ТОП три способа взломать WI-FI

5 апреля 2021

352 прочитали

Чего только в глобальной сети не найдешь, даже описания мошеннических действий по добыче бесплатного Wi-Fi. Если знания в области интернет-технологий не значительны, то лучше попросить помочь знакомого хакера. Кому под силу справиться самостоятельно, вот несколько популярных способов:

угадать пароль;

использовать специальную программу, чтобы она подбирала «ключ»;

раздобыть PIN устройства;

«фишинг»;

перехватить пароль.

Как самостоятельно угадать пароль

В каждом методе первоначально стоит выбрать Wi-Fi с наилучшим уровнем сигнала. Выбрав первый метод, придется немного поразмыслить. Вряд ли соседский Вай-Фай серьезно зашифрован. Если он далек от информационных технологий, обычный неопытный пользователь, то вряд ли он долго раздумывал над сложностью комбинации. Скорее всего, он использовал свою дату рождения, супруги или ребенка, а может, и вовсе фамилию.

Когда самые простые варианты с личной информацией не прошли, стоит обратить внимание на другие популярные «пассворды». Наиболее часто пользователи используют следующие комбинации цифр – «1234», «1111», «123123» и схожие с ними, также пароли из букв – «qwerty», «password» и прочие. Часто встречаемых сочетаний для защиты Wi-Fi существует немало, в сети на эту тему полно информации, а также представлены конкретные сочетания.

Плюс у метода значительный – простота, но минусы также присутствуют – длительность процесса. Особенно много времени потратит ограничение на попытки ввода. Если на чужом Wi-Fi стоит такая штука, то после трех неудачных попыток пароль придется вводить только через день вновь.

ПО для разгадывания пароля

Как же взломать сложный пароль от Wi-Fi? Принцип таких программ прост, они действуют по аналогии с человеком. Только компьютер в разы быстрее и смышленее. Программы имеют целые словари с популярными комбинациями. Иногда машина подбирает пароли за минуты, бывает, процесс затягивается на несколько суток. Сначала в ход идут простые версии, далее сложные. Время распознавания зависит от степени сложности пароля. Данную технологию еще называют «брутфорс», что и значит, поиск пароля.

К ознакомлению примеры программ – Aircrack-ng, Wi-Fi Sidejacking, Wi-Fi Unlocker AirSlax и другие. В интернете их множество, это лишь малая часть. Скачивая подобное программное обеспечение, мошенник сам рискует быть обманутым. Трояны и прочие неприятности мигом завладеют компьютером.

Мысль подключить технику для поиска пароля гениальна. Правда, в этом методе также есть свои минусы. Главный из них – отрицательный исход. Подбор может пройти безрезультатно. Это значит, что задумано слишком сложное сочетание символов, букв и цифр, которое еще не знакомо подобной программе.

Читайте также: Как правильно подключить Wi-Fi роутер?

Где взять PIN постороннего устройства

Заполучить PIN – несложное задание. Для чего стоит сходить в гости и переписать его с корпуса устройства для раздачи Wi-Fi. PIN полностью состоит из цифр. Не всегда устройство будет располагаться в удобном месте, но и на случай неудачи есть выход.

Еще один метод заполучить PIN – воспользоваться специальными программами. Можно воспользоваться, к примеру – CommView или Blacktrack. Такой вариант взлома запароленного Wi-Fi непрост. Устройство Вай-Фай постоянно обменивается пакетами информации между другими аппаратами, которые входят в зону его действия. Цель – перехватить данные.

Действовать нужно через компьютер или ноутбук с мощным железом, имея Wi-Fi карту с функцией Monitor mode. Создать загрузочный диск или флешку с дистрибутивом ПО для перехвата пакетов, установить оболочку на ПК. Выбрать сеть, а после переждать процесс перехвата около 10000 пакетов. Сначала программа выдаст PIN, а после и пароль.

Видео-материал по взлому сети с помощью стороннего ПО:

Совет: Запомните PIN-код. Когда хозяин изменит пароль, разгадать его будет гораздо проще, зная PIN.

Изменение Mac-адреса

Как же еще распаролить Вай-Фай? В представленном методе вопрос в принципе неуместен, иногда пользователи оставляют сеть открытой, но ставят фильтр по MAC-адресам. Это особый идентификатор каждого устройства. Узнать разрешенные MAC-адреса можно применив специальную программу. Например, Airdump-ng.

Видео:

Узнав белый список «идентификаторов», меняем свой. Для чего необходимо открыть «Панель управления», нажать «Центр управления сетями и общим доступом», после выбрать «Изменение параметров сетевого адаптера». Выбрать необходимое сетевое подключение, зайти в «Свойства». Произвести настройку сети – ввести MAC-адрес из 12 символов. Далее, перезапуск, и «вуаля», все получилось.

Фишинг

Фишинг – это один из методов сетевого мошенничества. Он позволяет обманом раздобыть логин и пароль. Так, посетив сайт, можно посетить фишинговую страницу и ввести свои данные, которыми и завладеет взломщик.

Информацию с секретными данными о Вай-Фай узнают с помощью программы WiFiPhisher.

По какой схеме работает ПО:

Настройка HTTP и HTTPS;

Поиск беспроводных сетей wlan0 и wlan1 до момента подсоединения к одному из них;

Отслеживание службой DHCP и вывод IP-адресов;

Выбор одной из доступных Wi-Fi точек;

Создается копия точки доступа, ей задается такое же имя. Скорость реальной точки уменьшается, благодаря чему пользователь начинает переподключаться и попадает на копию.

Браузер запрашивает ввод пароля, пользователь заполняет графу и пассворд попадает в руки мошеннику через WiFiPhisher.

Видео-инструкция:

Теперь у мошенника есть возможность настраивать посторонний роутер. Он может сменить WPS PIN, посмотреть данные для авторизации на любых ресурсах. С такими привилегиями появляется возможность отправлять пользователей банковских услуг на другие сайты, заполучая «свое».

Совет: Чтобы не попасться на «фишинговую» уловку, нужно всегда досконально перепроверять посещаемые сайты.

Варианты защиты собственной сети

Как оказалось, существует немало вариантов шпионажа за данными от Вай-Фай. Всем у кого есть дома или в офисе маршрутизатор стоит усложнить доступ третьих лиц. Иначе каждый рискует быть жестоко обманутым. Рекомендуется воспользоваться следующими советами:

Придумать сложное сочетание для пароля – не менее 10-12 символов, где учесть раскладку клавиатуры, регистр, знаки и цифры.

Отключить WPS, эта функция запоминает авторизованных пользователей и подключает их вновь в автоматическом режиме.

Периодическая смена PIN используемого устройства, а также удаление заводской надписи с корпуса.

Ограничьте доступ к информации о PIN, не вводите его на сомнительных сайтах.

Читайте также: Что делать, если роутер не раздает интернет по WiFi?

Эти шаги помогут качественно защитить свою сеть. Теперь ее может взломать только хакер с большой буквы. Будьте уверены, если взлом удался, он где-то рядом. Только близкое расположение злоумышленника может его привести к благополучному исходу.

Приложения с известными данными миллионов Wi-Fi

А может ни к чему взламывать защищенный Вай-Фай? Пользователи всего мира создали некую базу с паролями и точками Wi-Fi. Для доступа к ней стоит скачать уже готовую программу и выбрать нужную сеть. Информацию получают в следующих приложениях:

Wi-Fi Map – универсальное приложение для любой платформы телефона, оно покажет ближайшие Вай-Фай точки и пароли, если ранее кто-то уже подключался к выбранной сети;

Shift WiFi – популярное приложение пользователей системы Android, также как и предыдущая программа показывает все сохраненные ранее пароли к Wi-Fi.

Обзор приложения Wi-Fi Map:

Список таких приложений постепенно пополняется. Существует риск заполучить некачественный продукт. Всегда безопаснее загружать ПО с официальных и проверенных источников.

Взлом Wi-Fi c телефона

Сегодня осуществить взлом сети Wi-Fi можно даже с мобильного гаджета. Это даже удобнее, чем с ПК. Телефон проще приблизить к устройству, которое нужно взломать. Существует масса платных и бесплатных приложений. Часть из них – обман. Платные между собой могут отличаться актуализацией баз.

На сегодняшний момент известны:

Wi-Fi Prank;

WiHask Mobile;

IWep Lite.

Wi-Fi Prank – приложение «брутфорс». Для его работы необходима дополнительная закачка баз. Далее оно автоматически подбирает нужный пароль. Подходит для Android.

WiHask Mobile – действует по определенному алгоритму, не требует дополнительных баз. Работает до обнаружения скрытого пароля. Основано на той же технологии «брутфорс». Распространяется для системы Android.

IWep Lite – осуществляет поиск пароля на гаджетах iPhone. Для работы приложения необходима процедура активации. Необходимо найти сеть и выбрать статистику. После начинается автоматический поиск до удовлетворительного ответа с кодом.

Способы взлома беспроводной сети

В современном мире, где доступ к Wi-Fi является неотъемлемой частью нашей повседневной жизни, защита наших сетей и паролей становится все более важной задачей. Однако, несмотря на все меры безопасности, которые мы принимаем, существуют способы взлома, которые могут использоваться злоумышленниками для несанкционированного доступа к нашим данным. В этой статье мы рассмотрим некоторые из этих способов и расскажем о том, как защититься.

Как взломать пароль от вайфая?

Перед тем, как перейти к способам взлома, важно отметить, что вмешательство в чужие сети без разрешения владельца является незаконным и может повлечь за собой серьезные правовые последствия. Использование этих знаний и программ только с согласия владельца или в целях тестирования собственной безопасности - это единственно приемлемый сценарий.

Существуют программы, известные как "Wi-Fi взломщики паролей", которые позволяют злоумышленникам попытаться взломать пароли от защищенных беспроводных сетей. Однако, большинство современных Wi-Fi используют протоколы шифрования WPA/WPA2, которые довольно надежны и сложно поддаются атакам. Взломщики паролей могут использовать словарные атаки, перебирая множество возможных комбинаций паролей, но это требует большого объема вычислительных ресурсов и времени.

Как взломать запароленный Wi-fi?

Хакерские программы представляют собой специально разработанные инструменты, которые используются для взлома. Они обычно содержат различные уязвимости и эксплойты, которые позволяют злоумышленникам получить доступ к защищенной сети. Однако, использование таких программ является незаконным и неправомерным. Помимо этого, большинство операционных систем и антивирусных программ обнаруживают такие программы и могут предотвратить их работу.

Взлом Wi-Fi на Android

Android предлагает ряд приложений, которые утверждают, что позволяют взламывать Wi-Fi прямо с вашего мобильного устройства. Однако, подобные приложения обычно недоступны в Google Play Store, так как нарушают политику безопасности. Для их установки требуется получение root-доступа к устройству, что может повлечь потерю гарантии и создать серьезные уязвимости

Также можно найти программы для взлома Wi-Fi windows. Некоторые из них могут предлагать различные методы, такие как брутфорс атаки или использование уязвимостей в протоколе WPS (Wi-Fi Protected Setup). Однако, большинство современных маршрутизаторов имеют защиту от подобных атак, и использование таких программ может оказаться неэффективным.

Как узнать пароль Wi-Fi соседа?

Попытка узнать пароль Wi-Fi соседа без его разрешения является нарушением его частной собственности и противозаконной. Вмешательство в сеть другого человека без разрешения может повлечь за собой серьезные юридические последствия.

Хотя подключение к Wi-Fi без пароля может показаться привлекательным, это может создать безопасность сети и устройств. Отсутствие пароля позволяет злоумышленникам свободно получить доступ к вашей и украсть ваши личные данные. Рекомендуется всегда использовать пароль для защиты своей Wi-Fi.

Как подобрать пароль к Wi-Fi?

Подбор пароля к Wi-Fi, известный как брутфорс атака, является одним из самых распространенных способов взлома. Однако, если пароль достаточно сложный и содержит комбинацию букв, цифр и специальных символов, то такая атака может потребовать огромное количество времени и вычислительных ресурсов. Чтобы защититься, рекомендуется использовать длинные и сложные пароли, а также периодически изменять их.

Одно из руководств взлома:

Первый шаг состоит в загрузке программы Dumpper. Для этого просто выполните поиск в Google по запросу "скачать Dumpper" и загрузите самую последнюю версию программы.

Второй шаг заключается в распаковке и установке программы. Для этого потребуется любой архиватор, например, WinRAR. После распаковки просто откройте файл с расширением .EXE и следуйте инструкциям по установке до конца.

Третий шаг - запустить программу и начать сканирование доступных сетей. Для этого дважды щелкните на значке Dumpper и перейдите на вкладку WPS. Затем нажмите кнопку "SCAN".

Четвертый шаг - начать перебор паролей для различных сетей. Выберите позиции с наилучшим сигналом и нажмите кнопку "WPSWIN".

Кроме того, существуют и методы защиты от взлома, которые могут помочь обеспечить безопасность вашего Wi-Fi:

Используйте более сильные методы шифрования: При настройке беспроводного маршрутизатора выберите более безопасные протоколы шифрования, такие как WPA2-PSK (AES). Это обеспечит более надежную защиту, чем старые протоколы, такие как WEP.

Скрытие имени (SSID): Один из способов защитить свою беспроводную сеть - это скрыть ее имя (SSID). Это делает ее невидимой для обычных пользователей, и только те, кто знает точное имя, смогут подключиться к ней. Однако, этот метод не является 100% надежным и может быть преодолен опытными злоумышленниками.

Включите фильтрацию MAC-адресов: Фильтрация MAC-адресов позволяет указать, какие устройства имеют разрешение на подключение. Вы должны добавить MAC-адреса устройств, которым разрешено подключаться, и все остальные устройства будут блокироваться. Однако, учтите, что MAC-адрес можно подделать, поэтому этот метод также не является абсолютно надежным.

Обновляйте маршрутизатор и установленное программное обеспечение: Регулярное обновление маршрутизатора и всех установленных на нем программ и драйверов является важным шагом для обеспечения безопасности. Обновления часто содержат исправления уязвимостей и улучшения безопасности.

Используйте дополнительные уровни аутентификации: Рассмотрите возможность использования дополнительных уровней, таких как RADIUS-серверы или системы аутентификации на основе сертификатов. Это повысит безопасность вашей сети и усложнит задачу злоумышленникам.

Невзирая на все меры, помните, что абсолютной защиты не существует. Всегда оставайтесь бдительными, обновляйте свое программное обеспечение и следуйте хорошим практикам безопасности.