клик некачественная площадка может «откусить» существенную долю бюджета. Так что мы рекомендуем регулярно проверять и анализировать отчет по площадкам, и отключать сайты с плохими показателями. Некачественные площадки легко распознать по аномально высокому CTR, высокому показателю отказов и отсутствию конверсий.

Недовольные клиенты, которые пытаются отомстить компании

Некоторые недовольные клиенты не ограничиваются плохими отзывами в Интернете. Вместо этого они неоднократно кликают на рекламу конкретной компании.

К счастью, это маловероятный сценарий. И, если только один из ваших недовольных клиентов не обладает техническими знаниями и навыками, такое скликивание тоже легко обнаружить и остановить из-за повторяющегося характера кликов.

В целом, по сравнению с киберпреступниками или теми, кто предлагает услуги по скликиванию, злоумышленники, занимающиеся скликиванием в одиночку, наносят несущественный ущерб.

Организованные преступники, занимающиеся скликиванием

Киберпреступники используют программное обеспечение, чтобы извлекать прибыль для своих незаконных организаций, в том числе при помощи скликивания. Ниже приведены некоторые примеры того, как преступники могут получать прибыль от мошеннических кликов. Эти примеры не исключают друг друга и могут совмещаться.

Преступники, которые наживаются на мошеннических кликах, используя ботов

Преступники часто полагаются на трафик, состоящий из ботов, чтобы извлекать прибыль по-крупному. Согласно этой инфографике Invesp, на боты, или приложения,

выполняющие автоматизированные задачи, приходится 56% трафика сайтов. Однако не все эти боты посещают сайты, чтобы нанести им какой-то вред.

Полезные боты помогают следить за состоянием сайта, обеспечивают его присутствие в поисковой выдаче и распространяют его содержимое в социальных сетях. Также полезные боты проверяют наличие битых ссылок, собирают SEO-данные, следят за RSS-каналами и выявляют уязвимости в системе безопасности.

Плохие боты, занимающиеся скликиванием, созданы именно для этой цели. Один из распространенных признаков атак ботов — необычный всплеск кликов за пределами региона, на который настроен таргетинг рекламы. Еще один способ избежать обнаружения, которым пользуются боты, — сокрытие своего физического местоположения с помощью виртуальных частных сетей (VPN'ов) и прокси-сервисов или просто обеспечение анонимности своего IP-адреса.

С годами обнаруживать их становится всё труднее. Сложные роботы, созданные для имитации человеческого поведения, могут подделывать тип устройства, принимать и запоминать файлы cookies, имитировать движение мыши и даже заполнять формы. По словам Майкла Визарда, ссылающегося на результаты доклада Radware 2020 года, «более половины (58%) вредоносных ботов, обнаруженных в феврале, … теперь могут имитировать поведение человека».

Киберпреступники, создающие ботнеты, которые трудно обнаружить

Одна из распространенных практик среди киберпреступников — заражение компьютеров интернет-пользователей вредоносным программным обеспечением, чтобы создавать сети ботов, или ботнеты и с их помощью достигать различных преступных целей. Скликивание — одна из таких целей.

К несчастью для рекламодателей, ботнеты могут эффективнее избегать обнаружения, поскольку клики, на которые они запрограммированы, будут идти с множества обычных компьютеров с реальными IP-адресами. Чтобы обнаруживать ботнеты, нужно организовать продвинутое отслеживание поведения посетителей.

Злоумышленники, которые подключаются к рекламным сетям в качестве издателей интернет-рекламы, занимающихся мошенничеством

В этом случае преступники извлекают прибыль из мошеннических кликов через сайты, специально созданные для размещения рекламы. Сначала они направляют на свои недавно созданные сайты огромный объем искусственного трафика, состоящего из ботов. Набрав необходимую статистику, преступники присоединяются к рекламным сетям в качестве издателей и начинают получать прибыль от фальшивых кликов. Чаще всего такие

сайты легко распознать по странно выглядящим доменам, некачественному или скопированному контенту и обилию рекламы.

Как это работает?

Допустим, ваше объявление занимает первое место на поиске Яндекса по запросу «заказать пластиковые окна» в регионе Москва. Ниша перегрета, и у ближайшего конкурента не хватает бюджета, чтобы перебить вашу ставку. Он скликивает ваше объявление до тех пор, пока у вас не израсходуется дневной бюджет. Ваша реклама останавливается, а ближайший конкурент попадает на верхнюю строчку и получает переходы по более низкой цене — пока вы не поймете, что реклама не откручивается, и не увеличите бюджет.

Именно по причине скликивания часто «выгорают» рекламодатели, которые настраивают рекламу для себя. Не разобравшись, в чем дело, они делают вывод, что контекст не работает, и забрасывают этот канал. Конкуренты могут скликивать объявления двумя способами: ручным и программным.

При ручном методе по объявлениям кликают люди:

1. Сотрудники конкурента. У сотрудников может быть ЦУ — например, время от времени находить в поиске объявления конкурентов с разных устройств (рабочего, домашнего ПК, смартфона) и кликать по ним. Допустим, если у конкурента 50 сотрудников, и каждый кликнет по 1 разу в день, получится 50 кликов. При цене клика 30 рублей это 1500 рублей в день, или 45 000 рублей в месяц.
2. Специально нанятые фрилансеры, которые переходят по ссылкам за небольшую плату. Они используют анонимные VPN, чтобы обойти фильтры рекламных систем. Кроме того, их поведение похоже на реальных пользователей — они могут пребывать на сайте некоторое время и просматривать несколько страниц.

Для программного метода используется софт. По объявлениям переходят боты, которые имитируют поведение пользователей. Простейшие программы покидают сайт сразу после перехода. Более продвинутые — могут показывать визиты длительностью до 15 секунд. Резкая просадка в дневном бюджете — чаще всего именно результат работы ботов.

Что вы можете сделать?

Как бороться со скликиванием со стороны конкурентов

Начнем с того, что у Яндекса.Директ и Google Ads есть свои системы отслеживания и борьбы с мошенническими кликами. Каждый переход по объявлению проверятся по ряду

факторов и проходит десятки фильтров. При этом трафик фильтруется не только в момент клика, проверки продолжаются и через время после перехода.

Если защитные механизмы систем контекстной рекламы вычислили недобросовестные клики, рекламодателю делать ничего не нужно — деньги за такие переходы не списываются. Или возвращаются на счет, когда кликфрод вычислили через какое-то время после перехода.

Узнать количество переходов, которые система контекстной рекламы посчитала недействительными, можно в отчетах.

Google Ads. Откройте отчет по кампаниям, кликните на значок «Столбцы» над таблицей и в открывшемся окне поставьте галочку напротив пункта «Недействительные клики» в блоке «Эффективность».

Яндекс.Директ. Увидеть число переходов, которые система отфильтровала как кликфрод, можно в отчетах «Общая статистика» и «Поисковые запросы». Они прописываются отдельной строкой в конце таблицы, указывается общее количество отфильтрованных переходов за весь выбранный период.

Посмотреть, как вели себя пользователи в подозрительных визитах, можно в инструменте Яндекс.Метрики «Вебвизор», а увидеть все клики — и засчитанные и отфильтрованные — там же, в отчете «Рекламные системы».

Защитные механизмы систем контекстной рекламы развиваются, обучаются и распознают кликфрод лучше с каждым годом. Но они все еще могут давать сбои. Если в статистике вы видите гораздо больше похожих на скликивание визитов, чем недействительных кликов в отчетах рекламных систем, стоит сообщить об этом — подать жалобу в отдел клиентского сервиса Яндекса или заполнить форму для оценки качества кликов Google Ads.

Как быстро понять, что вас скликивают?

Не прибегая к анализу лог файлов вручную или специальными сервисами, опознать кликфрод можно по статистике рекламных кампаний. Если вас скликивают, скорее всего, в отчетах вы увидите такие признаки:

1. Количество кликов и CTR объявлений значительно выросли без видимых на то причин.
2. Количество конверсий не увеличивается пропорционально количеству кликов.
3. Показатель отказов за тот же период аномально высокий, а время на сайте, наоборот, низкое.
4. Большинство посетителей не передают cookies.

5. В Вебвизоре появилось много записей, на которых посетитель не делает ничего, кроме как закрывает страницу.

Общий масштаб проблемы скликивания

Как убедиться в наличии и масштабах умышленного вредительства? Откройте Wordstat Yandex и введите запрос “скликать конкурента”. Чтобы не делать выводов с одного запроса - возьмите их несколько по теме.

Какие признаки могут свидетельствовать о кликфроде?

1. Аномально высокое число кликов с одного IP- адреса. Ни один здравомыслящий клиент не будет кликать до 10 и более раз по одной и той же рекламной ссылке в течение двух-трех дней. Практика показывает, что мошенники обычно используют выходные дни для скликивания, чтобы рекламодатель оперативно не зафиксировал кликфрод;
2. Большое количество посетителей, которые быстро покидают сайт. В качестве подтверждения возможности кликфрода можно использовать видеозапись поведения посетителей на сайте. Если после прихода на сайт по ссылке посетитель вообще не взаимодействует с элементами сайта, то высока вероятность, что это мошенник, занимающийся скликиванием;
3. Высокое количество кликов на партнерских сайтах (например, в Яндекс.РСЯ).
4. Снижение уровня конверсии. Если вы отмечаете зависимость роста конверсии от деятельности вашей контекстной рекламы, то этот показатель может быть использован для выявления кликфрода. Т.е. падающий уровень конверсии при увеличении кликов на рекламу – это опосредованный признак скликивания.
5. Увеличение количества кликов на все ключевые слова, особенно если это происходит в условиях ограниченной узнаваемости сайта и его нахождении не на ведущих позициях в поисковых системах. Размещая рекламу по низкочастотным запросам, шанс нарваться на кликфрод существенно ниже.

Что вы можете быстро сделать сами для защиты?

1. Конкретные ключевые запросы. Показывайте объявление только целевой аудитории. Используйте конкретные ключевые запросы, которые не попадут в выдачу сторонним пользователям.
2. Оптимизированный текст объявления. Сделайте текст более побуждающим к действию – он работает лучше, чем неоптимизированное объявление вверху списка выдачи. Реальные покупатели смотрят все варианты и выберут более привлекательный, а мошенники направляют усилия на топовые объявления, так как клики по ним принесут им больше прибыли.
3. Четкое гео-таргетирование. Показывайте рекламу только в целевом регионе. Вы автоматически устраните угрозу скликивания с прокси других стран. Конечно, это

не мешает мошенникам, если они работают через прокси-сервер, установленный в вашем регионе или без определения географии. Но их не так много и поэтому выявить проще.

4. Блокировка по адресу. Google позволяет блокировать показ на определенных почтовых адресах – укажите их адрес или диапазон адресов. Для этого нужно знать адресное пространство конкурентов, что не всегда возможно или потребует помощи специалиста.
5. Управление рекламным бюджетом. Установите ограничение на дневной бюджет, то есть, показы объявления прекратятся, когда он закончится. Вы заметите, если деньги уходят быстрее, чем обычно, и проверите, целевые ли это переходы. Усложняйте график показов, например, убирайте объявление на неделю – так вы запутаете кликеров.
6. Выбор рекламной площадки. Не рекламируйтесь на площадках с низкой репутацией – их владельцы заинтересованы в прибыли, неважно какими способами. Отключите показы по категориям «Игры» и «Работа и образование». Особенно в сфере услуг и сложных товаров. Возьмите на заметку черный список площадок в КМС Google – там высокий CTR и 100% показатель отказов.
7. Запрет показов объявлений определенным IP- адресам — эта опция позволяет отключить показ для IP-адресов, которые вы заподозрили в мошеннических действиях. Показы с IP- адресов из подсетей Яндекса не учитываются в общей статистике, не влияют на ваши траты. Всего можно добавить до 25 адресов (в Google.Ads до 500 адресов на одну кампанию).

Скликивание как сфера услуг

Скликивание как услуга может выглядеть по-разному — от работников, за невысокую оплату кликающих на рекламу для увеличения прибыли издателей, до атак при помощи распределенных ботнетов, заказанных беспринципными конкурентами.

Клик-фермы — поддельные лайки, подписчики и клики по рекламе

Клик-фермы располагаются преимущественно в странах третьего мира, где для этой цели нанимают низкооплачиваемых работников, чтобы они ставили фальшивые лайки, накручивали подписчиков в социальных сетях или кликали по рекламным объявлениям. Клик-фермы могут использовать сочетание людей и роботов, но обнаруживать скликивание, связанное с «человеческим» трафиком, особенно сложно, поскольку отличить работников клик-фермы от добросовестных пользователей труднее.

Услуги ботов и сборщиков веб-данных

Помимо того, что киберпреступники в своих целях используют ботнеты и ботов, они еще и предлагают свои услуги заинтересованным сторонам, например, конкурентам,

желающим получить незаслуженное преимущество при размещении своей цифровой рекламы.

Нормальные клики, влияющие на эффективность рекламы

Бывают случаи, когда клики, собственно говоря, осуществляются без злого умысла, но все равно вредят рекламодателям из-за отсутствия намерения приобрести рекламируемый товар, продукт или услугу. В то же время их нельзя назвать случайными, поскольку пользователи кликают по рекламе, чтобы попасть на ваш сайт. Тем не менее, поскольку за такими кликами не следует покупка товаров или услуг, они будут влиять на ваш показатель ROAS. Вот три примера кликов, которые попадают в эту категорию:

- Клики от пользователей, которые «просто серфят по Всемирной паутине», но всё равно неоднократно нажимают на рекламу. Таких пользователей также называют «lookie-loos», то есть посетители-зеваки или интернет-серферы.
- Клики от уже привлеченных клиентов (конвертированных пользователей) с намерением перейти на сайт бренда.
- Клики за пределами выбранного рекламодателем региона.

Интернет-серферы

Интернет-серферы зачастую что-то неоднократно ищут во Всемирной паутине и кликают на рекламу множество раз, так и не совершив покупку. Это может не вызывать тревоги у компаний, которые проводят маркетинговые кампании с низкой стоимостью клика, но рекламодатели, проводящие кампании с высокой стоимостью клика, захотят предотвратить увеличение затрат на привлечение клиентов, обусловленное кликами интернет-серферов.

Отслеживая поведение посетителей и конверсии после клика по рекламе, вы сможете отличить качественный трафик от некачественного и исключить источники, где взаимодействие с вашей рекламой осуществляется сомнительным образом.

Уже привлеченные клиенты

В этом случае клиенты ищут определенный бренд по названию и кликают на рекламу бренда, чтобы попасть на соответствующий сайт. Возможно, есть смысл прекращать показ рекламы после конверсии, чтобы избежать такого рода расходов на рекламу.

Клики за пределами выбранного рекламодателем региона

Как мы уже говорили выше, киберпреступники часто используют VPN и прокси-серверы для маскировки своего местоположения. Во многих случаях прокси-серверы

используются обычными людьми, которые беспокоятся о своей конфиденциальности в Интернете или пытаются обойти интернет-цензуру в определенных регионах.

VPN также часто используются для доступа к сайтам с региональными ограничениями. Кроме того, они шифруют данные, и поэтому часто используются для сокрытия активности при интернет-серфинге от третьих лиц, например при использовании общественного Wi-Fi. Не все клики, выполненные с применением прокси-серверов или VPN, — мошеннические: если поисковые запросы разнообразны и распределены естественным образом, то эти клики, скорее всего, сделали обычные пользователи виртуальных частных сетей или прокси-серверов.

Однако независимо от намерений пользователей большинство кликов, выполненных с использованием прокси-серверов, влияют на точность отчетов ваших рекламных кампаний — в случае IP-адресов, скрытых прокси-серверами, показы рекламных объявлений будут основаны на ложных данных о местоположении и ложных сетевых данных. И до тех пор, пока геолокационные возможности Google не улучшатся, возможно, вам стоит рассмотреть дополнительные методы защиты рекламных объявлений.

Два фактора, которые определяют, подвержена ли отрасль, в которой вы работаете, скликиванию

Можно выделить два критерия, определяющие вероятность того, что в той или иной отрасли можно столкнуться со скликиванием:

- Объем онлайн-трафика.
- Стоимость одного клика по релевантным ключевым словам.

Согласно исследованию Bloomberg 2015 года, в зоне риска находятся такие отрасли, как финансы, семейный бизнес и пищевая промышленность. Эти три отрасли охватывают широкий спектр подотраслей, включая:

- Частных консультантов.
- Банки.
- Отели.
- Рестораны.
- Бары.
- Больницы.
- Производителей продуктов питания.
- Спа-салоны.
- Медицинские клиники.
- Кредитные организации.

Согласно тому же исследованию Bloomberg, три отрасли, которые меньше всего страдают от скликивания, — это спорт, наука и информационная отрасль. Причина в том, что у большинства пользователей, делающих запросы по любой из этих трех тем, практически нет намерения совершить покупку. Более того, развлечения и образование — чрезвычайно широкие отрасли, что защищает рекламу в этих отраслях от скликивания.

Тем не менее важные события, сезонность или научные достижения, заслуживающие внимания в СМИ, могут изменить структуру трафика и сделать его привлекательнее для злоумышленников.

Три эффекта, которые скликивание оказывает на ваш бизнес, помимо опустошения рекламного бюджета

Мало того, что недействительные клики опустошают рекламный бюджет. Из-за мошеннических кликов практически невозможно определить эффективность рекламных кампаний. Скликивание оказывает на бизнес еще три эффекта:

- Искажение статистических показателей рекламных кампаний.
- Снижение показателя ROAS.
- Расходование впустую времени и сил сотрудников.

Из-за искаженных показателей маркетинговые кампании могут проводиться вслепую

В некоторых случаях фальшивые клики могут составлять до 90% от общего количества зарегистрированных взаимодействий с рекламой. Когда значительное количество кликов и трафик в целом поступают из сомнительных источников, показатели эффективности становятся практически бесполезными.

Не зная источника каждого клика, легко предположить, что маркетинговая кампания провалилась из-за неправильно спланированной структуры или бюджета. Но очень часто рекламные кампании терпят неудачу потому, что скликивание не позволяет им добраться до реальных клиентов.

Когда оптимизация кампании основана на догадках или неточных данных, маркетологи могут в итоге потратить время на задачи с малой или нулевой отдачей. Например, они могут начать оптимизировать кампании с высоким объемом трафика и низкой эффективностью в надежде улучшить показатели конверсии, вместо того чтобы решить основную проблему — мошеннические клики, искажающие результаты кампаний.

Неэффективные маркетинговые кампании с низким показателем ROAS

Как и недобросовестные конкуренты или любители поглазеть, роботы никогда не сделают реальную покупку. Это означает, что недействительные клики увеличат стоимость каждой конверсии и повлияют на возможность находить потенциальных клиентов в Интернете.

Если вы не будете бороться с роботами, то будете переплачивать за полученные конверсии, упуская дополнительные возможности попасть в поле зрения реальной аудитории вашей рекламы.

Расходование впустую времени и сил сотрудников

Помимо искажения показателей рекламной кампании, мошеннические клики могут стать причиной того, что ваши сотрудники будут фокусировать свое внимание на работе, не приносящей дохода.

Например, ваш отдел продаж может в итоге заниматься гонкой за фиктивными потенциальными клиентами — ботами, которые формируют искусственный трафик, кликают по рекламе и разработаны для имитации поведения пользователей посредством заполнения форм, предназначенных для сбора лидов.

Почему скликивание так трудно пресечь?

Если вы посмотрите на данные Google Trends, то увидите, что пик поисковых запросов, связанных со скликиванием, пришелся на июнь 2006 года. «Adwords click fraud», то есть «скликивание на Adwords» было в тренде еще в 2005 году. И всё же, несмотря на снижение количества поисковых запросов, скликивание вовсе не исчезло — в своей колонке «Martech Today» Мэри Уоллес пишет, что «исследование, проведенное рекламными агентствами The&Partnership, m/SIX и компанией Adloox, занимающейся проверкой рекламы, показало, что в 2017 году рекламодатели потратили впустую 16,4 миллиарда долларов из-за мошеннического трафика и кликов». По оценкам экспертов Juniper Research потери рекламодателей достигнут 100 миллиардов долларов к 2023 году.

Конфликт интересов, находящийся в самом центре индустрии цифровой рекламы

Одна из основных причин, по которой цифровые маркетологи до сих пор сталкиваются со скликиванием, состоит в несоответствии мотивов рекламодателей и рекламных сетей. Джессика Нивер в 2010 году (еще 12 лет назад) в статье «Солнце, радуга и мошенничество в сети партнерских сайтов Google» писала о проблеме выявления недобросовестных издателей интернет-рекламы:

Очевидно, что чем больше сайтов будут показывать рекламу, тем больше будет кликов по ней, а значит, Google будет получать больше денег. Поэтому Google хочет, чтобы в ее рекламной сети было как можно больше сайтов. По правде говоря, увеличение доходов Google должно также означать увеличение доходов компаний, если они будут тщательно подбирать сайты, соответствующие их отраслям, а их маркетологи будут знать, как конвертировать поступающий трафик. Но не забывайте, что здесь участвует еще одна сторона-посредник — владелец сайта, на котором вы размещаете рекламу.

Эта проблема имела место еще в 2010 году. Согласно отчету Radware о вредоносных ботах, «многие из поддельных сайтов... также приносят дополнительный доход, участвуя в скликивании, которое обманывает рекламные сети».

Другая проблема заключается в том, что Google занимает уникальное положение в рекламной индустрии: она, несомненно, предлагает самый простой и эффективный способ попасть в поле зрения потенциальных покупателей.

В результате рекламодатели готовы мириться со многими недостатками, такими как невозможность легко менять стандартные параметры рекламных объявлений, невозможность корректировать рекомендуемые географические положения и предоставление доступа только к неполной информации, а тот факт, что Google Ads — чрезвычайно сложная платформа, не облегчает жизнь рекламодателей. В то время как обычная аналитика PPC-кампаний дает некоторое представление о том, кто делает клики,

«умные» кампании недоступны для анализа, что делает цифровую рекламу аналогом игрового автомата — что, по иронии судьбы, противоречит обещаниям, которые дают рекламодателям в индустрии цифровой рекламы.

Кроме того, последние события показывают, что конфликт между интересами рекламодателей и рекламных сетей становится все более явным. Дэниел Зраст подводит итог в этом посте от июня 2020 года: *«В то время как Google Ads действительно может помочь бизнесу добиться успеха, растущее давление, заставляющее тратить всё больше средств, выходит из-под контроля, и дальше будет только хуже, потому что у рекламодателей в любом случае не так много вариантов выбора рекламных сетей»*.

Звучит слишком пессимистично? В статье «Google Ads удаляет поисковые запросы, составляющие 28% бюджета на рекламу в поисковой выдаче», которая была опубликована на Seer Interactive всего через три месяца после публикации Даниэля Зруста, говорится:

За последние три года мы обнаружили более 40 миллионов долларов, неэффективно потраченных на рекламу в основном по низкочастотным поисковым запросам. Компания Seer изучила 5,1 миллиона измеряемых параметров по более чем 30 компаниям, проводящим рекламные кампании в поисковой выдаче, и обнаружила, что 15% бюджетов расходуется в основном на скрытые низкочастотные поисковые запросы, которые не оказывают влияния на конечный результат, то есть на конверсии.

Учитывая частые изменения в алгоритмах поиска и ежедневное развитие поисковых возможностей, доступных пользователям, ваши рекламные кампании в поисковой выдаче могут зачастую сопоставлять ваши объявления с поисковыми запросами, которые не всегда соответствуют целям вашего бизнеса.

Эти небольшие, но частые сопоставления приводят к большому количеству непреднамеренных кликов от пользователей, которые привыкли кликать по нескольким результатам в верхней части поисковой выдачи. Таким образом теряются реальные деньги, которые можно было бы повторно вложить в кампании с высоким ROI, то есть с высоким коэффициентом окупаемости инвестиций. Эти расходы не должны быть «платой за сотрудничество с Google».

Несомненно, реклама с оплатой за клик может помочь вам достичь целей своего бизнеса, но есть множество системных недостатков, которые снижают эффективность вашей рекламы с оплатой за клик и открыто подвергают цифровую рекламу риску стать жертвой скликивания. Учитывая, сколько выгоды получают мошенники, разрабатывая всё более продвинутых ботов и новые обходные пути, чтобы оставаться на шаг впереди, вряд ли рекламная индустрия в одночасье сможет избавиться от мошеннических кликов.

Прежде всего, расследование сложных киберпреступлений требует значительных усилий и глубоких знаний. Хуже того, мошенники, занимающиеся скликиванием, как известно, организуют и проводят махинации из-за рубежа, что еще больше затрудняет привлечение их к ответственности. Более того, в некоторых странах законов или регулирующих органов, необходимых для борьбы с мошенниками, просто еще не существует.

Время PPC-рекламы прошло?

Согласно отраслевым прогнозам, цифровую рекламу вряд ли заменят другие виды рекламы вне зависимости от того, будет ли усиливаться скликивание. Мы согласны с тем, что цифровую рекламу вряд ли заменит какой-либо другой вид рекламы, особенно учитывая, что для многих компаний электронная коммерция и цифровая реклама стали спасением, позволяющим находить клиентов без необходимости куда-то перемещаться.

Как говорит Маргарет Хоффман, стратег Brainlabs по платным рекламным каналам (платным медиа), в своей публикации *«Скликивание и боты: самые жуткие призраки PPC-рекламы»* на PPC Hero: *«Даже если вам становится жутко при мысли о том, какие монстры могут украсть ваши деньги, которые вы тратите на рекламу, это не повод полностью отказаться от использования PPC-рекламы…. Точно так же, как вы не закроете свой магазин из-за страха, что его ограбят, вы не перестанете заниматься цифровой рекламой из-за скликивания»*.

Тем не менее подобно тому, как владельцы магазинов принимают меры защиты от грабителей, так и рекламодатели в сфере цифровой рекламы могут защитить свои бюджеты от мошеннических кликов.

Что любая компания, запускающая цифровую рекламу, может сделать для борьбы со скликиванием

Есть много мер, которые любой маркетолог, использующий цифровую рекламу, может принимать для снижения риска стать жертвой скликивания, начиная от поддержки инициатив по борьбе со скликиванием на уровне всей отрасли и заканчивая повышением осведомленности сотрудников о скликивании и реализацией разнообразных методов минимизации риска скликивания на уровне маркетинговых кампаний.

Используйте отраслевые предложения по предотвращению скликивания

Американская ассоциация рекламных агентств (4A's), Ассоциация национальных рекламодателей (ANA) и Бюро интерактивной рекламы (IAB) создали Trustworthy Accountability Group (TAG), чтобы «сосредоточиться на четырех основных областях: устранение мошеннического рекламного трафика, борьба с вредоносным программным обеспечением, борьба с существующим за счет рекламы интернет-пиратством,

повышающая целостность брендов, и обеспечение безопасности брендов за счет большей прозрачности рекламы».

Помимо прочих инициатив, TAG разработала рекомендации для желающих стать сертифицированными борцами с мошенничеством, которые начнут применяться с января 2022 года. Программа сертификации TAG была запущена в 2016 году «для борьбы с недействительным трафиком в цепочке размещения цифровой рекламы». Здесь доступна база данных сертифицированных агентств, поставщиков технологических решений и издателей интернет-рекламы, в которой можно выполнять поиск. Кроме того, TAG публикует итоговые отчеты по недействительным кликам, региональные отчеты по мошенничеству и лучшие практики.

Повышайте осведомленность сотрудников о проблемах, связанных со скликиванием

Несмотря на масштабы скликивания и его влияние на рекламные расходы, эта проблема остается относительно малоизвестной: согласно данным из Google Trends, она уже давно не в приоритете у маркетологов.

Демонстрация того, как недействительные клики опустошают рекламный бюджет и искажают данные, — это первый шаг к обсуждению мер по защите от скликивания и разработке эффективных стратегий борьбы с ним.

Вот что могут сделать интернет-маркетологи для того, чтобы сотрудники были информированы о проблеме скликивания:

- Обмениваться информацией о внутренних маркетинговых процессах.
- Ориентировочно определять будущие расходы на цифровую рекламу и показатель ROAS, отслеживая для этого соответствующие данные.
- Внести защиту от мошеннического рекламного трафика в план информационной безопасности.
- При разработке следующего плана развития бизнеса определить роли, ориентировочные показатели и бюджеты, а также показатели эффективности для мер по защите от скликивания.

Используйте эти методы для борьбы со скликиванием, которые не требуют затрат на дополнительное программное обеспечение

Для первого шага в борьбе со скликиванием любая компания, использующая PPC-рекламу, может воспользоваться следующими методами защиты своих маркетинговых кампаний:

- Запуск маркетинговых кампаний в дневное время.

- Блокировка определенных IP-адресов и сетевых диапазонов интернет-провайдеров.
- Использование черного или белого списка IP-адресов.
- Проведение аудита используемой PPC-рекламы, чтобы понять, за что вы платите.

Проводите кампании в дневное время, пока не поймете, как обнаруживать источники мошеннических кликов

Исследование, проведенное ANA и White Ops, показывает, что большая часть мошеннического трафика поступает в нерабочее время, между полуночью и семью часами утра. Вы можете снизить риск опустошения рекламного бюджета из-за мошеннических кликов, проводя кампании только в дневное время. Конечно, это решение нельзя назвать идеальным, если ваша аудитория находится в Сети после полуночи, но для многих отраслей это один из самых простых способов значительно сократить случаи скликивания. И как только вы научитесь определять источники нормального трафика, вы сможете подготовить ночную маркетинговую кампанию и задать для нее параметры, защищающие ее от недействительных кликов.

Блокировка определенных IP-адресов и сетевых диапазонов интернет-провайдеров

Источники вредоносного трафика нередко захватывают определенные сетевые диапазоны интернет-провайдера. Внезапный приток кликов с одного и того же IP-адреса или непропорционально большой объем рекламного трафика от определенного интернет-провайдера — возможный признак подозрительной активности.

Вы можете легко найти информацию о связанных IP-адресах, чтобы заблокировать сетевой диапазон интернет-провайдера и предотвратить часть мошеннических кликов. Вы можете найти все исключения IP-адресов и диапазонов IP-адресов в настройках кампании (меню левой боковой панели) и заблокировать до 500 IP-адресов или диапазонов IP-адресов для каждой кампании в Google Ads.

Имейте в виду, что блокировка диапазонов IP-адресов интернет-провайдеров сопряжена с риском: вы можете исключить из аудитории своей рекламы реальных людей, которые могли бы стать вашими покупателями. Но, если всё сделано правильно, блокировка IP-адресов и диапазонов IP-адресов интернет-провайдеров может сэкономить бюджет ваших кампаний.

Использование черного или белого списка IP-адресов

В очень специфических случаях разные страницы на платформе для публикации рекламы могут обеспечивать разные типы трафика. Использование черного списка — это метод

исключения конкретных URL-адресов с целью запрета доступа к отдельным страницам, которые не приносят прибыльного трафика.

Однако ваша реклама может отображаться на тысячах сайтов, а домены, добавленные в черный список, могут быть в итоге заменены тем же количеством новых поддельных сайтов. Вместо того чтобы исключать определенные домены, вы можете составить список из нескольких сотен доменов, которым вы доверяете и на которых хотели бы размещать свою рекламу.

Доменами можно управлять в настройках размещения рекламы в Google Ads. По словам Ларри Кима, использование этой стратегии может снизить количество мошеннических кликов в контекстно-медийной сети Google (Google Display Network) на 90%. Однако она требует большого объема ручной работы.

Хорошо разбирайтесь в отрасли, в которой работаете, и регулярно проводите аудиты своей PPC-рекламы

Несмотря на то, что технологический прогресс усложняет эту задачу, по-прежнему можно идентифицировать реальных пользователей по закономерностям в их поведении. Как только вы узнаете, как выглядит «цифровой маршрут» вашего покупателя, вы сможете использовать эту информацию для защиты от скликивания.

Другими словами, если вы будете знать поведенческие модели своих покупателей, то сможете научиться выявлять необычное поведение пользователей. Например, если большинство ваших покупателей заполняют форму через неделю после того, как они впервые увидели рекламное объявление, поступление форм от пользователей, которым объявление было показано за несколько секунд до отправки формы, скорее всего, представляет собой атаку злоумышленников.

Понимание отрасли, в которой вы работаете, и того, насколько она подвержена скликиванию, может помочь определить риск столкнуться со скликиванием. Эта информация в сочетании с регулярными аудитами кампаний PPC-рекламы, поможет вам выявить признаки искусственного трафика и создать эффективную систему защиты своих маркетинговых кампаний.

Что можно попытаться сделать с кликфродом самостоятельно

☑ При создании и в процессе работы рекламной кампании уделите максимальное внимание настройкам: время показов, устройства и показывайте объявления только целевой аудитории в разрезе пол/возраст, регион. В Адвордс, например, можно исключить показы для посетителей с неопознанным полом.

✅ Контролируйте результативность показа в разрезе рекламных площадок и отключайте неэффективные.

✅ Воспользуйтесь возможностью установки дневного бюджета кампании. Так вы сможете и ограничить расход средств в рамках одного дня и исключить риск того, что месячный бюджет уйдет за несколько дней. Учтите такой нюанс, что обе рекламные системы допускают расхождение фактического дневного бюджета с установленным. Если в один день было потрачено меньше суммы дневного бюджета, то остаток этой суммы может быть выбран в другие дни. А в целом по месяцу вы выйдете на запланированный расход средств на кампанию.

✅ Отключайте поисковые запросы с подозрительной активностью. Через некоторое время возвращайте их к показу и наблюдайте за результатом.

✅ Если замечено скликивание с определенного IP - отключите для него показы. В Директ это можно сделать только для до 25 адресов.

✅ Воспользуйтесь возможностью задать минус-фразы при настройке кампании и минусуйте мусорные запросы в процессе ее работы.

✅ В Google Реклама рекомендую уделить внимание настройкам аккаунта “Исключенный контент” и “Исключенные типы и ярлыки”. Реклама не будет показываться рядом с контентом, который не подходит для вашего бренда, а значит часть случайных кликов уйдет.

Что делать, если вы знаете, что не можете отловить каждый мошеннический клик, или у вас нет времени всем этим заниматься

Применение перечисленных выше методов поможет вам ограничить влияние мошеннических кликов на ваши рекламные кампании. Как маркетолог, ориентирующийся на данные, вы, возможно, уже используете некоторые или большинство из этих методов. Проблема в том, что даже если вы уже анализируете данные о кликах, вносите определенные домены в черный или белый список и журналируете (логируете) IP-адреса, иногда у вас просто нет доступа ко всем необходимым данным.

Более того, отслеживание десятков или сотен кампаний вручную отнимает слишком много времени и сил. В этом случае для обеспечения защиты вы можете воспользоваться сторонними инструментами.

Что реально можно сделать, чтобы остановить скликивание с помощью сторонних инструментов

Беда в том, что ни одно решение не позволит избавиться от всех недействительных кликов раз и навсегда. Инструменты для защиты от скликивания и его предотвращения по определению представляют собой ответные, а не превентивные меры. Когда мошенники, занимающиеся скликиванием, придумывают новые способы грабежа рекламодателей, этим инструментам приходится играть роль догоняющих. Тем не менее сторонние решения могут пресечь большинство мошеннических кликов по рекламе и показов рекламы.

Поиск правильного баланса между блокировкой роботов и отсеиванием реальных клиентов

Пресечь деятельность разнообразных лиц, занимающихся скликиванием, и предотвратить бесполезные клики — главная цель большинства рекламодателей, ищущих стороннее программное решение.

И будет еще лучше, если это решение можно внедрить быстро и без лишних хлопот. Однако в тех случаях, когда вы возлагаете всю тяжелую работу на алгоритмы, работающие по принципу «настрой и забудь», вы не можете ясно видеть или контролировать их работу, если только у вас нет доступа ко всем данным и аналитическим выкладкам, доступным в программных решениях, благодаря чему вы можете проверить, что алгоритмы используют правильные данные.

Это и есть недостаточная прозрачность процессов, которую мы считаем проблемой в «умных» кампаниях рекламной платформы Google и которая также выражается в установке по умолчанию рекомендуемых настроек для рекламных объявлений Google Ads. Такой подход «черного ящика» создает дополнительные риски: вы не можете исключить столько угроз, сколько хотели бы, делаете рекламу недоступной для реальных покупателей и теряете возможные продажи своих товаров, продуктов или услуг из-за того, как настроена ваша защита от мошенников.

Чтобы защитить свои рекламные кампании от скликивания, не исключая из аудитории своей рекламы потенциальных клиентов, вам необходимо видеть, почему, когда и до какого момента конкретный источник кликов был исключен из ваших рекламных кампаний.

Как Google борется со скликиванием?

Во-первых, Google редко использует термин «скликивание» (click fraud). Вместо этого компания чаще говорит о «недействительном трафике» и «недействительных кликах». Ниже приведены некоторые типы кликов и показов, которые Google считает недействительными:

- Случайные клики, не имеющие ценности, например, второй клик при двойном клике или когда пользователь мобильного телефона тянется к ссылке, а вместо этого нажимает на рекламу.
- Вручную выполняемые клики, предназначенные для увеличения чьих-либо расходов на рекламу.
- Клики, выполняемые вручную с целью увеличения прибыли владельцев сайтов, размещающих ваши рекламные объявления. Сюда входят клики, в которых заинтересован издатель интернет-рекламы.
- Клики и показы, осуществленные с помощью автоматизированных инструментов, роботов или другого программного обеспечения, которым пользуются мошенники.
- Показы, предназначенные для искусственного снижения коэффициента конверсии (CTR) рекламодателей.

Google использует множество решений и анализирует различные данные, чтобы бороться со скликиванием. Эти меры включают в себя более 200 автоматических фильтров, работающих в режиме реального времени (например, по конкретным заголовкам User-Agent, IP-адресам, времени взаимодействия), а также ручное обнаружение скликивания и проверку кликов, которыми в Google занимается команда качества рекламного трафика.

Если Google обнаружит недействительные клики по вашим рекламным объявлениям с помощью любого из вышеперечисленных механизмов, на ваш счет будут начислены средства, чтобы вам не пришлось платить за клики мошенников и злоумышленников.

Обнаружение мошеннических кликов, выполняемое вручную

Команду качества рекламного трафика, которая не афиширует свою деятельность и редко рассказывает о своих методах работы, многие считают загадочной, даже люди из Google. В 2015 году в интервью AdAge они приоткрыли завесу тайны и немного рассказали о своей работе. Команда получает куски потенциально вредоносного необработанного кода из нескольких ресурсов, включая VirusTotal и spider.io, которыми владеет Google.

Затем команда должна провести обратный инжиниринг вредоносного кода, чтобы узнать характеристики и так называемые «сигналы» конкретной сети ботов, то есть ботнета. Сигнал — это особенности поведения, которые обычно не наблюдаются у обычных живых пользователей, но невольно закладываются мошенником при разработке бота. Сигналом

может служить значение в определенном поле cookie или характерные движения мыши между двумя точками на веб-странице.

Затем найденный набор признаков накладывается на данные о рекламных кликах для поиска совпадающих блоков трафика. Поскольку одного сигнала часто недостаточно для идентификации трафика как мошеннического, команде необходимо получить серию сигналов, появляющихся одновременно, чтобы однозначно сказать, что трафик принадлежит определенному ботнету, и избавиться от него.

На момент проведения интервью в команде Google по качеству рекламного трафика насчитывалось чуть более ста человек. Хотя за последние годы эта команда немного расширилась, она составляет лишь малую часть от общего числа сотрудников, то есть от более 135 000 человек. Словом, Google выделяет всего лишь около 0,1% своих сотрудников на обнаружение скликивания, чего, по мнению многих экспертов, недостаточно.

Как вручную проверить сайт в Google Adsense

Еще один уровень безопасности, который Google ввел для борьбы со скликиванием, — это ручная проверка сайта, когда их владельцы хотят встроить Google AdSense в свой сайт. Каждый сайт должен придерживаться правил Google Publisher Policies, чтобы получить разрешение на размещение рекламы.

Достаточные ли меры принимает Google?

Лаконичный ответ: конечно же, недостаточные. Хотя Google принимает многочисленные меры безопасности, чтобы оградить свой магазин от вредоносных приложений, всё равно каждый месяц появляется слишком много новостей о вредоносных приложениях для Android, у которых миллионы загрузок.

Исследование, проведенное в 2020 году совместно с NortonLifelock Research Group и IMDEA Software Institute, показало, что магазин Google Play — основной источник вредоносных приложений. 87% всех приложений устанавливаются из официального магазина приложений Google Play, но при этом оттуда же устанавливается и 67% вредоносных приложений.

«...] Хотя защита Android создает определенный барьер для нежелательных приложений, значительный процент таких приложений может обойти его, что подчеркивает необходимость дополнительных уровней безопасности. Постоянно развивающаяся экосистема угроз Android догоняет по размеру и сложности экосистему Windows», — NortonLifelock.

Другое исследование независимого института ИТ-безопасности AV-Test показало, что Google Play Protect — один из самых неточных методов обнаружения вредоносного

программного обеспечения. Фактически оно оказалось худшим из всех 17 протестированных приложений для обеспечения безопасности, обнаружив всего лишь около 37% вредоносных приложений.

«Нынешнее тестирование показывает, что пользователям Android всё-таки не стоит полагаться только на Play Protect. Инструмент сканирования Google выявляет всего лишь чуть более трети из почти 6 700 образцов вредоносного программного обеспечения, участвовавших в тестировании. Более 4 000 просто остались незамеченными. Для сравнения: самый низкий результат тестирования у защитного приложения AVG — 98,9 процента обнаружения», — AV-Test.

В 2020 году был заблокирован почти миллион приложений, а в 2019 году было предотвращено более 1,9 миллиарда установок вредоносных приложений, загруженных не из Google Play. Можно было бы сказать, что это огромные цифры, но сегодня они составляют лишь малую долю вредоносного программного обеспечения, обнаруженного в приложениях для Android.

Хотя Google вручную проверяет качество сайтов, прежде чем одобрить их для показа рекламы, предоставить сайт на рассмотрение в AdSense мошеннику не составит труда. Сайт просто должен выглядеть сносно, быстро загружаться и предоставлять достаточно контента, чтобы им могли пользоваться люди.

Однако мошеннику довольно легко создать сайт, отвечающий всем требованиям. Они автоматически парсят объемные публикации, переписывают контент с помощью простого искусственного интеллекта и через несколько минут получают готовый сайт, который можно монетизировать с помощью различных рекламных сетей, включая Google AdSense.

На самом же деле, например, один маркетолог, изучивший более 48 000 сайтов AdSense, подсчитал, что около 90% из них — поддельные. Он предлагает отказаться от автоматического размещения рекламы и вместо этого использовать инструмент наподобие SEMrush для поиска тематически подходящих сайтов, а затем вручную размещать на них рекламу.

Но нужно отдать должное Google — AdSense стала одной из немногих рекламных сетей, которая по результатам своей проверки отклонила поддельный сайт, созданный репортером CNBC. Основной причиной, вероятно, было то, что репортер создала точную копию основного сайта CNBC, что легко распознается поисковыми роботами-индексаторами Google как «результат парсинга» или «повторяющийся контент».

Автоматическое сканирование приложений при помощи защиты Google Play

В 2017 году Google представил Google Play Protect — комплексную службу безопасности Google для Android, которая встроена в каждое устройство с Google Play. Play Protect

предлагает два типа уровней защиты для обнаружения потенциально опасных приложений (Potentially Harmful Applications, PHA):

1. Обеспечение безопасности при помощи облачных технологий

Прежде чем приложение будет доступно в Google Play Store, оно должно пройти процесс проверки, который включает в себя автоматический анализ рисков приложения и, если необходимо, еще и ручную проверку. Также используются алгоритмы машинного обучения, поэтому системы Google узнают, какие приложения — вредоносные, а какие безопасны, анализируя всю базу данных приложений. Google сообщает: «Алгоритмы учитывают сотни сигналов и сравнивают поведение приложения во всей экосистеме Android, чтобы проверить, не выглядит ли оно подозрительным. Подозрительные приложения, например, необычными способами взаимодействуют с другими приложениями на устройстве, получают доступ к личным данным или делятся ими без разрешения, агрессивно устанавливают приложения, включая PHA, посещают вредоносные сайты или обходят встроенные системы безопасности».

2. Защита на уровне устройства

В дополнение к облачным механизмам защиты Play Protect предлагает несколько мер защиты на самих устройствах, чтобы обезопасить их от вредоносного программного обеспечения. Каждый раз, когда новое приложение загружается из магазина Google Play, Play Protect выполняет углубленное сканирование и ищет вредоносный код, преследующий хотя бы одну из следующих целей:

- Нарушить целостность устройства пользователя.
- Получить контроль над устройством пользователя.
- Обеспечить злоумышленнику возможность удаленно выполнять различные операции на зараженном устройстве, например получать к нему доступ или как-то иначе использовать его в своих интересах.
- Передавать личные данные или учетные данные с устройства без ведома и согласия пользователя.
- Распространять спам или выполнять команды с помощью зараженного устройства для воздействия на другие устройства или сети.
- Обманывать пользователя.

В конце 2018 года компания Google объявила, что заблаговременно анализирует каждое приложение, которое может найти в Интернете, декомпозируя APK каждого приложения и используя глубокий анализ для извлечения сигналов PHA.

«Статический анализ изучает различные ресурсы внутри APK-файла, а динамический анализ проверяет поведение приложения во время его работы. Эти два подхода дополняют друг друга. Например, динамический анализ требует выполнения приложения

независимо от того, насколько обфусцирован его код (обфускация препятствует статическому анализу), а статический анализ может помочь обнаружить попытки что-то скрыть в коде, которые динамический анализ может не выявить. В итоге этот анализ позволяет получить информацию о характеристиках приложения, которая служит основополагающим источником данных для алгоритмов машинного обучения».

Кроме того, Google сотрудничает с компаниями ESET, Lookout и Zimperium в рамках App Defense Alliance для обеспечения безопасности магазина Google Play.

Только в 2020 году благодаря возможностям машинного обучения и усовершенствованным процессам проверки приложений Google удалось предотвратить публикацию в Google Play более 962 000 приложений, нарушающих правила. Кроме того, заблокировано более 119 000 вредоносных или спамерских учетных записей разработчиков.

Крупнейшие случаи скликивания в рекламной сети Google

Чтобы дать вам некоторое представление о масштабах мошенничества с кликами, давайте рассмотрим некоторые из крупнейших афер последних лет.

Pareto

В начале 2021 года была обнаружена крупная сеть ботов под названием Pareto, маскирующая смартфоны Android под «умные» телевизоры (Connected TV). Вредоносная программа заразила более миллиона смартфонов Android и отвечала за более чем 650 миллионов рекламных запросов в день. Зараженные устройства выглядели для рекламодателей как телевизоры и запрашивали показ рекламы каждые 30 секунд. Однако вместо того, чтобы показывать рекламу реальным людям, приложения просто вызывали указанный API и сообщали, что видео просматривается. Вредоносный код распространялся в составе непримечательных на вид приложений через магазин Google Play.

Cheetah Mobile

В начале 2020 года Google удалила из магазина Google Play более 600 приложений от китайских разработчиков Cheetah Mobile и Kika Tech из-за спама кликами (click flooding) и инъекции кликов. При инъекции кликов приложения прослушивали, когда пользователь загружал новое приложение через магазин Google Play. Как только обнаруживалась новая загрузка, приложения искали вознаграждения за фактическую установку приложения, доступные для данного приложения, и делали клики, содержащие соответствующую информацию о разработчиках приложения, чтобы Cheetah и Kika выиграли вознаграждение — даже если они не имели никакого отношения к загружаемому приложению.

Хотя эти приложения не занимались именно обычным скликиванием, их скачали из магазина Google Play более двух миллиардов раз, и при помощи этих приложений осуществлялся более продвинутый вариант мошенничества с кликами.

Vidmate

В мае 2019 года вскрылось, что Android-приложение VidMate, которое позволяло пользователям загружать видео с потоковых видеосервисов, таких как YouTube или Vimeo, отображало скрытую рекламу и генерировало поддельные клики. Кроме того, приложение загружало и устанавливало другие подозрительные приложения в фоновом режиме без согласия пользователя.

Приложение было загружено более 500 миллионов раз благодаря своей популярности в развивающихся странах, таких как Индия и Бразилия.

Дополнительно: вредоносные расширения для Chrome

Одна из тем, которую мы еще не затронули, — это браузер Google Chrome. Обладая долей рынка более 65% на настольных и мобильных платформах, он единолично лидирует на рынке браузеров. Благодаря такой популярности он также становится интересным для мошенников, которые находят способы использовать его в своих целях.

В начале 2018 года четыре вредоносных расширения для Chrome предприняли мошенническую аферу с кликами. Расширения содержали вредоносный код, который не только позволял мошенникам посещать сайты через прокси-сервер и браузер жертвы, но и приносил им ежемесячный доход в размере около 350 000 долларов. Их можно было загрузить из официального магазина расширений для Google Chrome.

Почему Google не предпринимает более серьезные меры против скликивания?

Чаще всего Google предпринимает меры, которые выглядят ответными, а не упреждающими. Кроме того, Google не заинтересована возглавить борьбу со скликиванием. Реклама всегда была главным приоритетом Google, на нее приходится почти 81% ее прибыли. Из $181,69 млрд прибыли в 2020 году $146,9 млрд компания получила от рекламы, и $53,1 млрд из $65,1 млрд (81,5%) прибыли в третьем квартале 2021 года.

Как рекламодатель, Google зарабатывает деньги независимо от того, правомерны ли клики. До тех пор, пока это приносит им прибыль, они не видят острой необходимости что-либо менять.

С другой стороны, сомнительно, что вся рекламная индустрия заинтересована в полном исчезновении рекламного мошенничества. Конечно, ни одна мелкая компания не хочет тратить деньги без необходимости, особенно на неживых посетителей, которые вообще

не могут конвертироваться в продажи. Но у крупных рекламодателей количество показов объявлений настоящим пользователям из-за скликивания может резко сократиться, и поначалу они сильно удивятся этому сокращению. Ведущий исследователь мошенничества доктор Августин Фоу писал о том, что в наши дни рекламное мошенничество стало настолько нормальным явлением, что все о нем знают, но никто не хочет его замечать:

«Мошенническая цифровая реклама выглядит достаточно качественно, чтобы покупатели (медиа-агентства и рекламодатели) могли «похвастаться» перед своими руководителями большими объемами рекламы, которые они купили, и «отличными сделками», которые они заключили. (...) Теперь, когда рекламное мошенничество наблюдается уже столь долгое время, во всех типах цифровой рекламы (медийная, видеореклама, реклама на мобильных устройствах и в мобильных приложения, Connected TV и так далее), оно стало настолько обычным делом, что люди даже не замечают его, даже когда оно прямо у них перед глазами. Электронные таблицы и информационные панели наглядно демонстрируют рекламное мошенничество — но люди настолько привыкли видеть там большое количество показов и кликов, что подозрений не возникает. Фактически рекламодатели хотят более выгодных для себя условий — больше показов рекламы, более низкие цены и больше кликов — неутолимый спрос, который стимулирует еще большее мошенничество с рекламой и активность ботов», — доктор Августин Фоу.

Недавнее исследование показало, что:

- 11% кликов по поисковой рекламе — мошеннические или недействительные.
- 36% рекламных кликов по медийной рекламе — мошеннические или недействительные.
- 17% показов рекламы на Connected TV — мошеннические или недействительные.

Если учесть триллион показов рекламы в Google AdSense, средний коэффициент кликов 0,46% во всех отраслях и 36% мошеннических кликов по медийной рекламе, то получится ошеломляющая цифра в 1,65 миллиарда мошеннических или недействительных кликов по медийной рекламе в месяц. Если взять за основу среднюю стоимость одного клика по рекламе в 0,63 доллара для контекстно-медийной сети Google, то ежемесячные потери от скликивания медийной рекламы составят около миллиарда долларов. При взгляде на эти цифры становится тошно.

Если вы считаете, что в ваших рекламных кампаниях Google Ads фигурирует мошенничество, вам следует подать запрос на возврат средств. Перед подачей запроса на возврат средств от Google важно убедиться, что у вас есть все необходимые данные и доказательства, как например, из журналов сервера и инструментов отслеживания, поскольку запрос можно подавать только раз в 60 дней.

После того как вы соберете все данные и доказательства, вы можете подать запрос на возврат средств через официальную форму Google. Не надейтесь на этот вариант слишком сильно, так как всего лишь 20–25% претензий на возврат средств действительно принимаются.

Саймон Янг — генеральный директор цифрового медиа-агентства, в 2018 году обнаружил мошеннические клики на рекламных объявлениях своего клиента. Затем последовала охота за техническими данными предполагаемых посетителей и общение с Google, растянувшееся на несколько этапов.

Итог: несмотря на убедительные доказательства того, что сотни кликов по рекламе исходили всего от семи устройств (семи разных MAC-адресов), Google не вернул деньги. Клики, о которых идет речь, скорее всего, были выполнены при помощи программного обеспечения для автоматических кликов, используемого главным конкурентом клиента.

Но что делать, если Google не вернет вам деньги? Вы можете попытаться обратиться в суд.

Известные судебные иски против Google, поданные из-за скликивания

Поскольку не так много людей могут позволить себе судиться с таким технологическим гигантом, как Google, публичных исков не так много. Ниже приведены некоторые из немногочисленных исков против Google за мошенничество с кликами.

Подарки и коллекционные предметы от Lane

В 2006 году 70 истцов заявили, что Google ввела в заблуждение рекламодателей относительно мер, которые она будет принимать против скликивания, и что в действительности эти меры технологического гиганта были недостаточными. В коллективном иске, поданном компанией Lane's Gifts and Collectibles, также утверждалось, что Google взимал плату с рекламодателей за недействительные клики по их рекламным объявлениям, что нанесло ущерб их бизнесу и привело к большим убыткам.

Итог: Google урегулировал дело за 90 миллионов долларов. 30 миллионов долларов пошли на оплату услуг адвокатов, а остальная сумма была предоставлена истцам в качестве рекламных средств. Эти рекламные средства представляют собой возмещение в размере $4,50 за каждую тысячу долларов, потраченную на рекламную сеть Google за последние четыре года.

Гурминдер Сингх

В 2016 году предприниматель Гурминдер Сингх подал коллективный иск против Google. Он утверждал, что заверения компании в том, что она эффективно борется со скликиванием в своей сети медийной рекламы, были преувеличены.

Он провел серию тестов, чтобы проверить свои подозрения о мошеннических кликах в своей рекламной кампании: дважды создал реальное и бредовое рекламные объявления и сравнил количество полученных кликов. Настоящее объявление получило 68 кликов, а фальшивое — 64, что, по мнению Сингха, свидетельствует о 48-процентной доле мошеннических кликов.

После неоднократного отклонения иск был возвращен в суд низшей инстанции и теперь ожидает судебного разбирательства.

AdTrader

В 2017 году Google вернул деньги некоторым рекламодателям, чьи объявления были размещены на сайтах с подтвержденным мошенническим или недействительным трафиком. Когда мошенничество было раскрыто, Google был готов вернуть свою «плату за использование рекламной платформы», которая составляет от 7 до 10 процентов от общих рекламных расходов.

Компания AdTrader подала коллективный иск против Google в федеральный суд Калифорнии, утверждая, что Google «незаконно присвоил» обещанные рекламодателям компенсации. В иске утверждается, что Google на самом деле никогда не начислял компенсации после возврата денег от рекламных издателей, обвиненных в формировании завышенного или мошеннического трафика.

AdTrader отмечает, что даже собственная служба поддержки Google «признала, что у них никогда не было системы для осуществления таких компенсаций».

Малые и средние предприятия Австралии

В начале 2021 года австралийские малые и средние предприятия, подозреваемые в скликивании, вступают в судебную тяжбу с Google, утверждая, что Google не принимает достаточные меры для борьбы с поддельными кликами. По оценкам, в прошлом году австралийские маркетологи потеряли 756 миллионов долларов из-за недействительных кликов в своих рекламных кампаниях в поисковой выдаче.

Иск еще не подан, но Марк Станаревич — адвокат и консультант компании Matrix Legal в Мельбурне, говорит, что с ним связались несколько малых предприятий.

Google предпочитает урегулировать все иски во внесудебном порядке, чтобы не раскрывать подробности о своих методах борьбы со скликиванием. Если бы дело дошло до суда, Google пришлось бы публично представить и разъяснить свои алгоритмы и методы. Это, в свою очередь, стало бы большой победой для всех мошенников, поскольку они бы точно знали, каким образом Google противодействует им.

Как подать запрос на возврат средств в Google Ads, если вашу рекламу скликали?

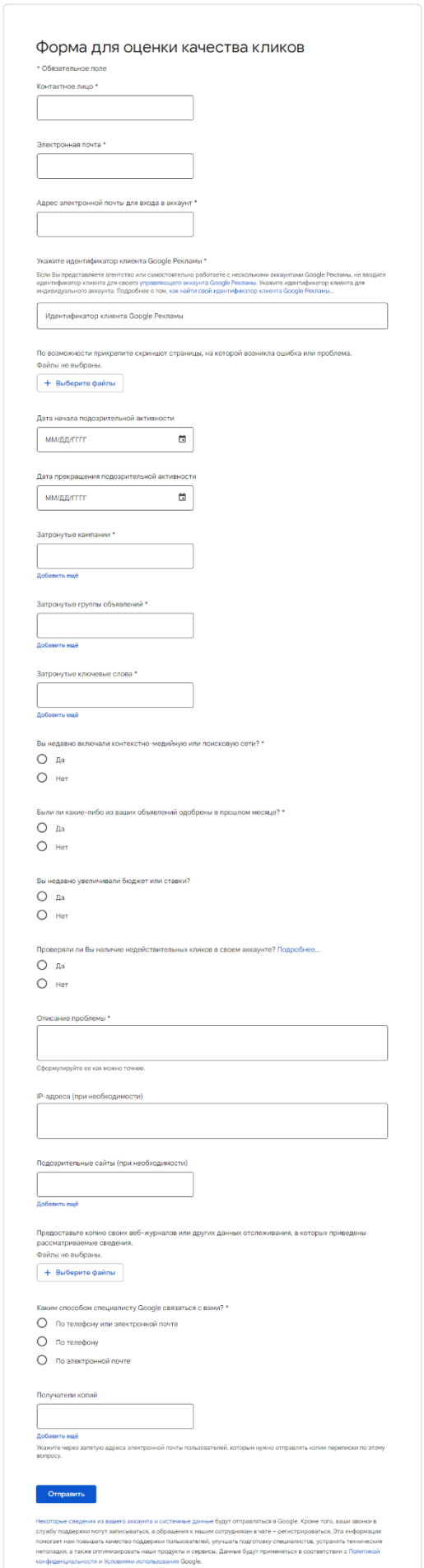
Перед тем как подавать в Google заявление на возврат средств, нужно убедиться, что вы собрали все необходимые данные и сведения, которые можно использовать в качестве обоснования для возврата средств. Этот шаг играет ключевую роль в том, добьетесь ли вы успеха, поэтому вам стоит отнестись к нему серьезно. Google возместит вам деньги только в том случае, если ваши данные в достаточной степени доказывают наличие недействительного трафика.

Кроме того, вы не должны просто отправить свою историю кликов по рекламе и надеяться, что Google сама во всём разберется. Фактически такой подход уменьшит шансы получить возврат средств. Вам нужно потратить время и силы на анализ своих данных и маркетинговых кампаний, потому что Google будет запрашивать очень специфическую информацию. Предоставить корректные данные и все доказательства — ваша забота.

Также помните о том, что вы можете запрашивать у Google возврат средств раз в 60 дней. Следовательно, очень важно, чтобы вы предоставляли все необходимые корректные данные. Шаг первый: определите, почему вам приходится подавать в Google Ads запрос на возврат средств:

CLICKFRAUD
защита от скликивания

Защита от скликивания вашей рекламы https://clickfraud.ru (Яндекс.Директ & Google.Ads)



Форма для оценки качества кликов

* Обязательное поле

Контактное лицо *

Электронная почта *

Адрес электронной почты для входа в аккаунт *

Укажите идентификатор клиента Google Рекламы *

Если Вы представляете агентство или самостоятельно работаете с несколькими аккаунтами Google Рекламы, не вводите идентификатор клиента для своего управляющего аккаунта Google Рекламы. Укажите идентификатор клиента для индивидуального аккаунта. Подробнее о том, как найти свой идентификатор клиента Google Рекламы...

Идентификатор клиента Google Рекламы

По возможности прикрепите скриншот страницы, на которой возникла ошибка или проблема.
Файлы не выбраны.

+ Выберите файлы

Дата начала подозрительной активности

ММ/ДД/ГГГГ

Дата прекращения подозрительной активности

ММ/ДД/ГГГГ

Затронутые кампании *

Добавить ещё

Затронутые группы объявлений *

Добавить ещё

Затронутые ключевые слова *

Добавить ещё

Вы недавно включали контекстно-медийную или поисковую сети? *

- Да
- Нет

Были ли какие-либо из ваших объявлений одобрены в прошлом месяце? *

- Да
- Нет

Вы недавно увеличивали бюджет или ставки?

- Да
- Нет

Проверяли ли Вы наличие недействительных кликов в своем аккаунте? Подробнее...

- Да
- Нет

Описание проблемы *

Сформулируйте ее как можно точнее.

IP-адреса (при необходимости)

Подозрительные сайты (при необходимости)

Добавить ещё

Предоставьте копию своих веб-журналов или других данных отслеживания, в которых приведены рассматриваемые сведения.
Файлы не выбраны.

+ Выберите файлы

Каким способом специалисту Google связаться с вами? *

- По телефону или электронной почте
- По телефону
- По электронной почте

Получатели копий

Добавить ещё

Укажите через запятую адреса электронной почты пользователей, которым нужно отправлять копии переписки по этому вопросу.

Отправить

Некоторые сведения из вашего аккаунта и системные данные будут отправляться в Google. Кроме того, ваши звонки в службу поддержки могут записываться, а обращения к нашим сотрудникам в чате – регистрироваться. Эта информация помогает нам повышать качество поддержки пользователей, улучшать подготовку специалистов, устранять технические неполадки, а также оптимизировать наши продукты и сервисы. Данные будут применяться в соответствии с Политикой конфиденциальности и Условиями использования Google.

Помимо недействительных кликов от ботов, могут быть и другие причины подавать в Google Ads запрос на возврат средств. Самые распространенные причины:

- Повышение количества недействительных кликов.
- Подтвержденные или обнаруженные случаи скликивания.
- Перерасход рекламного бюджета.
- Неправильное отображение ваших рекламных объявлений в Google Ads.

В каждом из этих случаев вы должны предоставлять Google информацию одного и того же характера. Просто не забудьте сообщить Google причину своего запроса на возврат средств, чтобы расследование прошло максимально эффективно. Сотрудники Google находятся под постоянным давлением, поэтому расскажите о своей ситуации настолько доступно, насколько это возможно.

Что касается недействительных кликов, вам следует обращать внимание на следующие признаки в своих отчетах:

- Резкие увеличения трафика, которые зачастую наблюдаются в нехарактерные для этого периоды времени.
- Высокие показатели отказов зачастую в сочетании со всплесками трафика.
- Множество кликов, поступающих от одного и того же IP-адреса.
- Клики, поступающие не из тех географических областей, на которые вы настроили таргетинг рекламы.

Шаг второй: соберите все необходимые данные

Перед тем как отправлять в Google Ads запрос на возврат средств, вам нужно собрать много подробных сведений. В частности, в форме для подачи запроса в Google Ads на возврат средств вас попросят указать следующую информацию:

- Ваш идентификатор клиента (customer ID).
- Даты начала и окончания периода, когда наблюдались предположительно недействительные клики.
- Затронутые скликиванием маркетинговые кампании.
- Затронутые скликиванием группы рекламных объявлений.
- Затронутые скликиванием ключевые слова.
- Список IP-адресов, через которые осуществлялись недействительные клики.
- Подробные сведения о любых рекламных объявлениях, одобренных за последний месяц.
- Подробные сведения о возросших ставках и/или бюджетах.
- Список сетей медийной или поисковой рекламы, в которых вы участвовали.
- Подробные сведения о подозрительных местах размещения медийной рекламы.

- Проверили ли вы свою учетную запись Google Ads на наличие недействительных кликов.
- Краткое описание проблемы.
- Копия журналов (логов) вашего сайта или данных о поведении пользователей.
- Предпочитаемый способ связи с вами.

Как видите, это длинный список запрашиваемой информации, и вам потребуется много времени, чтобы собрать ее и заполнить соответствующие поля формы. Кроме того, зачастую Google требуется вплоть до шести недель, чтобы обработать запрос, и нет никакой гарантии, что вы получите возврат средств. К сожалению, это единственный способ запросить возврат средств в Google Ads. Пожалуйста, обратите внимание, что к сбору данных следует отнестись очень серьезно. Мало того, что вы можете запрашивать возврат средств только раз **в 60 дней**, но Google еще и может отказаться в дальнейшем отвечать на ваши запросы на возврат средств, если информация, которую вы предоставили, была некорректной или недостаточной.

Совет: проверьте логи своего сервера — встречаются ли там повторяющиеся IP-адреса

Вероятно, самая важная информация, которую вам стоит включить в свой запрос на возврат средств, — это список подозрительных IP-адресов. По умолчанию Google Ads и Google Analytics не фиксируют IP-адреса пользователей, которые кликнули по вашим рекламным объявлениям, так как они считаются персональными данными согласно постановлению General Data Protection Regulation (GDPR). Если вы не используете другое программное обеспечение для аналитики данных, вам нужно будет с головой окунуться в журнальные файлы своего сервера. Поговорите с сотрудниками своего IT-отдела, чтобы получить полный набор данных.

Затем вам просто нужно выявить пользователей, которые пришли на ваш сайт через одну из рекламных кампаний, затронутых скликиванием. Это можно сделать либо через URL-адреса определенных целевых страниц, либо через параметры URL-адресов, которые вы привязали к этим кампаниям.

Последнее, что вам следует сделать, — это поискать повторяющиеся IP-адреса в оставшемся наборе данных. IP-адреса, которые появляются несколько раз в день в течение длительного периода, — это, скорее всего, мошеннические, а значит недействительные IP-адреса. Дополнительно вы также можете поискать подозрительные IP-адреса при помощи соответствующего инструмента:

- Инструмент от WhatIsMyIP.com для проверки присутствия IP-адреса в черных списках (IP Address Blacklist Check).
- Blacklist Master.
- IP Tracker Blacklist Check.

Если любой из IP-адресов в вашем наборе данных присутствует в черном списке, то высока вероятность, что этот IP-адрес ведет себя подозрительно и может быть связан с сетью ботов (ботнетом).

Шаг третий: отправьте форму для запроса на возврат средств в Google Ads:

1. Во-первых, перейдите на страницу с формой для оценки качества кликов. Эта форма представлена на картинке выше.
2. Внесите в форму все необходимые сведения. Ранее приводился список запрашиваемых сведений. Будьте внимательны при заполнении этих полей, а также перепроверьте, всё ли заполнено правильно.
3. Не забудьте загрузить копии логов вашего сервера или данных о поведении пользователей, демонстрирующих найденные вами подозрительные IP-адреса.
4. Введите адрес электронной почты, на который вы хотели бы получить ответ Google, и нажмите кнопку «Отправить».

После успешной отправки формы вам остается только ждать ответа от Google. Google уведомит вас о том, был ли ваш запрос на возврат средств удовлетворен, и когда он был удовлетворен. Кроме того, вы сможете увидеть возвращенные вам средства на вкладке «Транзакции» → «Настройки» в разделе с данными о платежах по своей учетной записи Google Ads.

Важно, чтобы у вас не было завышенных ожиданий, так как всего 20–25% запросов на возврат средств удовлетворяются. Более того, в действительности возмещается всего лишь приблизительно 10–15% от всех средств в каждом запросе на возврат, поэтому в целом возвращается всего около двух процентов от затрат на рекламу.

Как выявить скликивание, направленное на вашу рекламу в Google Ads

Как узнать, скликивают ли вашу рекламу? Есть хорошая новость — в зависимости от того, сколько времени и ресурсов вы можете выделить, есть много возможностей узнать, скликивают ли вашу рекламу.

Можно сделать всё собственноручно

Один из способов самостоятельно справиться со скликиванием — использовать *внутреннюю отчетность*. Чтобы следить за скликиванием с помощью внутренних отчетов, убедитесь, что вы собираете следующие данные:

- **IP-адрес** — у любого пользователя есть IP-адрес. Его можно сравнить с домашним адресом его активности в Интернете. Когда вы заходите на сайт, ваш IP-адрес оставляет следы, которые могут быть обнаружены веб-мастерами.

- **Отметка времени клика** — время, когда кто-то приходит на ваш сайт после клика по рекламному объявлению.
- **Отметка времени действия** — время, когда этот человек совершил какое-либо действие на вашем сайте.
- **Заголовок User-Agent** — характеризует устройство, на котором посетитель просматривал ваш сайт.

Собрали эту информацию? Отлично.

Теперь используйте **отметку времени клика** совместно с **отметкой времени действия**. Вам нужно искать IP-адреса, обладатели которых неоднократно заходят на ваш сайт, кликая по вашей рекламе на Google, но не предпринимая никаких действий на вашем сайте. Заметили ли вы какой-нибудь IP-адрес с большим количеством отметок времени клика, но без отметок времени действия?

Скорее всего, через этот IP-адрес выполняется скликивание.

Теперь посмотрите на **User-Agent**.

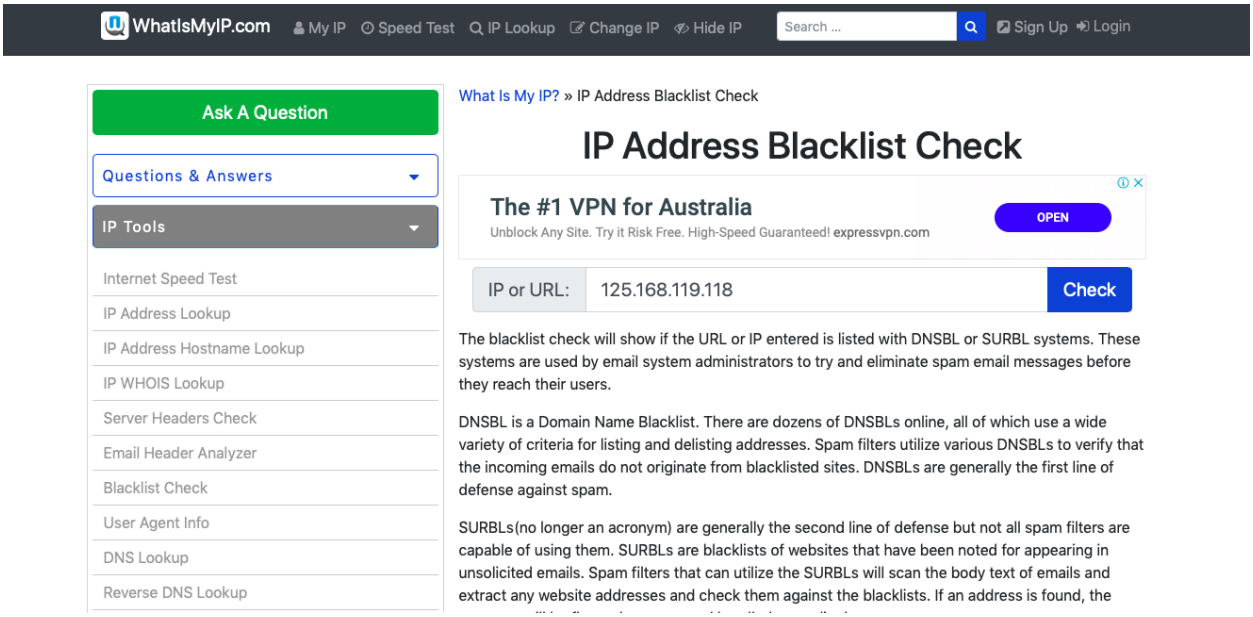
Этот HTTP-заголовок фиксирует все характерные особенности устройства, используемого для доступа к вашему сайту, как например: тип устройства, браузер и программное обеспечение.

Словом, он показывает, стоит ли за определенным IP-адресом тот же пользователь.

Что делать после обнаружения IP-адреса, через который, предположительно, осуществляется мошенническая деятельность?

При помощи быстрой проверки узнайте, кому он принадлежит. Зайдите на сайт наподобие What is my IP address («Что представляет собой мой IP-адрес»).

Если вы видите, что значительная часть вашего трафика поступает из одного и того же источника, не поленитесь проверить, принадлежит ли подозрительный IP-адрес прокси-серверу. Если поисковые запросы, инициированные анализируемым IP-адресом, разнятся, скорее всего, это прокси-сервер. Однако, если поисковые запросы похожи друг на друга, то соответствующие клики, скорее всего, мошеннические.



Как предотвратить скликивание рекламы на Google Ads

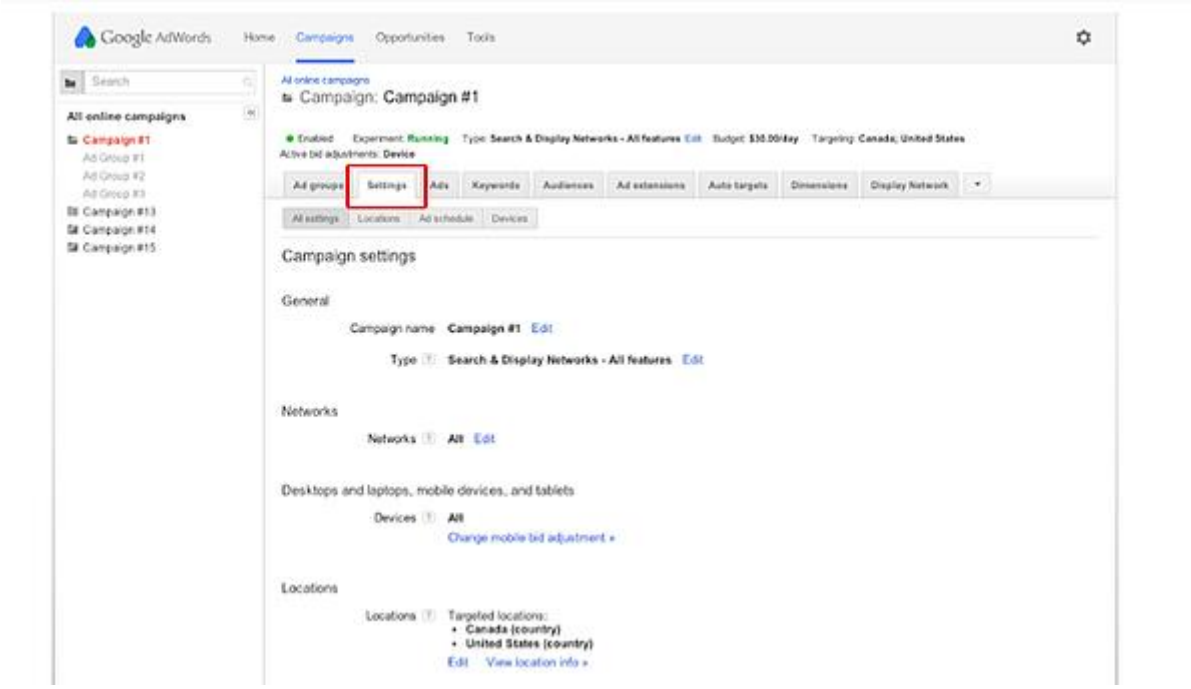
У вас создалось впечатление, что вы не можете всецело доверить Google борьбу с поддельными кликами? Хотя нельзя полностью исключить риск скликивания, есть способы собственноручно управлять предотвращением скликивания рекламы на Google Ads. Попробуйте эти восемь методов снижения риска того, что вашу рекламу будут скликивать:

- Добавьте подозрительные IP-адреса в список исключений.
- Не забывайте о конкурентах.
- Настройте ретаргетинг рекламы.
- Настраивайте таргетинг только на качественные сайты.
- Отслеживайте недействительные клики.
- Проводите ремаркетинговые кампании.
- Установите пиксель для отслеживания конверсии там, где вы можете четко сопоставить ее с другими показателями.
- Купите программное обеспечение для обнаружения мошенничества с интернет-рекламой.

1. Ведите список исключенных IP-адресов в Google Ads

Если вы в результате проверок узнали, что через определенный IP-адрес осуществляется скликивание, вы можете запретить показ своей рекламы для этого IP-адреса. Вам просто нужно добавить этот IP-адрес в список исключений в своей учетной записи Google Ads.

1. Перейдите на вкладку «Настройки».



2. Щелкните по кампании, от участия в которой вы хотите отстранить какие-либо IP-адреса.

3. Перейдите к «Дополнительным настройкам» и нажмите на пункт Исключение IP-адресов.

4. Щелкните по соответствующему полю.

5. Введите IP-адреса мошенников (до 500 адресов на одну кампанию).

6. Щелкните «Сохранить».

Вот и всё! Начиная с этого момента, Google не будет отображать ваши рекламные объявления для этих IP-адресов. Это очень эффективный способ защиты вашей учетной записи от мошенников, занимающихся скликиванием рекламы. Минус в том, что этот процесс может занимать очень много времени, если у вас большое количество IP-адресов, которые нужно блокировать и будьте осторожны — не заблокируйте потенциальных покупателей.

У пользователей часто есть несколько IP-адресов, потому что они выходят в Интернет дома, на работе и в кафе. Это не значит, что они — преступники, занимающиеся скликиванием! Убедитесь, что тщательно проверили IP-адреса, перед тем как добавлять их в список исключений.

2. Не забывайте о своих конкурентах

Учитывая потенциал скликивания к стремительному опустошению рекламных бюджетов, легко понять, почему скликивание дает конкурентам преимущество, для получения которого не требуется много усилий.

Всегда обращайте внимание на то, кто конкурирует с вами за ключевые слова в поисковых системах. Используйте Google, чтобы найти ключевые слова, на которые вы собираетесь настроить таргетинг, и посмотрите, какие еще компании тоже создают рекламные объявления по этим ключевым словам. Выясните, обладают ли ключевые слова, на которые вы планируете ориентироваться, коммерческое значение, проверяя уровень конкуренции в оплачиваемых рекламодателями результатах поиска.

Также вы можете заметить любые другие релевантные ключевые слова или фразы, на которые можно настроить таргетинг и которые тоже можно проверить на наличие коммерческого значения. Используйте эти релевантные ключевые слова или фразы, чтобы найти среди них более узкоспециализированные, на которые можно было бы настроить таргетинг, таким образом снижая количество конкурентов для вашей рекламы, но увеличивая вероятность возникновения кликов и конверсий.

Наконец, анализируйте рекламные объявления, которыми пользуются ваши конкуренты. Попытайтесь сделать какие-либо выводы из форматов рекламы, рекламных текстов и посадочных страниц, которыми пользуются ваши конкуренты, обращая особо пристальное внимание на текст, используемый для описания продукта или услуги, а также на то, как бренд стимулирует конверсию.

Кроме того, вы можете использовать отслеживающие инструменты, такие как SEMrush и iSpionage, чтобы узнать, кликают ли конкуренты по вашим рекламным объявлениям с оплатой за клик, и если кликают, то когда.

3. Настройте свой таргетинг рекламы на определенные страны

Возможно, вам всего лишь нужно немного отрегулировать таргетинг, чтобы избавиться от мошеннических кликов. А что, если вашу рекламу скликивают мошенники из определенного региона или страны? Иногда мошенники нанимают людей, чтобы они кликали по рекламным объявлениям. Такие формирования называют «клик-фермами».

Они не всегда географически расположены в одном и том же месте, но обычно находятся в странах, которые характеризуются дешевой рабочей силой. Исключите эти территории и их язык из своих кампаний на Google Ads. Не запускайте рекламу в странах, где она легко может стать жертвой скликивания.

Если вы подозреваете, что ваш основной конкурент занимается мошенничеством, исключите его почтовый индекс. Предупреждение: будьте осторожны — не заблокируйте трафик с высокой конверсией при добавлении регионов в исключения.

4. Настраивайте таргетинг только на качественные сайты

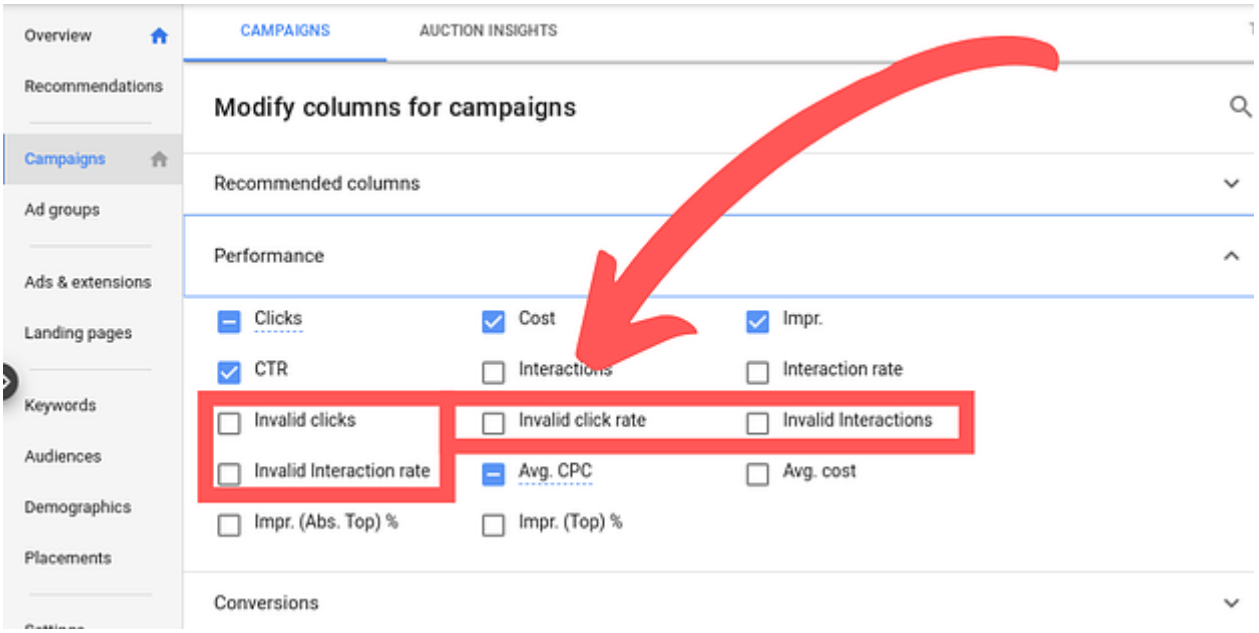
Некачественные сайты часто связаны с ботами, которые автоматически берут «под прицел» ваш сайт и рекламные объявления, а также представляют собой источник большого объема мошеннических кликов. Держитесь подальше от некачественных сайтов, размещая рекламу только на сайтах, которые, по вашему мнению, просматривает много ваших потенциальных клиентов.

И Google, и Yahoo! позволяют планировать рекламные кампании, которые размещают рекламу только на указанных сайтах, таким образом позволяя избегать сайтов, которые занимаются рекламным мошенничеством.

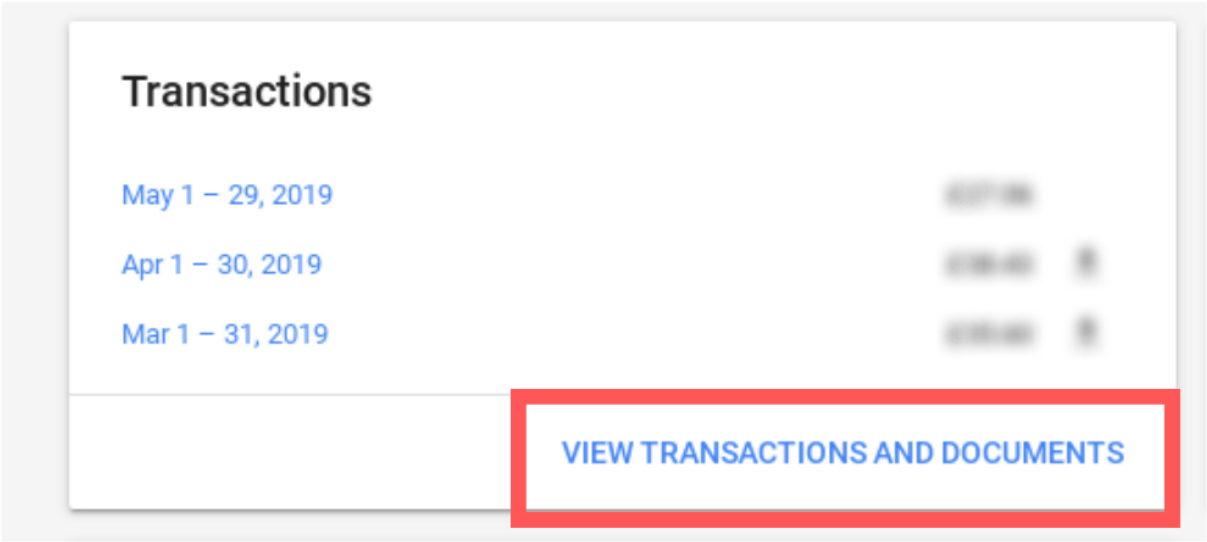
5. Внимательно следите за своими кампаниями и присутствием мошеннических кликов

Чтобы узнать, приносят ли ваши кампании PPC-рекламы реальных посетителей, всегда следите за состоянием кампаний. Если вы используете Google Ads, то отчеты Campaign Performance и Account Performance позволят вам увидеть количество и процент кликов, которые Google отнесла к недействительным.

Чтобы просмотреть недействительные клики в своих отчетах в Google Ads, щелкните на вкладку «Кампании» и выберите «Изменить столбцы». Найдите вкладку «Эффективность» и отметьте опции, отвечающие за отображение недействительных кликов и взаимодействий в ваших показателях кампании.



Любые поддельные клики, с которыми вы столкнулись, будут фиксироваться в вашей истории транзакций. Обязательно сопоставьте расходы, и если компенсационные выплаты не сходятся, создайте обращение в службу поддержки Google, чтобы не платить за ненастоящие клики.



6. Проводите ремаркетинговые кампании

Ремаркетинг — это когда вы показываете рекламу людям, которые уже посетили ваш сайт ранее. То есть ваше рекламное объявление отображается людям, которые продемонстрировали свой интерес к вашим товарам, продуктам или услугам. Возможно, они зашли на определенные веб-страницы, загрузили электронную книгу, добавили продукт в корзину и так далее.

Риск того, что мошенники будут кликать по рекламным объявлениям, здесь нулевой, поскольку они в принципе не могут их увидеть.

7. Установите пиксель для отслеживания конверсии там, где можете четко сопоставить ее с другими показателями

Отслеживание конверсии — самый эффективный способ измерить и оценить успех кампании на Google Ads. Сначала вы устанавливайте их пиксель для отслеживания конверсии на веб-страницы своего сайта.

Затем этот пиксель будет срабатывать всякий раз, когда пользователи кликают по объявлениям вашей кампании в Google Ads и посещают веб-страницы, которые отправляют сигнал этому отслеживающему механизму.

Итак, как для борьбы со скликиванием использовать пиксель, отслеживающий конверсию?

Сайты, занимающиеся спамом, используют ботов для осуществления большого количества «примитивных» конверсий, например через формы для сбора лидов. Так как эти сайты обеспечивают массу таких «конверсий», алгоритмы Google поощряют их, еще чаще размещая ваши рекламные объявления на таких сайтах.

К чему это приводит?

В итоге вы тратите впустую много денег на фальшивые конверсии из бюджета, выделенного на PPC-рекламу. Этот хитрый прием заключается в том, чтобы не отслеживать конверсию при выполнении какого-нибудь действия, которое не требует много времени и усилий, например при заполнении формы. Вместо этого настройте свой пиксель для отслеживания конверсии на какие-нибудь более сложные действия, например бесплатные пробные периоды или когда вы точно знаете, что кто-то у вас что-нибудь купил.

Эта несложная мера уменьшит количество фальшивых конверсий и обеспечит вам гораздо более точные данные о состоянии рекламной кампании.

8. Подключите программное обеспечение для обнаружения мошенничества с интернет-рекламой

Программное обеспечение для борьбы со скликиванием обнаруживает мошенничество с PPC-рекламой и защищает от него своих пользователей. Хороший способ остановить скликивание — вложиться в программное решение, разработанное для выявления сайтов, направляющих подозрительно много посетителей на ваш сайт.

Программы для борьбы со скликиванием активно следят за состоянием вашего трафика в Google Ads и автоматически заносят в черный список источники недействительных кликов. Словом, покупка программного обеспечения для защиты от скликивания может помочь защититься от разоряющих кликов и оптимизировать рекламные кампании, чтобы увеличить конверсию и прибыль.

Из-за своей простоты скликивание может стать проблемой любого рекламодателя. Но благодаря советам, предложенным в данной книге, вы сможете его выявить и принять меры по его предотвращению.

Вот краткий список шагов, с которых вы можете начать борьбу со скликиванием:

- 1. Выявите скликивание, собирая соответствующую информацию.
- 2. Добавьте подозрительные IP-адреса в список исключений.

- 3. Настройте свой таргетинг рекламы.
- 4. Проводите ремаркетинговые кампании.
- 5. Грамотно и эффективно используйте свои пиксели для отслеживания конверсии.

Нет времени на всё это? Дело в том, что проведение кампаний в Google Ads может потребовать много времени, особенно если вы в этом деле не эксперт. Пользуясь услугами агентства, которое занимается PPC-рекламой, вы можете спать спокойно, зная, что ваши кампании обладают очень высокими показателями конверсии, а для того, чтобы не дать мошенникам скликивать вашу рекламу и опустошать ваш бюджет, используются все эффективные методы.

Как наказать мошенников?

Это сетевое мошенничество?

Можно предположить, что скликивание рекламы является мошенничеством и подпадает под статью 159.6 УК РФ (мошенничество в сфере компьютерной информацией). Это предположение формируется статьями в Интернете, где скликивание расшифровывается не иначе, как сетевое мошенничество.

Однако с юридической точки зрения скликивание не является мошенничеством, т.к. в нем отсутствует ключевой элемент мошенничества — хищение вашего имущества (совершенное с корыстной целью противоправное безвозмездное изъятие и обращение чужого имущества в пользу виновных или других лиц, причинившие ущерб собственнику). При кликфроде рекламы происходит списание денежных средств в пользу рекламной площадки (например Яндекс.Директ), а не переход имущества в пользу кликеров. А если нет хищения имущества, то нет и мошенничества!

Скликивание следует квалифицировать по статье 165 УК РФ (причинение имущественного ущерба путем обмана или злоупотребления доверием). Указанный состав преступления образуется при наличии имущественного ущерб в крупном размере (не менее 250 000 рублей), причиненного путем обмана или злоупотребления доверием. При этом под ущербом понимается не только реальный материальный ущерб, но и ваша упущенная выгода, то есть неполученные доходы (пункт 22 Постановления Пленума Верховного Суда РФ от 30.11.2017 N 48).

В результате скликивания рекламы компании причиняется имущественный ущерб. Доказать размер причиненного ущерба можно, т.к. сервисы контекстной рекламы (например Яндекс.Директ) сохраняют всю статистику вашей рекламной кампании.

Для квалификации действий по статье 165 УК РФ требуется не только наличие ущерба, но и его размер не менее 250 000 рублей. Если размер ущерба ниже указанной суммы, то к

уголовной ответственности привлечь мошенников нельзя. Их действия в таком случае будут подпадать под статью 7.27.1 КоАП РФ и это административная ответственность в виде штрафа (в размере до пятикратной стоимости причиненного ущерба, но не менее 5 000 рублей).

Для возбуждения уголовного преследования мошенников необходимо обратиться в полицию с заявлением о преступлении. Поскольку кликфрод достаточно сложное в доказывании преступление, то к заявлению нужно приложить все имеющиеся у вас доказательства, подтверждающие факт скликивание (выгрузки с нашего личного кабинета, ответы из службы технической поддержки поисковых систем, сведения об оплате контекстной рекламы, статистику рекламных компаний и т.д.). Без этих доказательных данных снижаются шансы на возбуждение уголовного дела и, соответственно, на привлечение виновных к ответственности.

Для доказывания скликивания в уголовном процессе можно использовать заключение экспертов (статьи 57,58,80 УПК РФ). Это лица (могут быть сотрудниками нашей компании) с соответствующим образованием и знаниями, которые могут провести анализ определенных показателей вашей рекламы и сделать вывод о наличии или отсутствии мошеннических кликов, их количестве и т.д.

Заключение эксперта нужно приобщить к заявлению о преступлении. Все необходимые данные от рекламной площадки (например Яндекс.Директ) могут запросить должностные лица при проверке сообщения о преступлении или расследовании уголовного дела. Стоит отметить, что проводить исследования и доказывать факт скликивания дело сложное и заниматься этим целесообразно только при крупном размере имущественного ущерба, когда ваша компания систематически теряет рекламный бюджет.

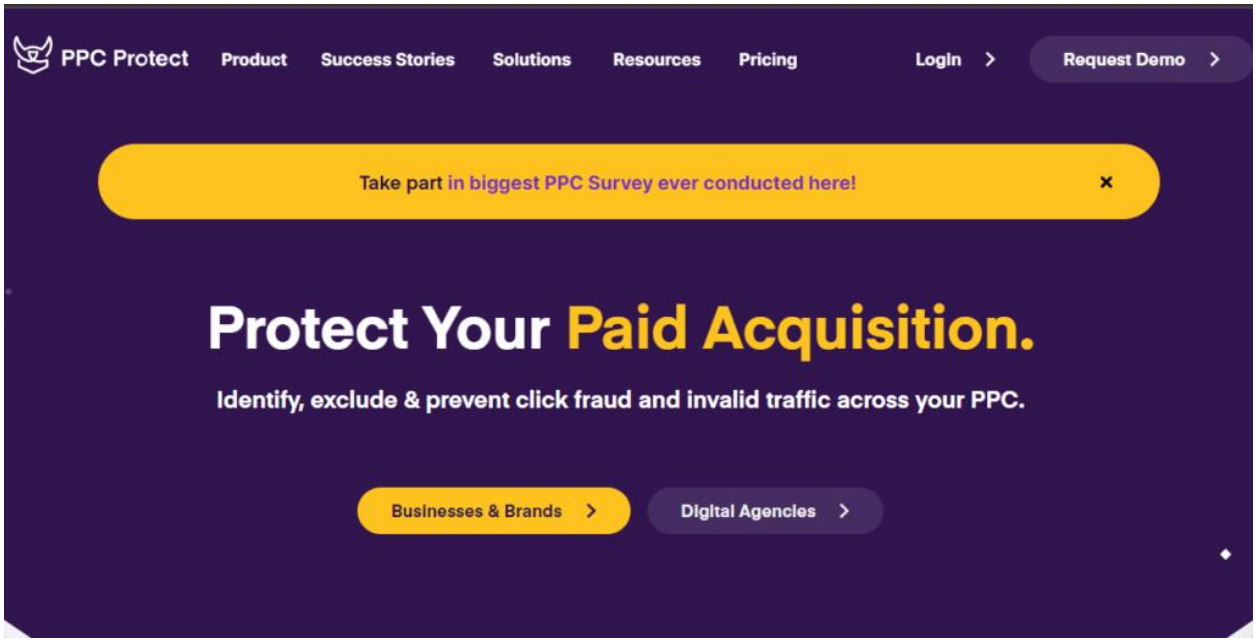
Лучшее программное обеспечение для защиты от скликивания

1. PPC Protect

PPC Protect — лучшее программное обеспечение для борьбы со скликиванием, которое помогает обнаруживать мошеннические клики, уменьшает стоимость действия (CPA) и повышает эффективность рекламы с оплатой за клик (PPC-рекламы). Вы можете наблюдать положительные результаты в пределах бюджета маркетинговой кампании. Данное программное обеспечение улучшит ваши показатели конверсии и будет ограничивать ненастоящим и неблагонадежным пользователям доступ к вашему сайту. У PPC Protect доступное ценообразование. Этот инструмент стоит $200 в месяц с ограниченным доступом к возможностям и $750 в месяц с полным доступом.

Возможности и особенности PPC Protect:

- Им очень легко начать пользоваться.
- Это экономически эффективное программное обеспечение.
- Сокращает объем работы, выполняемой вручную.
- Правильно отслеживает трафик сайтов.
- Дает хорошие результаты.
- Будет полезен рекламным агентствам.
- Защищает от скликивания рекламы, размещаемой в Google.



2. ClickGuard

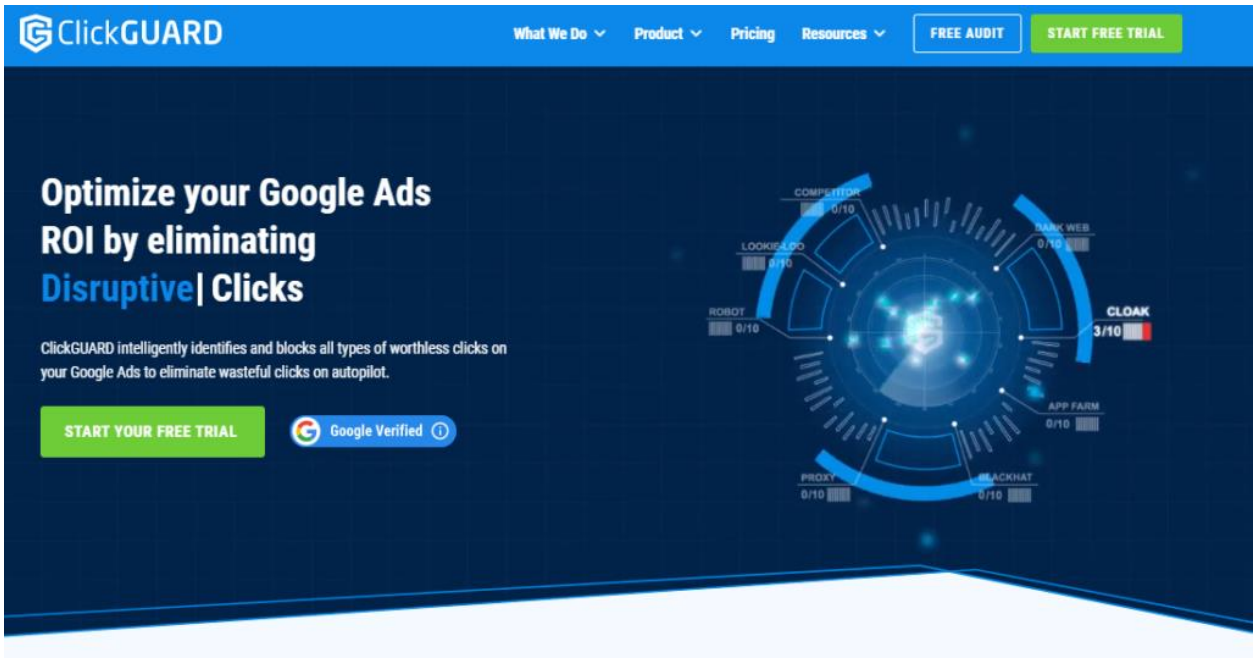
ClickGuard — программное обеспечение для борьбы со скликиванием, доступное на рынке. Цель этого программного обеспечения — не допускать того, чтобы вы впустую тратили деньги на повторные клики, которые не приносят прибыли вашей организации. Это надежное программное обеспечение, которое увеличивает отдачу от PPC-рекламы. Оно предотвращает противоправные действия и нажатия по ссылке на сайт.

Ценообразование ClickGuard разделяется на три категории, которые отличаются друг от друга по возможностям и количеству предоставляемых услуг:

1. $59 в месяц.
2. $79 в месяц.
3. $99 в месяц.

Возможности и особенности ClickGuard:

- Это программное обеспечение можно настраивать под себя.
- К функциям удобно обращаться.
- Удаляет повторные клики.
- Экономит деньги, направляемые на рекламу с оплатой за клик.
- Достойная служба поддержки пользователей.
- Аналитика данных и полезные результаты, которые она позволяет получить.



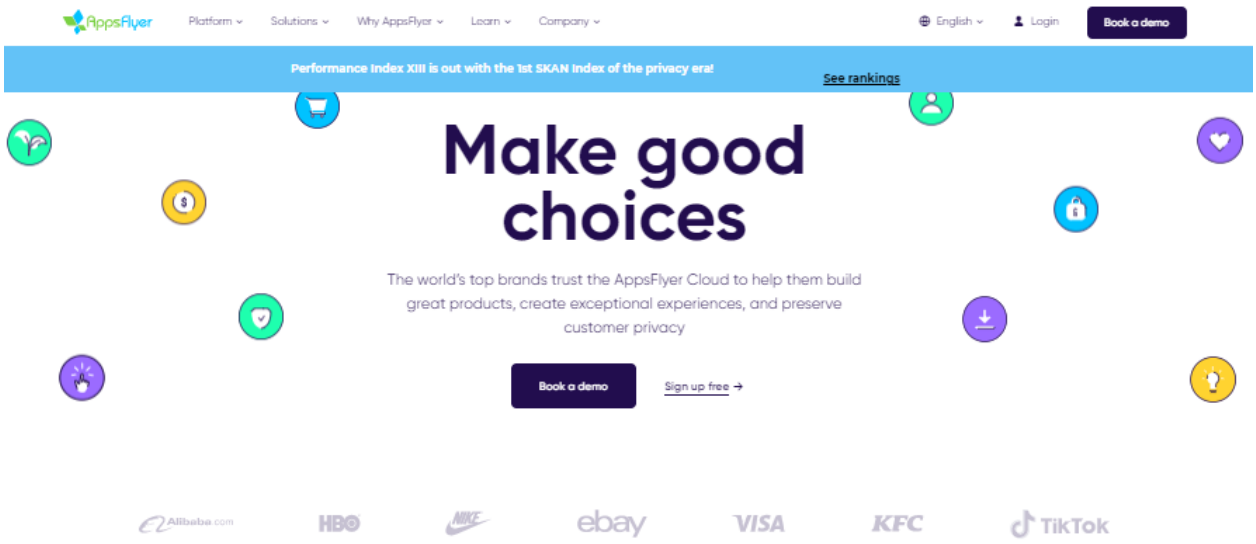
3. AppsFlyer

Это программное обеспечение для борьбы со скликиванием рекламы на Google следит за всеми, кто приходит на ваш сайт, кликая на рекламу. AppsFlyer создан для удержания нормальных кликов и отбрасывания повторных кликов путем наблюдения за трафиком. В этом программном обеспечении используется технология защиты от скликивания рекламы в Google. Кроме того, в настоящее время оно используется известными брендами. Некоторые сталкиваются с проблемами, связанными с ценообразованием AppsFlyer. К тому же предварительный просмотр контента, доступного в мобильном приложении, не поддается оценке.

Возможности и особенности AppsFlyer:

- Предоставляет достоверные измерения.
- Потрясающие надежные выводы, полученные в результате анализа данных.
- В реальном времени обновляет данные.

- Обширный функционал.
- Защитит ваш бюджет от скликивания.
- Полезен для рекламодателей.



4. ClickCease

ClickCease — еще одно удивительное программное средство, которое защитит вас от мошеннических кликов. Удобство работы и отличная поддержка пользователей — важные особенности этого программного обеспечения. Это недорогое программное обеспечение, которое предоставит вашему сайту защиту от мошеннических действий. ClickCease будет экономить деньги и защищать вас от мошеннических кликов. ClickCease не ударит по вашему карману. Предлагается два тарифных плана: стандартный пакет услуг стоимость $50 и профессиональный пакет стоимостью $75.

Возможности и особенности ClickCease:

- Им легко управлять.
- Мощная возможность «Междоменная блокировка IP-адресов» (cross-domain blocking).
- Пригодится рекламодателям, размещающим рекламу в Google.
- Отслеживает IP-адреса, чтобы блокировать нежелательных пользователей.
- Прост в настройке.
- Отслеживает релевантные ключевые слова.

5. Clixtell

Clixtell внимательно проверяет посетителей сайта. Он отделяет настоящие клики по вашей рекламе от поддельных. Это и делает его одним из лучших программных решений для борьбы со скликиванием. Инструмент для защиты от скликивания Clixtell позволит вам обезопасить ваш бюджет, выделяемый на рекламу с оплатой за клик. Он защитит ваши рекламные объявления не только в Google, но и в Bing. Clixtell — автоматизированное программное обеспечение для борьбы со скликиванием, при разработке которого особое внимание уделяли удобству использования.

Возможности и особенности Clixtell:

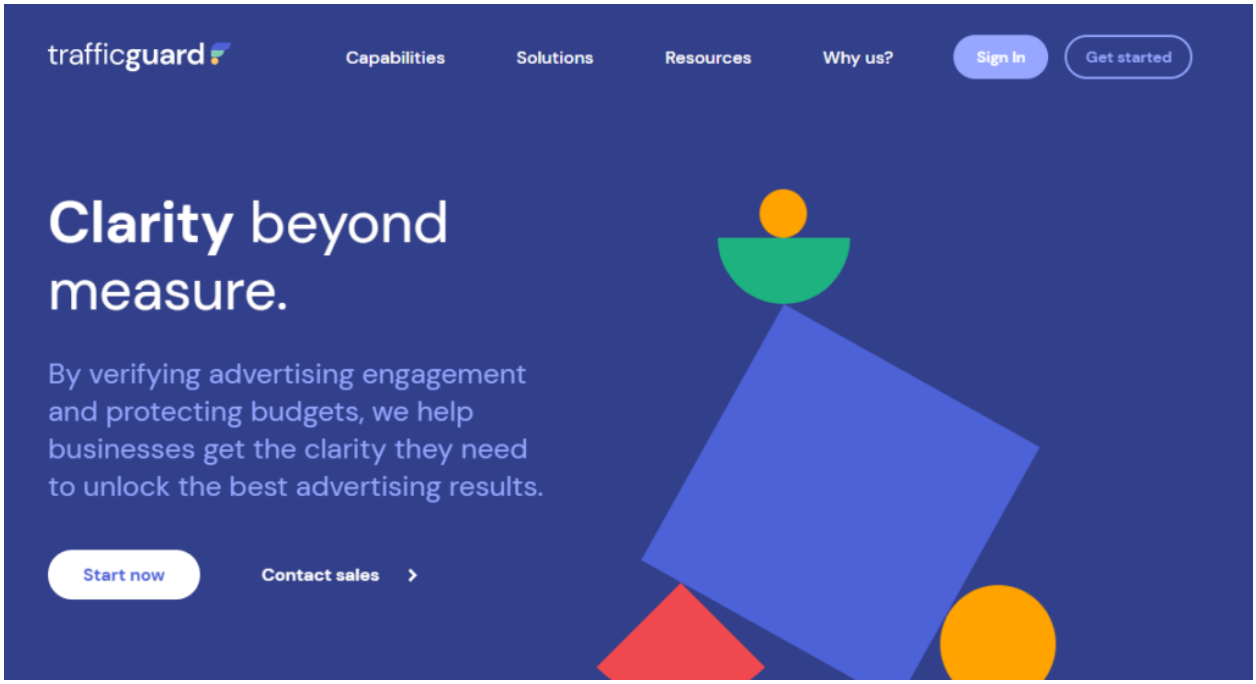
- Предоставляет бесплатный период использования.
- Незамедлительно разбирается с мошенниками.
- Действует быстро.
- Работает без задержек и сбоев.
- Услуги стоят тех денег, которые за них просят.
- Защитит ваши маркетинговые кампании.
- Позволяет улучшить показатели конверсии.
- Великолепно обнаруживает скликивание.

6. TrafficGuard

Это многоязычное программное обеспечение для борьбы со скликиванием рекламы в Google предлагает лучшие услуги по защите от мошеннических кликов. Защита PPC-рекламы от TrafficGuard подходит для компаний любого размера и рекламных кампаний в Google. Это программное обеспечение автоматически блокирует мошенников и оберегает ваши деньги, чтобы они не тратились впустую на мошеннические клики. Оно поможет вашей компании привлекать обычных, настоящих пользователей, а значит соответствующим образом продвигать ваши продукты и услуги. TrafficGuard предлагает мало возможностей, но эти возможности качественные.

Возможности и особенности TrafficGuard:

- В данном программном обеспечении реализована внушительная система безопасности.
- Подходит для любых крупных и мелких компаний.
- Данные просматриваются и обновляются в реальном времени.
- Повышает показатели конверсии, защищая вашу рекламу от скликивания.

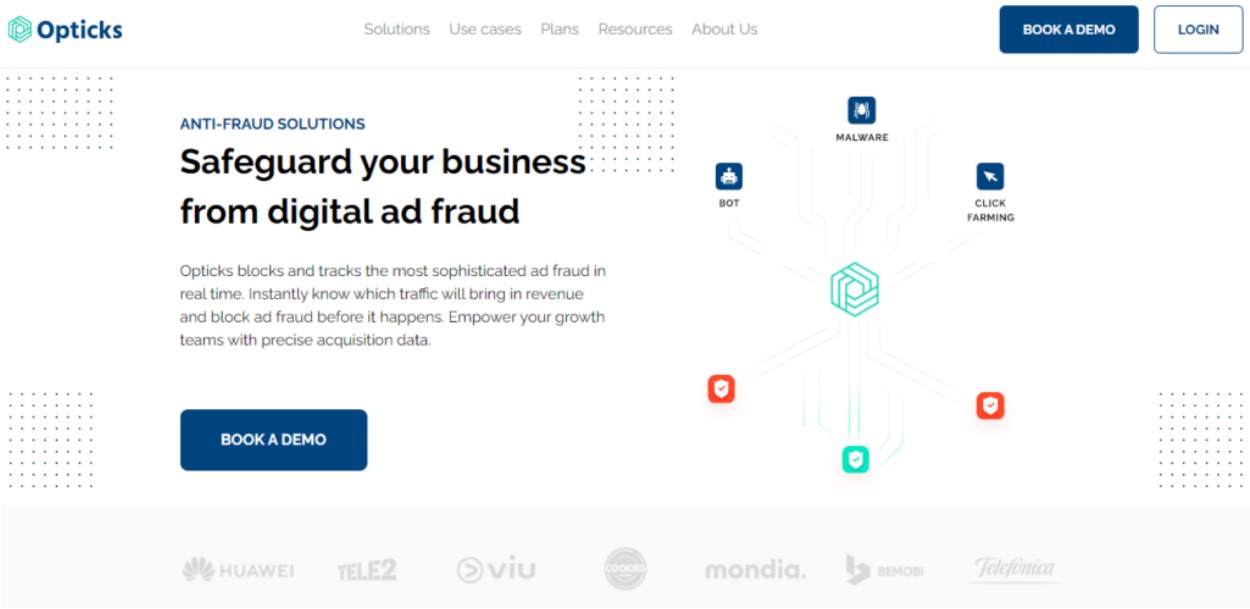


7. Opticks

Opticks — еще одно из наиболее «умных» и качественных программных решений, предназначенное для компаний, маркетологов и рекламодателей. Оно управляется искусственным интеллектом и без промедления вносит в черный список сомнительные и совершающие повторные клики IP-адреса. Для многих компаний это программное обеспечение становится очевидно лучшим вариантом благодаря тому, что оно работает плавно и точно.

Возможности и особенности Opticks:

- Разработано таким образом, чтобы у пользователей было как можно меньше трудностей.
- Позволит увеличивать ваши расходы на рекламу без опасений, связанных со скликиванием.
- Не допускает ложные срабатывания при обнаружении скликивания и предоставляет надежные результаты.
- Можно легко разобраться в том, как им пользоваться.
- Эффективная система поддержки пользователей.
- Доступны возможности пользовательской настройки.

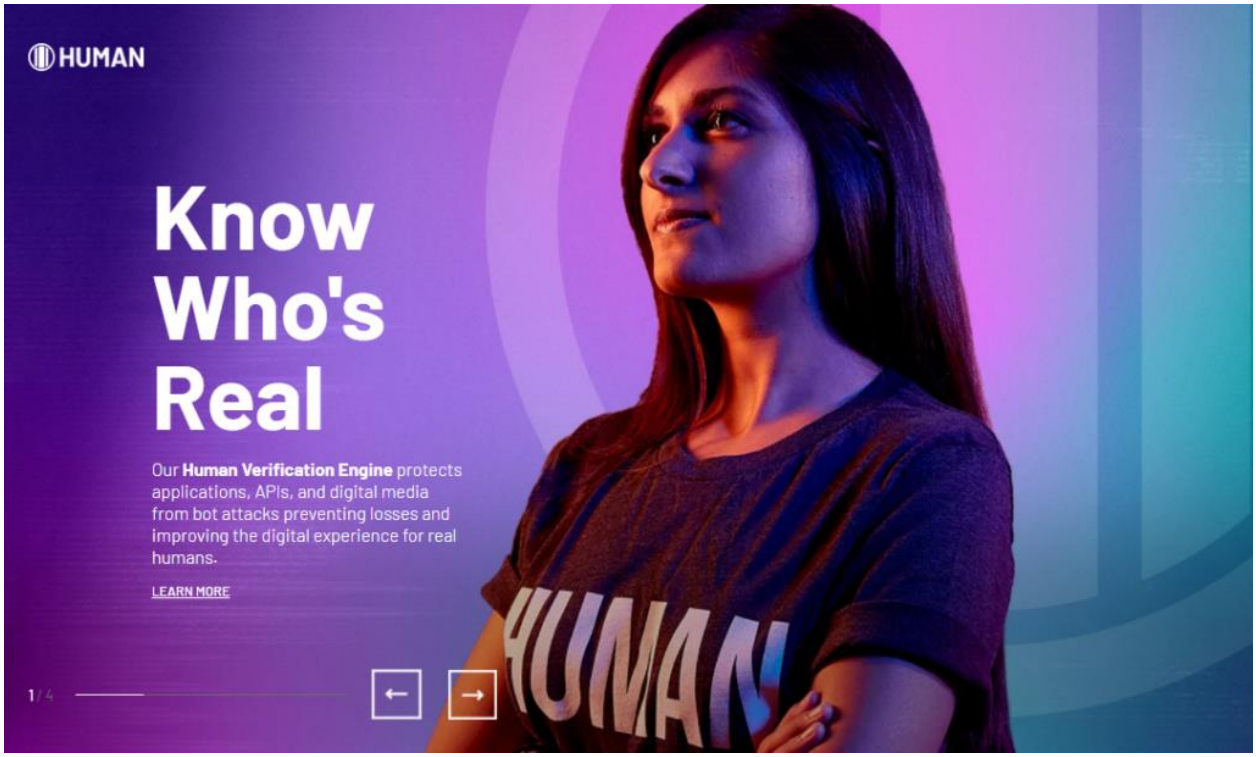


8. Human

Human — программное обеспечение для борьбы со скликиванием, которое используется перспективными компаниями, стремительно развивающимися при помощи рекламы в Google и Bing. Эта компания обладает самой продвинутой системой проверки поведения пользователей на схожесть с человеческим поведением, то есть это программное обеспечение может выявлять автоматические повторные клики по вашей рекламе, цель которых — снизить приоритет вашей кампании, а также подорвать ваш бюджет кампании и помешать вам достичь поставленной цели.

Возможности и особенности Human:

- Защищает вашу компанию от атак ботов.
- У пользователей не будет проблем с языковым барьером. Поддерживает множество языков.
- На данное программное обеспечение крайне положительные отзывы.
- Служба поддержки оперативно реагирует на обращения.
- Интерфейс и вся система удобны в использовании.

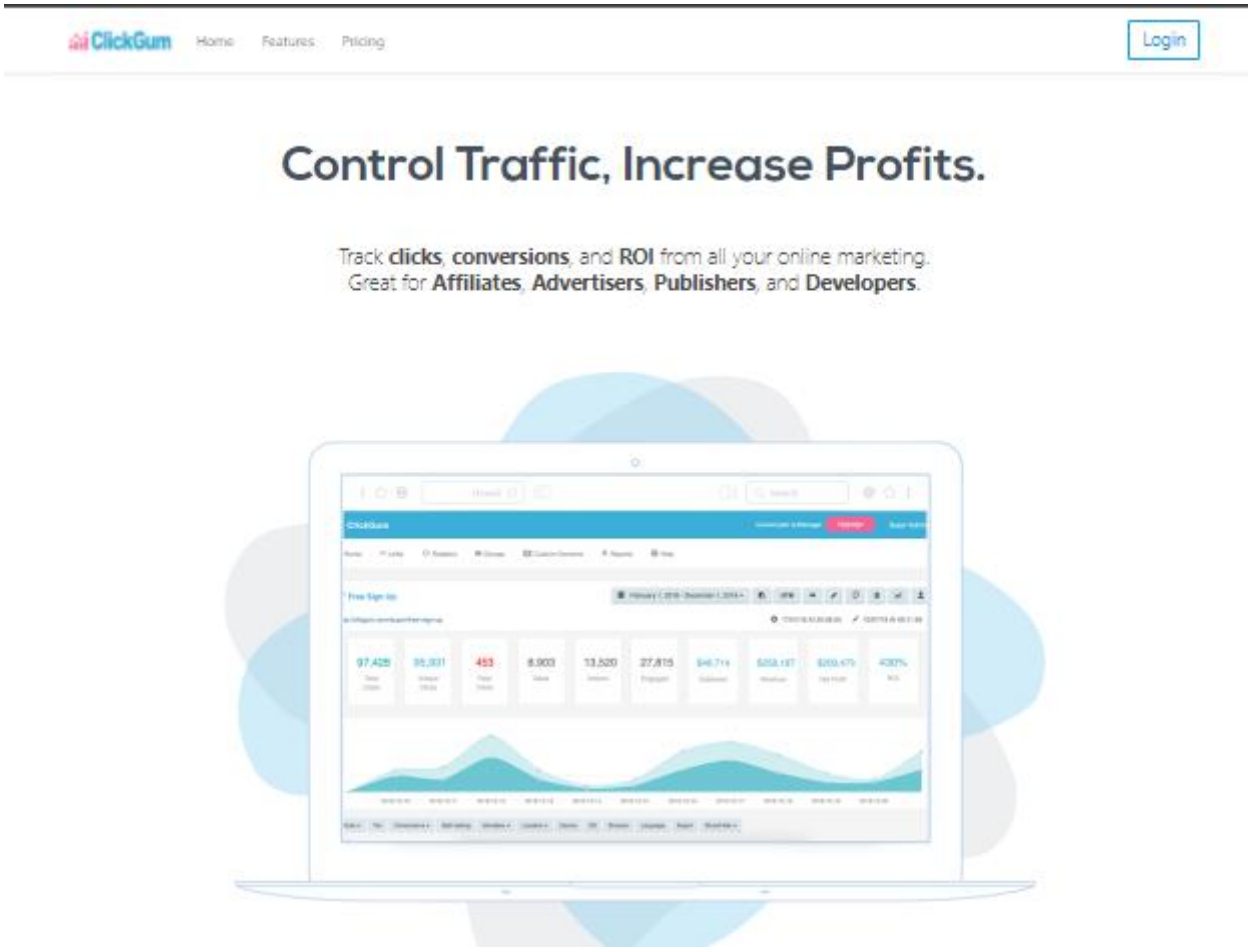


9. ClickGum

Это программное обеспечение контролирует трафик, поступающий на вашу рекламу, и увеличивает вашу выручку. ClickGum отслеживает и контролирует все источники трафика, а также удаляет ненадежные и подставные IP-адреса. Данное программное обеспечение для обнаружения скликивания предназначено для того, чтобы оптимизировать ваши маркетинговые кампании и отбирать лучшие из них. Эту работу и делает ClickGum для своих клиентов.

Возможности и особенности ClickGum:

- На профессиональном уровне управляйте своей кампанией PPC-рекламы.
- Следите за показателями конверсии.
- Это программное решение также можно использовать в email-маркетинге и маркетинговых кампаниях в социальных медиа.
- Отличные отзывы от пользователей.
- Вводит вас в курс дела, показывая, откуда приходят пользователи, которые становятся вашими покупателями.
- Помогает вам планировать маркетинговую кампанию и эффективнее настраивать таргетинг.

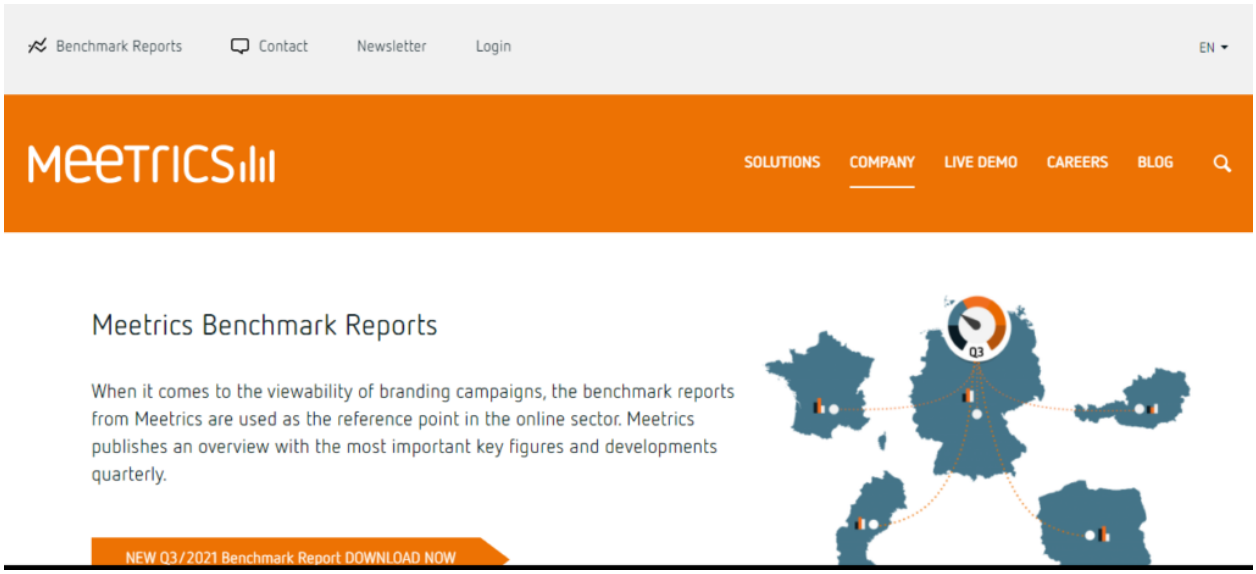


10. Meetrics

Meetrics на постоянной основе отслеживает аудиторию вашей рекламы и без промедления реагирует на мошеннические клики. Этот инструмент наблюдает за аудиторией вашего бренда и в реальном времени предоставляет вам обновления о ее состоянии. Данное программное обеспечение работает эффективно. Оно акцентирует внимание на безопасности и образе бренда. Кроме того, разработчики стремились к тому, чтобы их продукт давал впечатляющие результаты своим пользователям. Хотя Meetrics ориентирован на результат, этот инструмент поначалу сложно понять.

Возможности и особенности Meetrics:

- Контролирует вашу CPC (стоимость за клик).
- Заботится о бюджете вашей кампании.
- Разработан с использованием эффективных и профессиональных технологий.
- Обучает пользователей при помощи событий в реальном времени.



11. Forensiq

Forensiq — еще один потрясающий инструмент для контроля над скликиванием рекламы и защиты ваших объемов рекламы. Это один из лучших вариантов программного обеспечения для защиты от скликивания. Вы можете отправлять данные о скликивании в аналитику Google, и компания вернет вам потраченные из-за мошеннических кликов деньги. Именно так выглядит этот процесс. Также этот инструмент предоставляет данные о том, завершил ли посетитель нужные вам действия. Forensiq позволяет прорабатывать или оптимизировать вашу компанию при помощи машинного обучения.

Возможности и особенности Forensiq:

- Предоставляет своим клиентам ожидаемые результаты.
- Очень активная служба поддержки.
- Этим программным обеспечением просто пользоваться.
- Простой и понятный пользовательский интерфейс.
- В системе применяются новейшие технологии.
- Используется продвинутая технологическая система выявления скликивания.

Далее представлен список всех упомянутых выше программных решений вместе со средней оценкой пользователей. Взгляните:

Наименование решения	Оценка*
PPC Protect	4.8/5
ClickGuard	4.7/5
AppsFlyer	4.4/5
ClickCease	4.5/5
Clixtell	4.9/5
TrafficGuard	4.1/5
Opticks	4.9/5
Human	4.8/5
ClickGum	4.9/5
Meetrics	4.8/5
Forensiq	4.8/5

*по отзывам пользователей

Часто задаваемые вопросы

Как предотвратить скликивание?

Есть разные способы защиты от скликивания. Прежде всего, тщательно следите за своими рекламными кампаниями и данными. Если вы следите за тем, кто и как часто кликает по вашей рекламе, это поможет вам выявлять клики, характеризующиеся слабым желанием что-то у вас купить, ботов, интернет-серферов и конкурирующие с вами компании, которые хотят, чтобы вы потратили свой рекламный бюджет впустую. Будьте бдительны и следите за своими рекламными объявлениями! Если вы что-нибудь заподозрили, всегда полезно провести проверку.

Еще один отличный способ предотвращения скликивания — купить подписку на соответствующее программное обеспечение. На рынке представлено несколько различных вариантов программного обеспечения.

Как Google Ads (Adwords) противодействует скликиванию?

Google — гигант в сфере программного обеспечения, поэтому у этой компании есть методы предотвращения скликивания и снижения противозаконной деятельности, связанной с рекламными объявлениями. Google, например, использует алгоритм закупки рекламы, который должен обнаруживать и отфильтровывать недействительные клики еще до того, за них будет выставлен счет. Хотя так бывает не всегда, Google признает, что недействительный трафик — это проблема, и рекламодатели должны знать о нем и разработать стратегию защиты от скликивания.

В Google также есть команда специалистов по фильтрации трафика — они отслеживают мошенническую активность в режиме реального времени. Будь то поднастройка алгоритма, чтобы отвести мошеннические клики от вашего объявления, или блокировка всех кликов, команда Google активно работает над фильтрами, чтобы обеспечить защиту ваших рекламных кампаний. Кроме того, чем чаще используются фильтры, тем умнее они становятся.

Google также отлично справляется с предотвращением скликивания. Если активность мошенников связана с каким-либо IP-адресом или у издателя интернет-рекламы крайне подозрительный показатель CTR, то Google предотвратит недействительные клики, чтобы вам не пришлось за них платить. Google без колебаний отключит учетные записи, связанные с большим количеством недействительного трафика.

Хотя большинство случаев скликивания совершается людьми, за некоторыми стоят боты. Поэтому Google будет искать аномалии в данных и образцы инородного программного

кода, а также постоянно исследовать новые виды недействительного трафика, которые существующий алгоритм или фильтр пока не может обнаружить.

Скликивание и закон РФ

Является ли скликивание преступлением? Если это преступление, то по какой статье закона РФ можно привлечь злоумышленника?

Это сетевое мошенничество?

Можно предположить, что скликивание рекламы является мошенничеством и подпадает под статью 159.6 УК РФ (мошенничество в сфере компьютерной информацией). Это предположение формируется статьями в Интернете, где скликивание расшифровывается не иначе, как сетевое мошенничество.

Однако с юридической точки зрения скликивание не является мошенничеством, т.к. в нем отсутствует ключевой элемент мошенничества — хищение вашего имущества (совершенное с корыстной целью противоправное безвозмездное изъятие и обращение чужого имущества в пользу виновных или других лиц, причинившие ущерб собственнику). При кликфроде рекламы происходит списание денежных средств в пользу рекламной площадки (например Яндекс.Директ), а не переход имущества в пользу кликеров. А если нет хищения имущества, то нет и мошенничества!

Скликивание следует квалифицировать по статье 165 УК РФ (причинение имущественного ущерба путем обмана или злоупотребления доверием). Указанный состав преступления образуется при наличии имущественного ущерб в крупном размере (не менее 250 000 рублей), причиненного путем обмана или злоупотребления доверием. При этом под ущербом понимается не только реальный материальный ущерб, но и ваша упущенная выгода, то есть неполученные доходы (пункт 22 Постановления Пленума Верховного Суда РФ от 30.11.2017 N 48).

В результате скликивания рекламы компании причиняется имущественный ущерб. Доказать размер причиненного ущерба можно, т.к. сервисы контекстной рекламы (например Яндекс.Директ) сохраняют всю статистику вашей рекламной кампании.

Для квалификации действий по статье 165 УК РФ требуется не только наличие ущерба, но и его размер не менее 250 000 рублей. Если размер ущерба ниже указанной суммы, то к уголовной ответственности привлечь мошенников нельзя. Их действия в таком случае будут подпадать под статью 7.27.1 КоАП РФ и это административная ответственность в

виде штрафа (в размере до пятикратной стоимости причиненного ущерба, но не менее 5 000 рублей).

Для возбуждения уголовного преследования мошенников необходимо обратиться в полицию с заявлением о преступлении. Поскольку кликфрод достаточно сложное в доказывании преступление, то к заявлению нужно приложить все имеющиеся у вас доказательства, подтверждающие факт скликивание (выгрузки с нашего личного кабинета, ответы из службы технической поддержки поисковых систем, сведения об оплате контекстной рекламы, статистику рекламных компаний и т.д.). Без этих доказательных данных снижаются шансы на возбуждение уголовного дела и, соответственно, на привлечение виновных к ответственности.

Для доказывания скликивания в уголовном процессе можно использовать заключение экспертов (статьи 57,58,80 УПК РФ). Это лица (могут быть сотрудниками нашей компании) с соответствующим образованием и знаниями, которые могут провести анализ определенных показателей вашей рекламы и сделать вывод о наличии или отсутствии мошеннических кликов, их количестве и т.д.

Заключение эксперта нужно приобщить к заявлению о преступлении. Все необходимые данные от рекламной площадки (например Яндекс.Директ) могут запросить должностные лица при проверке сообщения о преступлении или расследовании уголовного дела. Стоит отметить, что проводить исследования и доказывать факт скликивания дело сложное и заниматься этим целесообразно только при крупном размере имущественного ущерба, когда ваша компания систематически теряет рекламный бюджет.

Скликивание противозаконно?

Сложно сказать. В большинстве стран существуют законы о конфиденциальности, кибербезопасности и даже информационных технологиях, но иногда трудно пробраться сквозь дебри юридической терминологии и понять, противозаконно ли скликивание.

Когда речь идет о законе, скликивание обычно не рассматривается обособленно — на самом деле оно связано с отмыванием денег (как в случае с Methbot), электронным мошенничеством, кражей данных, обманом и так далее. Поскольку эти виды мошенничества идут рука об руку, бывает трудно определить, какое преступление на самом деле рассматривается.

В Соединенных Штатах было рассмотрено несколько дел о скликивании. Есть несколько громких и малоизвестных дел, в которых фигурировали такие крупные технологические компании, как Google и Yahoo, хотя эти иски закончились урегулированием, а не изменением законодательной базы.

Так считается ли скликивание противозаконным? Ответ зависит от того, где вы находитесь. Однако лучше всего проявлять осторожность и вообще не заниматься им.

Как количественно оценить скликивание?

Скликивание можно и нужно количественно оценивать с помощью программного обеспечения, предназначенного для защиты от скликивания.

Может ли программное обеспечение остановить или предотвратить скликивание?

Да, может! Как уже говорилось выше, есть несколько программных решений, позволяющих предотвратить и даже остановить скликивание.

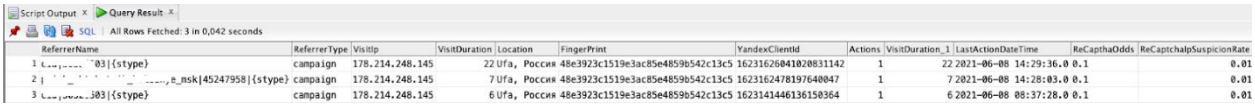
КЕЙС №1

Давайте детально изучим, как происходит скликивание рекламы на небольшом сайте и почему важно использовать все механизмы защиты.

Мы подготовили данный кейс (точнее, это даже анти-кейс) по одному из наших клиентов, которому мы подключили защиту от скликивания рекламы. Почему анти-кейс? Дело в том, что мы предлагаем несколько степеней защиты, но клиент, к нашему сожалению, выбрал только один вариант и, как вы поймете ниже, боты все еще «съедают» его рекламный бюджет. Мы решили, что будет честно публиковать не только успешный «успех», а делится вообще нашими наблюдениями в части скликивания.

Ввиду того, что мы не можем раскрывать данные наших клиентов, мы удалили с изображений ниже часть данных, но поверьте, что для понимания масштаба скликивания, это будет не критично.

Итак, начали? Давайте сразу посмотрим на изображение ниже (можно увеличить по клику). Это фрагмент из нашей внутренней базы данных, где фиксируются в режиме онлайн все визиты пользователей на сайты клиентов.


Script Output | Query Result

All Rows Fetched: 3 in 0,042 seconds

	ReferrerName	ReferrerType	VisitIp	VisitDuration	Location	FingerPrint	YandexClientId	Actions	VisitDuration_1	LastActionDateTime	ReCapthaOdds	ReCaptchaIpSuspicionRate
1	[illegible]03|{stype}	campaign	178.214.248.145	22	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623162604102083114 2	1	22	2021-06-08 14:29:36.0	0.1	0.01
2	[illegible]e_msk|45247958|{stype}	campaign	178.214.248.145	7	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623162478197640047	1	7	2021-06-08 14:28:03.0	0.1	0.01
3	[illegible]03|{stype}	campaign	178.214.248.145	6	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623141446136150364	1	6	2021-06-08 08:37:28.0	0.1	0.01

Что тут видно? На сайт клиента было сделано 3 захода (визита) с одного IP- адреса (вот этот адрес 178.214.248.145) в один день (8 июня 2021 года). При этом каждый визит пользователя содержал **одно** действие (Actions) и длительность первых двух была порядка **6 секунд**, третий 22 секунды. Источник определялся как город Уфа, оператор связи https://www.ufanet.ru/.

Почему именно это привлекло наше внимание и легло в основу кейса? Дело в том, что наша система защиты от скликивания считает цифровой отпечаток браузера, с которого был выполнен заход. И в данном случае он одинаковый (поле FingerPrint на изображении выше). Вот он:

48e3923c1519e3ac85e4859b542c13c5

«Цифровой отпечаток браузера» — это механизм, используемый сайтами и сервисами для отслеживания посетителей. Пользователям присваивается уникальный идентификатор (отпечаток). Он содержит много информации о настройках и возможностях браузера пользователей, что используется для их идентификации.

Согласно результатам исследований, уникальность отпечатка браузера очень высока. Если говорить о статистике, то только раз на ~300 000 случаев случается полное совпадение отпечатков браузеров двух разных пользователей. Исходя из этого, мы можем с высокой вероятностью предположить, что по рекламе в нашем рассматриваемом кейсе кликал один пользователь (дальше будем называть его бот, хотя допускаем, что это был человек, которые вручную скликивал рекламу).

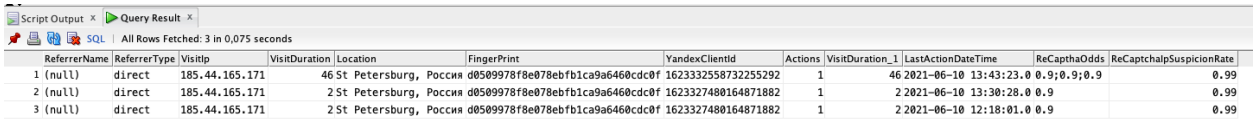
Итак, что мы имеем? Бот в этот день кликнул три раза на рекламу в Яндекс.Директ, у него был в каждом случае один IP — адрес, один отпечаток браузера и … разные Яндекс.ClientID (поле YandexClientID на изображении выше).

Обратите внимание на поле reCaptchaOdd с значением 0.1, мы чуть позже обязательно вернемся к этому, т.к. данное значение на 99% подтверждает наше подозрение, что это бот.

Что такое Яндекс.ClientID?

ClientID — это анонимный идентификатор, который Яндекс.Метрика автоматически присваивает каждому уникальному посетителю сайта. Идентификатор создается случайным образом и определяет браузер, в котором посетитель просматривает ваш сайт. Если бот заходил на один и тот же сайт, например, с помощью Google Chrome и Opera, в Яндекс.Метрике будет зафиксировано два разных ClientID.

В нашем случае Яндекс.Метрика выдавала каждый раз разные ClientID одному пользователю-боту. Почему так? Чтобы ответить на этот вопрос, мы провели простой эксперимент, и вы легко можете повторить его сами. Наш сотрудник зашел на один и тот же сайт напрямую три раза с одного ПК (рабочий ПК). Первые два раза он зашел с одного браузера с интервалом в один час, третий раз — он открыл браузер в режиме «инкогнито».



Script Output | Query Result

SQL | All Rows Fetched: 3 in 0,075 seconds

	ReferrerName	ReferrerType	VisitIp	VisitDuration	Location	FingerPrint	YandexClientId	Actions	VisitDuration_1	LastActionDateTime	ReCapthaOdds	ReCaptchaIpSuspicionRate
1	(null)	direct	185.44.165.171	46	St Petersburg, Россия	d0509978f8e078ebfb1ca9a6460cdc0f	1623332558732255292	1	46	2021-06-10 13:43:23.0	0.9;0.9;0.9	0.99
2	(null)	direct	185.44.165.171	2	St Petersburg, Россия	d0509978f8e078ebfb1ca9a6460cdc0f	1623327480164871882	1	2	2021-06-10 13:30:28.0	0.9	0.99
3	(null)	direct	185.44.165.171	2	St Petersburg, Россия	d0509978f8e078ebfb1ca9a6460cdc0f	1623327480164871882	1	2	2021-06-10 12:18:01.0	0.9	0.99

Яндекс.Метрика корректно определила повторной заход (мы специально выждали час, чтобы закрыть сессию) и присвоила одинаковые ClientID. А в третий раз (13.43) из-за режима «инкогнито» был сгенерирован новый ClientID и для Яндекс.Метрика это по сути новый пользователь.

Возвращаясь к кейсу. С очень высокой вероятностью можно предположить, что скликивание осуществлялось каждый раз с очисткой cookies браузера, чтобы Яндекс.Метрика вновь индентифицировала пользователя как нового. Зачем? Чтобы данные клики учитывались и средства с бюджета Яндекс.Директ клиента списывались.

Уникальный идентификатор конфигураций веб-браузера и операционной системы, который формируется на основе собранных данных различными технологиями отслеживания. При этом не используются традиционные методы отслеживания, такие как IP адреса и уникальные файлы cookie.

Цифровой отпечаток браузера имеет вид 32-битного числа шестнадцатеричной системы типа b2cf59b36581399ebf54d4ab425ac4a7, которое получается в результате обработки всех принятых от браузера данных. Полученный отпечаток браузера позволяет отслеживать пользователей в сети Интернет с точностью до 94%.

Давайте посмотрим, как часто пользователь с указанным «цифровым отпечатком» заходил на данный сайт вообще (по рекламе и нет). Посмотрите на изображение ниже. Это данные за один день. Видно, что заходы происходят постоянно.

Script Output | Query Result

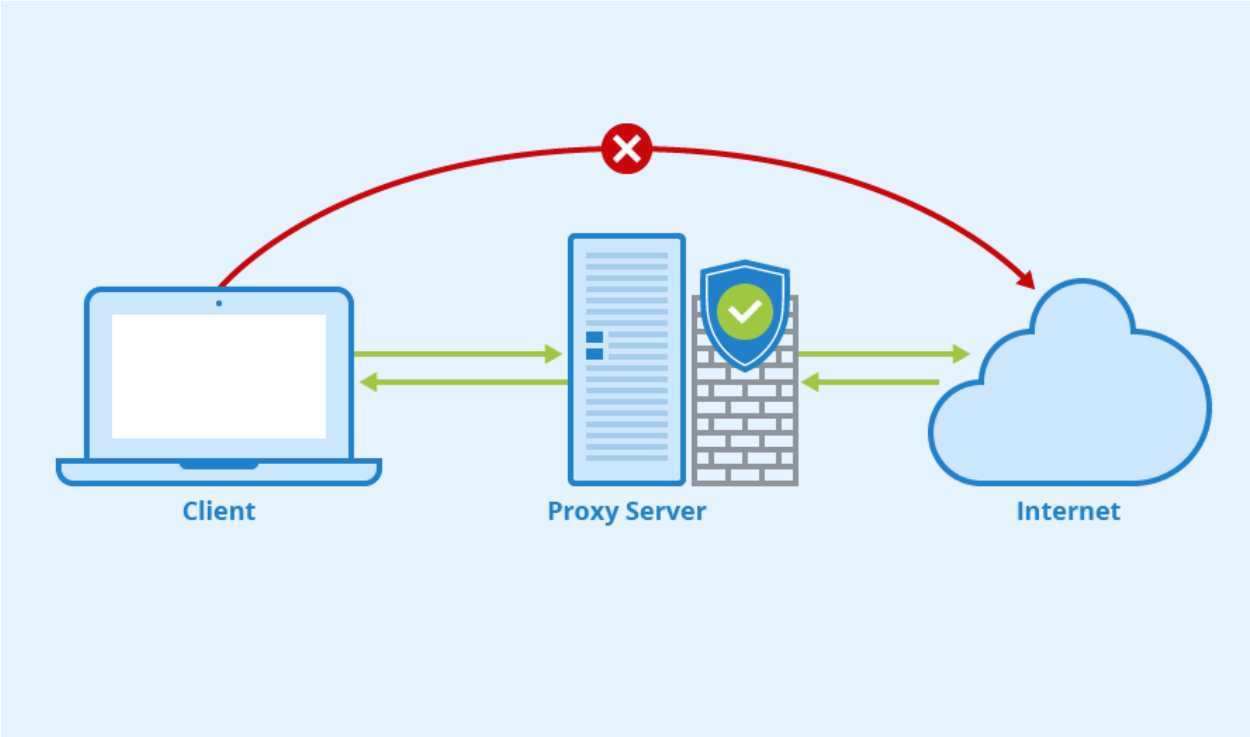
SQL | Fetched 50 rows in 0,087 seconds

	ReferrerName	ReferrerType	VisitIp	VisitDuration	Location	FingerPrint	YandexClientId	Actions	VisitD...	LastActionDateTime	ReCaptha...	ReCaptch...
1	c	campaign	5.206.61.97	14	Kopeysk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623322837800785785	1	14	2021-06-10 11:00:30.0	0.1	0.01
2	p |{stype}	campaign	46.191.137.253	6	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623322820103900838 7	1	6	2021-06-10 11:00:19.0	0.1;0.1	0.01
3	c	campaign	5.3.252.26	5	Saratov, Россия	48e3923c1519e3ac85e4859b542c13c5	1623322804486787588	1	5	2021-06-10 11:00:00.0	0.1	0.01
4	c	campaign	94.28.183.41	10	Tula, Россия	48e3923c1519e3ac85e4859b542c13c5	1623322000376189784	1	10	2021-06-10 10:46:43.0	0.1	0.01
5	p {stype}	campaign	178.214.246.55	9	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	(null)	1	9	2021-06-10 10:46:15.0	0.1	0.01
6	p 7903|{stype}	campaign	5.206.61.97	13	Kopeysk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321973313000149	1	13	2021-06-10 10:46:13.0	0.1	0.01
7	p 7903|{stype}	campaign	178.214.255.221	13	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321978218779735	1	13	2021-06-10 10:46:08.0	0.1	0.01
8	c	campaign	5.165.217.208	9	Yaroslavl, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321976432886320	1	9	2021-06-10 10:46:07.0	0.1	0.01
9	p {stype}	campaign	77.222.96.104	7	Chelyabinsk, Россия	48e3923c1519e3ac85e4859b542c13c5	(null)	1	7	2021-06-10 10:46:05.0	0.1	0.01
10	c	campaign	5.166.212.170	4	Nizhniy Novgorod, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321974230361682	1	4	2021-06-10 10:46:03.0	0.1	0.01
11	p 7903|{stype}	campaign	5.227.15.18	11	Dzerzhinsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321951286446085	1	11	2021-06-10 10:45:44.0	0.1	0.01
12	c	campaign	5.3.252.26	6	Saratov, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321956151122309	1	6	2021-06-10 10:45:39.0	0.1	0.01
13	c	campaign	136.169.243.255	5	Orenburg, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321923192846893	1	5	2021-06-10 10:45:30.0	0.1	0.01
14	p {stype}	campaign	46.191.233.120	4	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	(null)	1	4	2021-06-10 10:45:28.0	0.1	0.01
15	r ext	campaign	5.165.75.58	6	Voronezh, Россия	48e3923c1519e3ac85e4859b542c13c5	1623321724594323718	1	6	2021-06-10 10:41:50.0	0.1	0.01
16	(	direct	37.232.138.172	3	Cheboksary, Россия	48e3923c1519e3ac85e4859b542c13c5	1623309143209871478	1	3	2021-06-10 07:12:19.0	0.1	0.01
17	(	direct	95.79.86.15	4	Nizhniy Novgorod, Россия	48e3923c1519e3ac85e4859b542c13c5	1623309080616374919	1	4	2021-06-10 07:11:58.0	0.1	0.01
18	(	direct	176.214.2.140	5	Omsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623309110479066350	1	5	2021-06-10 07:11:54.0	0.1	0.01
19	p |{stype}	campaign	5.129.3.8	4	Novosibirsk, Россия	48e3923c1519e3ac85e4859b542c13c5	(null)	1	4	2021-06-10 06:56:55.0	0.1	0.01
20	p |{stype}	campaign	94.28.183.41	3	Tula, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308196840366581	1	3	2021-06-10 06:56:51.0	0.1	0.01
21	c	campaign	46.191.137.253	4	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308228422580862	1	4	2021-06-10 06:56:48.0	0.1	0.01
22	c	campaign	5.128.67.145	4	Novosibirsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308230943861175	1	4	2021-06-10 06:56:48.0	0.1	0.01
23	c	campaign	5.165.214.175	8	Tomsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308192936527306	1	8	2021-06-10 06:56:21.0	0.1	0.01
24	p 7903|{stype}	campaign	5.3.254.132	5	Saratov, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308176339065 56	1	5	2021-06-10 06:56:12.0	0.1	0.01
25	c	campaign	77.222.96.104	3	Chelyabinsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308192171776441	1	3	2021-06-10 06:56:11.0	0.1	0.01
26	p 5|{stype}	campaign	176.226.244.79	3	Chelyabinsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308174676865009	1	3	2021-06-10 06:56:11.0	0.1	0.01
27	p 5|{stype}	campaign	5.128.67.145	2	Novosibirsk, Россия	48e3923c1519e3ac85e4859b542c13c5	1623308187759324669	1	2	2021-06-10 06:56:09.0	0.1	0.01
28	Y	search	178.214.255.221	4	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623307041885687854	1	4	2021-06-10 06:37:17.0	0.1	0.01
29	p |{stype}	campaign	185.4.204.53	4	Ekaterinburg, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304801514860269	1	4	2021-06-10 05:59:32.0	0.1	0.01
30	p |{stype}	campaign	178.214.246.55	2	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304772106370060 3	1	2	2021-06-10 05:59:15.0	0.1	0.01
31	c	campaign	46.191.233.120	4	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304771268661032	1	4	2021-06-10 05:59:15.0	0.1	0.01
32	p 7903|{stype}	campaign	178.214.247.159	7	Ufa, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304769281264 16	1	7	2021-06-10 05:59:10.0	0.1	0.01
33	c	campaign	95.79.89.59	3	Nizhniy Novgorod, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304745146305241	1	3	2021-06-10 05:59:08.0	0.1	0.01
34	c|{stype}	campaign	5.166.5.227	3	Yaroslavl, Россия	48e3923c1519e3ac85e4859b542c13c5	1623304781402075348	1	3	2021-06-10 05:59:06.0	0.1	0.01

Какие характеристики у этих визитов? Всегда одно действие (клик), 3-5 секунд на сайте и разные IP- адреса. Обратите внимание, что в некоторых случаях Яндекс не присвоил клиенту ClientID. Это может быть в нескольких случаях. Первый — бот слишком быстро ушел с сайта и счетчик Яндекс.Метрика просто не запустился, второй — Яндекс сам определил визит как бота и посчитал клик «недействительным». К сожалению, таких

визитов очень мало. В основном каждый визит получает новый ClientID, при одинаковом «цифровом отпечатке».

Как пользователь менял IP- адрес? Скорее всего он использовал прокси- сервера. Мы не будем писать детально что такое прокси, информации масса и я думаю читатель уже знает этот термин. Сейчас важно понимать, что все клики были по рекламе (тип источника campaign, что означает «платный источник»). Очевидно, что имеет место быть яростное скликивание рекламы.



Прокси — это посредник, который маршрутизирует через себя ваш трафик и заменяет ваш IP-адрес на свой. Когда вы отправляете сайту (например, магазину ОЗОН.РУ) запрос через прокси, сайт не видит ваш IP, он видит только IP-адрес прокси-сервера, что дает вам возможность анонимно просматривать (или парсить) веб-страницы.

Как часто этот пользователь менял IP- адреса при кликах на рекламу сайта? Мы сделали простую выборку, см. изображение ниже. Видно, что каждый IP- адрес использовался несколько раз и легко обратить, что некоторые адреса явно брались с одного пула (например 176.222.*.* или 176.214.*.*).

	VisitsCount	VisitIp
1	15	185.4.204.53
2	13	178.214.255.206
3	11	5.206.61.97
4	10	77.222.118.201
5	10	176.226.129.68
6	10	95.84.212.18
7	8	176.226.244.79
8	8	77.222.96.104
9	6	5.227.15.18
10	6	46.172.13.120
11	6	176.15.208.33
12	6	176.226.189.252
13	6	176.226.128.74
14	6	178.214.245.114
15	6	178.214.247.176
16	6	95.105.64.8
17	5	93.157.144.31
18	5	176.226.232.74
19	5	178.141.155.209
20	4	109.198.164.248
21	4	145.255.2.241
22	4	178.214.247.68
23	4	178.214.246.202
24	4	178.214.251.143
25	4	46.191.138.206
26	4	46.191.232.57
27	4	46.147.158.19
28	4	77.222.98.103
29	4	81.88.222.206
30	4	95.79.160.106

Почему мы вообще решили, что это бот? В своей защиты мы используем несколько алгоритмов, которые работают последовательно, шаг за шагом идентифицируя ботов. В самих алгоритмах нет секретов, вы можете повторить их на своем сайте при наличии программистов. Например, мы проверяем вхождение IP- адреса в «черные» списки.

Если мы возьмем адрес 178.214.248.145 (см. изображение №1), то можно легко проверить его на чистоту с помощью любого сервиса. Вы можете сделать это сами, перейдя по ссылке: https://dnschecker.org/ip-blacklist-checker.php?query=178.214.248.145 (учтите, что через некоторое время адрес может уйти из черных списков, поэтому важно делать проверку оперативно). Данный адрес был найден в нескольких списках.

Что мы делаем еще? Мы проверяем визит с помощью Google reCaptcha, чтобы получить дополнительную оценку качества сессии. Если мы вернемся на изображения выше, то увидим, что для всех визитов ботов коэффициент reCapcha был равен 0.1 (очень высоко вероятно это бот в терминологии Google), а визит нашего сотрудника при проверке расчета Яндекс.ClientID дал коэффициент 0.9 (очень высоко вероятно это человек). Следом у нас работает алгоритм машинного обучения (если быть конкретнее, алгорим К-ближайшее), который кластеризует все визиты, чтобы находить тех ботов, который стараются мимикрировать под обычных пользователей (для описания этого алгоритмы мы подготовим отдельную статью).

Возвращаясь к поведению данного скликивающего бота. Мы посчитали, сколько раз вообще данный бот менял свое окружение так, что Яндекс.Метрика определяла его каждый раз как нового... получается 400 раз.

```
SELECT TOP(1000) COUNT(Id) as 'VisitsCount', YandexClientId
FROM Sessions WITH(NOLOCK)
WHERE SiteId = 410
AND Fingerprint = '48e3923c1519e3ac85e4859b542c13c5'
GROUP BY YandexClientId
ORDER BY COUNT(Id) DESC;
```

Script Output | Query Result

SQL | All Rows Fetched: 462 in 0,057 seconds

	VisitsCount	YandexClientId
1	39	(null)
2	3	1623089210774454717
3	1	1623089213667689320
4	1	162308921934616410
5	1	162308922685433073
6	1	1623089239845737141
7	1	1623089243136935067
8	1	1623089246116074322
9	1	1623089258664812137
10	1	1623105370372679510
11	1	1623126636730673516
12	1	1623128813439337984
13	1	1623128834981076408
14	1	162312883721027137
15	1	1623128848652558290
16	1	1623128849519255650
17	1	1623128854260238923
18	1	1623128862979106934
19	1	16231288651053435709
20	1	1623128871361842146
21	1	1623128875152638844
22	1	1623128880711696795
23	1	1623128907519005971
24	1	1623128913879288727
25	1	1623135738894548682
26	1	162313869822241201

Почему мы решили, что это точно бот, ведь наверняка сказать невозможно? Это так, никогда нет абсолютно точной вероятности, что мы заблокировали именно бота. Но мы можем судить по подмене ClientID, по одинаковому цифровому отпечатку Fingerprint (который вкупе с другими данными только подтверждает нашу гипотезу). Такое поведение не похоже на действие реального пользователя. Также, чтобы убедиться, можно дополнительно посмотреть через Вебвизор в Яндекс.Метрика — часто действия

ботов отличаются однообразием и линейностью движений мышкой, в то время как у реального пользователя они более хаотичны. Однако не всегда наши клиенты готовы предоставить доступ к данному инструменту нашим аналитикам, поэтому приходится полагаться на те данные, которые мы собираем сами в представленных в этом обзоре таблицах.

Данный клиент подключился к нашей системе 2 июня. За 8 первых дней июня было сделано порядка 400 кликов по платной рекламе. Мы не знаем стоимость одного клика, предложим, что она находится в пределах 50 руб. К сожалению, у нас нет доступа к Яндекс.Метрика/Яндекс.Директ, чтобы точно проверить какое количество кликов было признано Яндексом как недействительные, но из нашего опыта анализа других клиентов получается, что при наличии Яндекс.ClientID в 90% случаев клики засчитываются. Фактически, нехитрая математика дает нам оценку потерь: 8 дней, 400 кликов * 50 руб. = 20 000 руб.