Каждый пользователь желает, чтобы его приватные данные и личные файлы были скрыты от посторонних глаз, чтобы конфиденциальная информация была известна только ему, и никто не смог к ней получить доступ. Чтобы позаботиться о своей информационной безопасности, не нужно быть профи в сфере IT-технологий, достаточно знать несколько важных хитростей, чтобы обойти ловушки хакеров и обезопасить себя от взлома.

Содержание

Далее будут рассмотрены главные способы, как защитить себя от слежки и взлома через Интернет. Важно понимать, что они не дают абсолютную гарантию, однако в разы повышают ваш уровень кибербезопасности.

Скрыть свой IP-адрес через сервис VPN

VPN – это виртуальная частная сеть, работа которой ориентирована на то, чтобы защитить данные пользователя и их передачу посредством шифрования и полного сокрытия реального адреса IP. Когда вы используете сервис, никто не сможет перехватить ваш трафик и определить вашу геолокацию. Кроме того, преимущество VPN заключается в том, что вы сможете заходить на заблокированные сайты, недоступные в вашей стране.

Устанавливайте vpn для пк и сможете всегда спокойной подключаться к публичным Wi-Fi, не боясь, что вас взломают. Это безопасная и эффективная технология, чтобы повысить свою приватность в Интернете.


UP TO 70 % OFF
Featured Collections

Тщательно думать прежде, чем загружать данные в облако

Не всегда такие действия логичны и оправданы, несмотря на то, что множество крупных компаний и фирм пользуются облачным хранилищем для своих корпоративных данных. Безусловно, такие сервисы безопасны, но только в том случае, если вы точно знаете, как им правильно пользоваться и настраивать его. Если вдруг случайно опубликуете данные, которые должны были оставаться в секрете от посторонних глаз, уже поздно будет плакать.

Для максимальной защиты приватных данных лучше всего скопировать их на внешний носитель (флешку, диск), а не переносить в облако.

Не связывать все аккаунты между собой

Если привязывать аккаунты между собой, это, конечно же, удобно для вас, но и для хакеров тоже. Да, таким способом вы оптимизируете свою цифровую информацию, но и повышаете риски взлома.

Воспринимать вопрос безопасности как пароль и придумывать надежный шифр

Речь идет о том, что не нужно в качестве подтверждений личности задавать параметры девичьей фамилии матери или любимого питомца/блюда/города, а потом публиковать об этом посты в соцсетях. Все данные в разделе безопасности должны быть тайными, например, можно использовать случайную фразу. Если ваш код будет доступен в публичных постах, ни о какой безопасности и речи быть не может.

Вводя данные платежной карты, проверяйте безопасность самого сайта

Если вам требуется ввести платежные реквизиты, убедитесь в том, что данный веб-ресурс, защищен. Доказательством этого служит иконка замка в начале адресной строки. Кроме того, адрес должен начинаться с буквенной комбинации «https://», что говорит о безопасности его трафика.

Использовать двухуровневую идентификацию

Когда вы заходите в аккаунт почты или социальной сети, электронный кошелек или аккаунт бронирования, рекомендуется применять метод двухфакторной аутентификации, чтобы хакерам было сложнее обойти вашу защиту. Данный способ подразумевает, что кроме логина и пароля вы должны подтвердить свою личность посредством мобильного устройства – на него придет смс-ка с кодом или входящий вызов. В таком случае хакеру не удастся взломать ваши аккаунты.

Использовать сложные пароли для входа

Многие знают это предостережение, но не всегда пользуются им. В 2014-ом году топ самых популярных паролей возглавила комбинация «123456», которая легко и быстро поддавалась раскрытию. Чем сложнее пароль, чем больше он содержит рандомно выставленных заглавных и прописных букв, а также символов и цифр, тем он сложнее. Никогда не используйте в качестве пароля даты рождения, номера машины, фамилии и имена своей семьи.

Пользоваться PGP для приватной и защищенной переписки

PGP, или pretty good privacy, представляет собой достаточно несложный вариант шифрования сообщений, в которых задействуются открытые и частные ключи. Информация, с помощью которой происходит шифровка сообщения, идентифицируется как открытый ключ. Все лица, которые будут получать послания в зашифрованном виде, должны держать ключ доступным, что позволяет принимать и расшифровывать их. Частный ключ – это код для единственного пользователя, он всегда закрыт.

Данную технологию можно сравнивать с коробкой и двумя ключами. Отправитель написал сообщение и закрыл его в коробочке своим ключом. А получатель открывает замок уже собственным ключиком, чтобы расшифровать содержимое.

Можно создавать такие ключ прямо в своем браузере, но лучше всего использовать специальный инструмент GPGTools. Данная программа популярна и востребована среди тех, кто беспокоится о своей безопасности. Для генерации собственного ключа необходимо выбрать опцию File и далее New Key.

Ввод данных

Вы вписываете необходимые данные и кодовую фразу, которая и служит основой для создания ключа. Никому нельзя ее произносить и уж тем более передавать по электронной почте. Фразу придумаете длинную из рандомного набора букв и символов.

Ключ готов

Когда ключ сгенерирован, вам будет представлена сокращенная символьная последовательность, именуемая как Fingerprint. Если вызвать команду копирования, вы сможете вставить его, например, в блокнот, и тогда фраза высветится целиком. Этот ключ передается тому, кто будет отправлять вам сообщения с предварительным их шифрованием. Для расшифровки полученного послания вы используете свой частный ключ.

Включать Tor, если требуется анонимный серфинг в Интернете

Браузер Tor полезен всем, кто хочет скрыть свой реальный IP и в анонимном режиме посещать сайты в Интернете. Принципе его работы аналогичен традиционным обозревателям, только с дополнительным шифрованием и скрытием пользовательских данных. Выстроенная длинная цепочка запросов

позволяет передавать данные от пользователя к сайтам в рамкам своей подсети, чтобы нельзя было отследить первоисточник.

Tor в чем-то напоминает VPN, однако замедляет скорость соединения и загрузки веб-ресурсов. Но если правительство через суд может принудить провайдеров VPN рассекретить данные пользователя, то с анонимным браузером подобной угрозы нет. Его можно быстро скачать и установить для работы.

После запуска обозревателя вы просто нажимаете кнопку Connect. При необходимости могут потребоваться дополнительные настройки через Configure.

Когда вы подключены к Tor, все просторы Интернета открыты для вас и можно посещать сайты, которые ранее были заблокированы или ограничены ввиду региональных требований.

Пользоваться утилитами для блокировки рекламы, чтобы сохранить конфиденциальность

Программа-блокировщик полезна тем, что ограждает пользователя от назойливой рекламы, но, с другой стороны, лишает заработка сайты, которые вы любите и часто посещаете. Рекомендуется создать список исключений, чтобы на ваших популярных веб-ресурсах была разрешена реклама.

Такие утилиты могут рассматриваться как полезный инструмент для повышения уровня своей приватности в Интернете. Они блокируют не только рекламу, но и скрытые инструменты, с помощью которых компании отслеживают ваши действия и собирают данные о вас.

В браузере Google Chrome установить расширение Ugly Email

Сегодня можно найти большое количество инструментов, с помощью которых происходит отслеживание электронных писем и информирование отправителя о том, что письмо было доставлено и даже прочитано получателем. Но, если установить расширение в Ugly Email Гугл-браузер, вы сможете узнавать, кто следил за вашим почтовым ящиком. При этом даже не надо открывать полученные письма. Утилита будет контролировать письма, которые отслеживаются с помощью таких программ как Streak, Bananatag, Yesware.

Запретить рекламодателям в Фейсбуке собирать данные

В режиме умолчания каждый пользователь дает разрешение разработчикам Facebook собирать приватную информацию для подбора целевой рекламы. Но вы всегда можете отменить это действие, следуя простой инструкции:

- зайти в Настройки;
- выбрать Ads и отключить рекламу.

В этом же разделе можно установить, чтобы никто не смог видеть ваши социальные действия, удалить все свои предпочтения и т.д.

Отключить слежку в Google-аккаунте

Google всегда следит за своими пользователями, собирая данные о привычках, посещаемых сайтах, покупаемых товарах и т.д. Но можно легко отключить эту опцию, чтобы обеспечить себе приватность.