Автор: Whiteworm
02.02.2008 21:43 -

Над тем, как обеспечить свою анонимность в интернете, наверняка задумывались многие. Причем, неузнаваемость для веб-сайтов или www-сервисов может оказаться полезной не только какому-нибудь "типа крутому хакеру", но и обыкновенному пользователю сети

Зачем это нужно

При посещении интернета необходимость скрыть свой реальный ip-адрес, позволяющий идентифицировать ваш компьютер, может возникнуть в силу целого ряда причин. Например, таким образом можно выдать себя за жителя другого государства и получить доступ к ресурсу, заблокированному для вашей страны. Далее, некоторые порталы выдают пользователю содержимое в зависимости от региона, в котором человек находится, что можно наблюдать на примере новостей на главной странице Яндекса. Подмена ip адреса поможет обойти это ограничение.

Кроме того, путешествуя по интернету, мы зачастую и не задумываемся о том, что оставляем следы своих посещений каждый раз, когда заходим на какой-либо сайт. Пожалуй, об этом и не стоило бы беспокоиться, если бы не был так велик тот объем информации, который потенциально могут добыть о нас владельцы сайта.

При помощи стандартных log-файлов, разнообразных скрипов и прочих ухищрений администратор может узнать о нас многое: тип компьютера и операционной системы, страну пребывания, название и адрес провайдера. Сокрытие своего реального ip также может оказаться полезным, если вас вдруг забанили в чате или на каком-то форуме, а вам все равно хочется туда попасть. Хотя бы для того, что бы сказать модератору все, что вы о нем думаете :)

Анонимный серфинг может быть использован и как средство обхода ограничений различных онлайновых файловых сервисов, например, той же RapidShare. Как известно, для тех, кто не является платным подписчиком этого сервиса, на RapidShare установлен лимит количества загрузок с одного ip адреса. И если такое ограничение для вашего ip было превышено, то при помощи замены своего сетевого адреса на какой-нибудь другой вполне можно попытаться решить и эту проблему. Достичь же той, или иной степени анонимности в интернете можно несколькими способами.

Сайты-анонимайзеры

В сети существует предостаточное количество так называемых сайтов-анонимайзеров, таких как этот Все что нужно пользователю, желающему обеспечить свои анонимность, это зайти на такой анонимайзер, и ввести в специальном поле адрес сайта, который необходимо посетить. Дальнейший переход по ссылкам также будет анонимным, а при серфинге обычно вверху загружаемых страниц будет находиться небольшая, не мешающая просмотру панель анонимайзера.

На большинстве таких сайтов-анонимайзеров можно выбрать настройки серфинга, например - включить блокировку скриптов или cookies, отключить загрузку изображений. Проверяя работу этих сервисов на практике, можно заметить, что они действительно подменяют ip, но все же не скрывают данные о браузере, при этом на некоторых из них наблюдаются проблемы с отображением кодировки русскоязычного текста.

Прокси-серверы

Для тех, кто не в курсе: прокси-сервер, это такой специальный компьютер, через

который вы можете выходить в интернет. Возможно, вы уже используете прокси-сервер вашего провайдера, или корпоративный прокси, если вы выходите в интернет с вашего рабочего места из офиса. В случае со служебным интернетом прокси-сервер может быть использован для блокировки доступа к сайтам с нежелательным содержимым, ограничения трафика и в целях безопасности (защита от вирусов, несанкционированных проникновений на компьютеры пользователей, и так далее)

Но существуют и другие, так называемые публичные прокси-серверы, через которые при желании пользователь также может выходить в интернет. В любом случае прокси-сервер сначала "забирает" для вас информацию с сайта, и только потом данные попадают на ваш компьютер. Создавая такой сервер, провайдер обычно предназначает его только для своих абонентов, при этом доступ для посторонних интернет-серферов на него закрыт. Однако бывают и исключения, когда прокси-сервер настроен так, что им может воспользоваться любой желающий, причем совершенно бесплатно. Осталось среди таких прокси-серверов найти анонимные и настроить свой интернет-браузер таким образом, что бы он "ходил" именно через выбранный прокси-сервер. Списки рабочих анонимных прокси-серверов достаточно легко найти в интернете. Но такие прокси-серверы следует обязательно проверять на предмет их анонимности. Для этого необходимо сначала прописать адрес и порт прокси в настройках браузера, а затем зайти на специальную страницу проверки Дело в том, что не все прокси-серверы в интернете являются анонимными и могут передавать ваш ip сайту в поле "X-Forwarder-For:". Такие прокси-серверы называются искажающими.

Есть и прокси-серверы так называемой повышенной анонимности. Они сообщают веб-узлу такой набор данных, что в узел в результате даже не должен видеть, что вы используете прокси-сервер. Как и сайты-анонимайзеры, прокси-серверы также не обеспечивают полной анонимности. Любой прокси-сервер может вести логи подключений, в которых отображаются ip-адреса пользователей и посещаемых ими сайтов.

При очень большой надобности эти записи вполне могут попасть "куда следует", так что особенно надеяться на прокси-сервер в плане анонимности было бы наивно. Можно правда выстроить так называемую цепочку из нескольких анонимных прокси-серверов, и тогда "вычислить" вас будет намного сложнее. Однако из-за своей технической сложности для простого пользователя данный способ, скорее всего, не имеет особого смысла. Дополнительно о типах прокси-серверов можно прочитать здесь

Программы-анонимайзеры

Еще одним способом обеспечения анонимности при веб-серфинге может стать использование специальных программ. Судя по всему, это достаточно прибыльная рыночная ниша для разработчиков софта, поскольку таких программ существует великое множество, причем большинство из них - платные. В своей работе они используют те же анонимные прокси-серверы, разница лишь в том, такие программы самостоятельно и автоматически выполняют поиск, проверку и подключение к анонимным прокси вместо пользователя.

Способ весьма удобный, но опять же не обеспечивает стопроцентной безопасности. Например, программа HideIp сразу после установки на моем компьютере попыталась соединиться со своим сайтом. Может для того, что бы проверить триальность версии, а может и еще для чего, кто знает.. Ну и, наконец, немногие подозревают, что попытаться использовать анонимные прокси-серверы можно, в том числе и находясь за прокси

корпоративной локальной сети, но это, как говорится, уже отдельная тема, которую я надеюсь "обозреть" в ближайшем будущем.