**Chrome и позиция Google относительно конфиденциальности**

В редакцию интернет-журнала lifehacker.com обратился читатель с вопросом о том, какой же браузер лучше в плане безопасности персональных данных. Многие считают, что такие популярные браузеры как Firefox и Chrome пристально следят за действиями своих пользователей, что небезопасно. Быть может проще использовать такие браузеры как Opera или Safari, чтобы обезопасить личную жизнь от вмешательства с их стороны?

Chrome позволяет отключать и включать различные опции приватности, такие как проверка орфографии, подстановку наиболее вероятного адреса сайта, статистика использования браузера и ответы об ошибках. В стандартных настройках большинство этих опций активны и отключить их можно на вкладке chrome://settings, нажав на ссылку «Показать дополнительные настройки». Там же можно активировать функцию «Отправлять с исходящим трафиком запрос «Не отслеживать», что позволит сообщить сайтам, что вы не хотите, чтобы они следили за вами (работает в том случае, если посещаемые сайты обрабатывают этот параметр). В разделе «Примечания о конфиденциальности Google Chrome» вы можете найти подробное объяснение, какую информацию собирает Chrome и как он с ней поступает.

Объемы информации, которые Google пересылает к себе, зависит от используемых функций. Например, если вы используете голосовой поиск, функцию подстановки вероятного адреса сайта или проверку правописания, то вся эта информация отправляется на сервера Google для обработки. Если включена опция сбора анонимной статистики и отправки отчетов об ошибках, то на сервера также отправляется и другая дополнительная информация. Но вся она, по заверению Google, анонимна.

Но при этом Google не говорят, как долго они хранят эту информацию и насколько сложно на основе всей собранной информации составить профиль пользователя на основе тех данных, что у них есть. Также представители Google заявили, что  безопасность и конфиденциальность пользователей имеет для них наивысший приоритет. Также они ведут серьезную борьбу с государствами и компаниями, которые хотят собирать приватную информацию об их пользователях. На сайте Google даже есть публичная статистика, в которой отображается количество запросов от государственных органов с различными требованиями.

Также представители Google напомнили о высокой степени безопасности браузера Chrome, различные уязвимости для которого поощряются финансово, что провоцирует хакеров очень пристально следить за браузером и изо всех сил пытаться его «сломать». Также стоит помнить о том, что всегда можно посетить chromium.org и посмотреть на исходный код проекта. Также Chrome одним из первых ввел «песочницу» в качестве меры безопасности, а даже синхронизации учетной записи Google перед отправкой шифруются.

Компания Google уверена в безопасности Chrome, но вот некоторые независимые специалисты по безопасности не так однозначны. С одной стороны Chrome безусловно безопасен. Но с другой стороны у Google есть ряд других источников информации, из которых они могут по крупицам собирать данные и на их основе подставлять рекламные объявления в поиске, на сайтах и интернет-сервисах, которыми владеют (YouTube, Google Drive, Google+ и другие).

**Mozilla Firefox**

Firefox давно позиционируется в качестве лучшего браузера для защиты частной жизни. Он с открытым исходным кодом и руководит его разработкой некоммерческая организация Mozilla Foundation (стоит отменить, что Google является инвестором данной компании). Даже мобильная версия Firefox для Android распространяется с открытым исходным кодом и посмотреть его может любой желающий. Так как Mozilla Foundation не является коммерческой организацией, то у многих сложилось впечатление, что у фонда нет резона получать данные пользователей для внутреннего использования или продажи.

Но все же Firefox собирает некоторую информацию. Например, сервис синхронизации Firefox Sync работает с закладками, паролями, последними открытыми вкладками и другой информацией, которая необходима для обмена между мобильными и стационарными устройствами. Но эта информация, как и в случае синхронизации в Google Chrome, также полностью шифруется. Все расширения для Firefox, в отличие от Chrome, проходят тестирование перед тем, как попасть к пользователям. Такой подход позволил Mozilla избежать проблем, с которыми недавно столкнулся Chrome.

У Mozilla также есть собственная политика конфиденциальности Firefox, которая повествует о том, какая информация и для чего именно используется их браузером. В целом, все примерно так же, как и у Google Chrome в этом плане. К сожалению, все попытки связаться с представителями Mozilla Foundation не увенчались успехом.

Несмотря на это, у Firefox есть свои проблемы безопасности, с которыми они столкнулись. Не так давно они объявили о том, что планируют ввести рекламу в Firefox в виде спонсируемых плиток на начальной вкладке. При первом открытии браузера они будут рекомендовать сайты, за размещение которых им заплатят. Многие стали ругать за это разработчиков, утверждая, что они «продали душу».

**Что на счет Opera, Safari и Internet Explorer?**

Если вы решили отказаться от Chrome или Firefox, то какой браузер следует выбрать? Существуют еще Opera,  Safari и Internet Explorer. Это тоже хорошие браузеры, которые вполне безопасны и у каждого есть свои плюсы и минусы. Но главный их минус в закрытом коде – нельзя посмотреть на то, как устроен браузер и как он работает. Opera не так давно перешла на движок Blink – тот же, что использует Chrome. У каждого производителя браузера есть своя политика конфиденциальности, в которой описываются принципы сбора и обработки информации браузером.

**Заключение**

Все браузеры передают информацию на сервер разработчиков, но вся она необходима исключительно для того, чтобы поддерживать работу текущих функций и совершенствовать удобство использования продукта в целом. Синхронизация закладок, паролей и открытых вкладок не опасна, так как все данные шифруются. Это касается как Firefox, так и Chrome.

Однако стоит внимательнее относиться к используемым расширениям (плагинам), которые могут сыграть на невнимательности и получить доступ к важным персональным данным. Не стоит слепо доверять и устанавливать неизвестные расширения. Лучше почитать отзывы, посмотреть количество оценок и принять решение. Перестраховавшись, вы обезопасите себя и свои персональные данные.

Помимо этого, не стоит пропускать настройки конфиденциальности в браузере и проверить, все ли важные для вас настройки отключены.