Автор: admin.

Из чего состоит Интернет? Весь Интернет состоит из сайтов, это его основа. Не будет сайтов - не будет и Интернета. Посещая тот или иной сайт, мы получаем необходимую нам информацию, но вместе с этим, мы также подвергаем себя определённым рискам. В диапазон этого понятия входит широкий спектр различных обстоятельств и главная наша задача, это максимально обезопасить себя от воздействия этих негативных факторов.

В большинстве своём, для интернет-серфинга, все мы пользуемся, так называемыми веб-обозревателями, или иными словами, браузерами. Правильная настройка браузера, в дополнение с использованием всякого рода расширений, даёт нам возможность, обезопасить себя от непредсказумеых результатов. В данном случае, речь пойдёт о браузере *Firefox*, находящимся в одной линейке самых популярных и востребованных обозревателей.

Для начала попробуем, в общих чертах, определить возможные риски. Открываем браузер и заходим на сайт: 2ip.ru (специализированный сервис по определению *IP*-адре са и многого другого). И что мы видим? Сервис определил:

1. Реальный *IP*-адрес.
2. Имя компьютера.
3. Операционную систему (*user agent*).
4. Используемый браузер (*user agent*).
5. Ваша страна и если кликнуть по ссылке, то и город.
6. Ваш интернет-провайдер.
7. Наличие прокси.

Много это или мало? Это очень много, но далеко ещё не всё, что вообще могут собирать о вас, посещаемые вами сайты. Каждый браузер и *Firefox* в частности, хранит в себе определённую информацию, которую тоже, при современных технологиях можно легко заполучить, а это:

1. Журнал посещений и загрузок.
2. Активные сеансы.
3. Журнал форм и поиска.
4. Куки.
5. Кэш.
6. Сохранённые пароли.
7. Настройки сайтов.
8. Данные автономных веб-сайтов.
9. *Flash*-куки.
10. А также, отправка отчётов.

Кроме всего прочего, существуют такие "вещи", которые могут собирать и передавать соответствующую информацию:

1. *Java* скрипты.
2. Такая "штука", как межсайтовые запросы.
3. Сбор статистики.
4. *HTTP-referer*.
5. *HTTP* вместо *HTTPs*.
6. Несанкционированная установка дополнений.
7. Атакующие сайты.
8. Фишинг.
9. Вредоносная реклама.

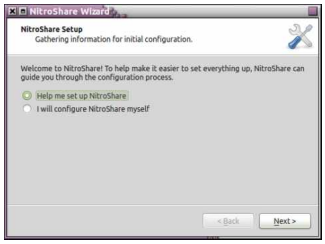
Всё это, как бы в общих чертах и скорее всего, можно ещё чего-то добавить, но остановимся на самом главном. Если всё вышеперечисленное использовать против вас, то "картина" складывается весьма не красочная. Практически, при желании и соответствующем умении, можно узнать о пользователе всё. Как всего этого избежать? Этим и займёмся.

Настройка браузера.

Прежде всего, настроим правильную приватность, так, как это показано на снимке ниже.

Переходим на вкладку "Параметры".

Здесь обратите внимание на пункт "*Flash Cookies*", которого по-умолчанию в *Firefox* нет. Это специальный плагин
Better Privacy
о котором, будет упомянуто чуть-чуть позже, при разговоре об
LSO
и
Flash cookies
. Также, непомешало бы отключить кеш вообще.



И ещё лучше, добавить на странице настроек *Firefox*: ***about:config*** (ввести в адресную строку браузера), есть параметр:
browser.cache.disk.enable
(ввести в строку поиска) и затем, установить значение:
false
. Теперь защитим себя от опасных сайтов.

Не смотря на то, что в браузере имеется мастер-пароль (один пароль для всех), лучше

вообще, пароли в браузере не хранить. Для этого имеется отличный плагин *LastPass*, который отлично справляется с этой задачей и сохраняет все пароли, в облаке, и в зашифрованном виде (об этом тоже, чуть позже).

Совершенно лишним будет отправлять какую-либо служебную информацию в *Mozilla*, поэтому отключим эти функции.

Вот собственно, при таких настройках, и браузер должен нормально работать, и при его закрытие, вся информация будет автоматически удаляться, что и требовалось!

Удаляем LSO и Flash Cookie.

Вообще, сам процесс удаления *Local Shared Objects* (*LSO*) или *Flash cookies*, довольно сложный и сделать это вручную бывает крайне трудоёмко, да это и не нужно. Для *Firefox*
, имеется отличное расширение (плагин), который хорошо с этим справляется. Называется он "
Better Privacy
". Установить можно обычным способом из самого
Firefox
(са), в
"Инструменты" "Дополнения"
.

Подменяем User Agent (отпечаток браузера).

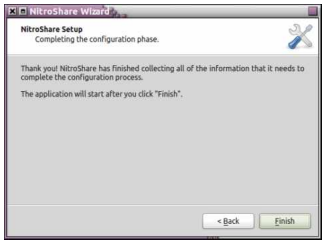
Любой браузер, в процессе своей работы предаёт серверу различные категории данных, включая и *User Agent*. В результате этого, образуется некий уникальный «цифровой отпечаток браузера», благодаря чему, его можно идентифицировать среди множества других браузеров. Это то, что мы с вами рассматривали на самом первом этапе, заходя на сайт ***2ip.ru***, который нам определил: наш браузер и операционную систему (оба эти параметра входят в состав *User Agent*).

Для маскировки этих данных существует много разных дополнений к браузеру и одно из них, отлично выполняющее свою работу, это «*User Agent Overrider*». Установить можно также, обычным способом, через встроенную в браузер установку дополнений.

Запрещаем HTTP-referer.

Данный параметр - позволяет отслеживающему вас сайту, определять то, откуда вы к нему пришли. Если вы с одного сайта, по ссылке, передающей этот показатель, перешли на другой, отслеживающий вас, то данный сайт будет знать, с какого именно домена вы к нему перешли. Данную ситуацию можно изменить в настройках ***about:config***. Но, здесь есть одно "но".

Так называемые "рефери" могут использоваться на многих, очень нужных ресурсах (например почта *GMail.com*), как неотъемлимая надобность и поэтому получается, что есть необходимость переодического включения или отключения данной функции. Делать это каждый раз через «***about:config***», ну очень неудобно. Зато есть плагин «
Change Referer Button
», который располагается в основной панели навигации браузера, в виде кнопочки. Устанавливается стандартным способом, как расширение.



В настройках ***about:config***, параметр: ***network.http.sendRefererHeader***, имеется три варианта отправки
referer
:

0 – никогда не отсылать *HTTP-referer*
1 – отсылать только по кликнутым ссылкам
2 – отсылать для ссылок и картинок (по умолчанию)

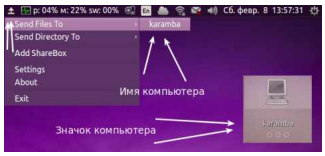
В плагине на кнопочке прописаны цифры, соответствующие этим же значениям, которым в свою очередь, соответствуют каждый отдельный цвет:

0 - красный
1 - жёлтый
2 - зелёный

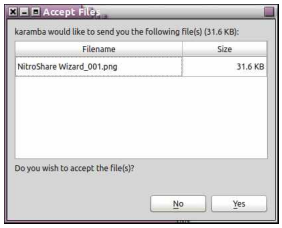
Благодаря этому плагину, будет очень удобно управлять отправкой *referer*, по-мере

необходимости. Что бы реально проверить, как это работает, надо зайти по адресу:
http://www.whatismyreferer.com/
и кликнуть по ссылке внизу, под текстом (она там одна). В результате вы увидите:

Это - Referer передаётся.



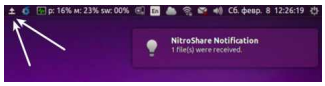
Или это - Referer не передаётся.



Принудительное HTTPS-Everywhere.

В кратце, это выглядит так. Есть соединение по протоколу: *HTTP* (опасное) и есть по протоколу: *HTTPs* (безопасное). Некоторые сайты, которые поддерживают протокол *HTTPs* (банки, магазины и т.д.), не всегда настроены на *HTTPs* по-умолчанию. Данный плагин, отслеживает такую ситуацию, и если, безопасная поддержка всё-таки имеется, то он "автоматом" подключает вас к сайту по протоколу: *HTTPs*

(на снимке помечен белой стрелочкой).

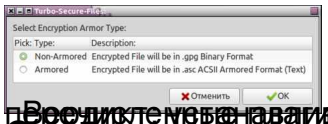


В самом меню плагина, также отображаются все сервисы (в том числе и скрытые), имеющиеся на посещённой странице и работающие по данному протоколу. Устанавливается плагин стандартно из расширений *Firefox*.

Запрещаем Web Bugs + рекламу.

Web Bugs - это определённые детали веб-страниц (могут быть скрытыми), отслеживающие посещаемость ресурса (разные счётчики, аналитика, виджеты и прочее), собирающие разного рода данные о клиенте и дополнительно отсылающие их на сервер. Для предотвращения таких действий, имеются, ну наверное много расширений антислежения, мне известны два, довольно-таки неплохих: *Ghostery* и *DoNotTrackMe*.

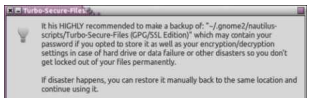
А ещё есть, очень популярное и полезное расширение: *AddBlock* или *AddBlock +* (плюс), удобные такие "штуки", блокирующие рекламу (реклама тоже может быть вредоносной и опасной). До определённого времени для запрета *Web Bugs*, можно было пользоваться *Ghostery* и *DoNotTrackMe*, да и сейчас можно тоже. Но, дело в том, что в *AddBlock* (и в плюсовом тоже), появился новый фильтр: *EasyPrivacy*, который неплохо справляется с этой задачей (на снимке плагин помечен стрелочками).



Рекомендуем также использовать *AdBlock*, который стандартно решающий эти проблемы. Все перечисленные плагины устанавливаются стандартно.

Сохраняем пароли в облаке.

В браузере *Firefox* имеется свой собственный менеджер паролей, с защитой по мастер-паролю. В принципе, можно пользоваться и им, но на мой взгляд и не только на мой, лучше воспользоваться плагином *LastPass* (облачный менеджер паролей), хранящий все пароли на сервере в зашифрованном виде (на снимке плагин помечен стрелочками).



Плагин устанавливается стандартно.

Javascript.

Скрипты *Javascript*, исполняемые на стороне клиента, могут собирать для сервера множество категорий идентифицирующий данных. Более того, если посещаемый сайт подвержен *XSS*, то включенные на нём скрипты *Javascript* помогут злоумышленнику провести успешную атаку со всеми вытекающими последствиями. Для того, чтобы запретить данные скрипты лучше всего подходит дополнение *NoScript*
(помечено белыми стрелочками).

Помимо *Javascript,* дополнение может блокировать еще множество различных

элементов: *Java, Flash* и пр. Пользователь может временно разрешить выполнение всего активного содержимого на странице или сделать это на постоянной основе. Установить плагин можно стандартно. Кроме того, придётся потерпеть какое-то время, что бы привыкнуть к данному расширению.

Javascript - это неотъемлимая часть современных сайтов и полный запрет на его исполнение, просто приводит сайт в нерабочее состояние по разным показателям. Пользоваться плагином придётся интенсивно, поэтапно исключая знакомые и проверенные сайты.

Запрещаем межсайтовые запросы.

Что такое межсайтовые запросы? Вы попадаете на один некий сайт, а он в свою очередь (сайт), делает запрос на другой сайт, что бы получить с него, например, изображение и продемонстрировать его вам. Подобная структура запросов, весьма активно используется рекламными технологиями и по своей сути, нечего плохого в этом нет. Но, у каждой палки есть два "конца", и не очень "чистоплотные" сайты могут использовать данный метод для своих "грязных" замыслов. Допустим, уже где-то на третьем сайте, могут выполняться неправомерные действия, используя при этом куки вашего веб-обозревателя. Оно вам надо?

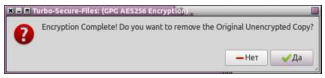
Расширение *RequestPolicy* может предотвратить подобные действия. Рекомендуется использовать напару с *NoScript* (на снимке помечен стрелочками).

Устанавливается также стандартно и требует, как и *NoScript*, привыкания и активного

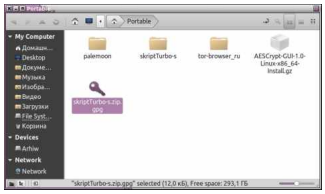
участия, по такому же принципу, постепенного отсеивания проверенных сайтов.

Безопасный поисковик по-умолчанию.

Самой безопасной поисковой системой на сегодняшний день, считается поисковик *Duck DuckGo*
, который не ведёт никакой слежки за пользователями. Чтобы его установить в браузере по-умолчанию, нужно открыть меню (см. снимок ниже) и просто выбрать его.



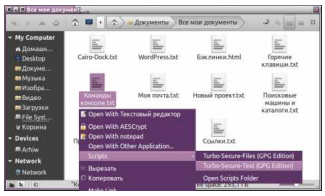
Если данного названия не оказалось, то нужно просто установить дополнительный плагин. Для этого кликаем на пункт "Управление поисковыми системами".



Кликаем на ссылку "Плагины других поисковых систем..." и затем, устанавливаем данный плагин, после чего, данный поисковик должен будет появиться в списке. Выбрав его просто из списка, мы сделаем его поисковиком по-умолчанию.

Меняем IP-адрес и прочее.

Из наиболее простых и удобных плигинов для изменения *IP*-адреса, имени компьоютера, страны и имени провайдера для *Firefox*, так, что бы не нужно было "париться" со всякими там *proxy*-листами, а просто кликнул и всё, мне известны два плагина: *Browsec* (устанавливается, но почему-то не работает), сайт: https://browsec.com/ru/ и плагин: *AnonymoX* (устанавливается стандартно, на снимке отмечен белыми стрелочками).



Выставьте все настройки так, как это видно на снимке и будет вам счастье. Кнопочка "*Change Identity*" меняет *IP*-адрес и всё остальное. Правда у этого плагина, на каждые 3-4 открытия страниц, появляется рекламный баннер, и это серьёзно раздражает. Но, к сожалению, нечего лучше для *Firefox* в этом отношении мне пока не известно.

Кроме того, можно не устанавливать данный плагин, а воспользоваться *VPN*-соединением в самой системе. Такой вариант, вообще обеспечит соединение с Интернетом через *VPN*-сервер, не только браузеру, а и многим другим приложениям, установленным в систему. Как это сделать, смотрите здесь: http://www.linux-info.ru/vpnbook.html .

Ещё, как один из параноидальных вариантов - это использование сразу двух вышеперечисленных способов одновременно. Таким образом, наше соединение будет проходить через два *VPN*-сервера, что обеспечит удвоенную безопасность, но правда, всё будет работать чуть-чуть медленнее обычного.

Ну и наконец, в дополнение ко всему, могу порекомендовать ещё один нестандартный способ интернет-серфинга. Это, через виртуальную машину, в которой также можно использовать какие-то перечисленные здесь способы для наружной безопасности, а в случае безопасности внутренней, можно спокойно удалить всю виртуальную систему и тем самым, полностью замести следы.

Не сочтите меня параноиком, просто статья она и есть статья и в ней рассматриваются разные аспекты, а поэтому, после того, как вы закончили работать с браузером, для пущей безопасности, ежели вы в таковой нуждаетесь, запустите ещё какую-нибудь утилиту очистки, например: *bleachbit (as root)* или же *Ubuntu Tweak*, которые подчистят то, что должны подчистить. Всё!

Положительные характеристики всего этого:

- Создаём собственную безопасность и анонимность.

Отрицательные характеристики всего этого:

- Безусловно вся эта система будет работать более медленно, чем без неё, особенно это может быть чувствительным при слабом и медленном интернете.

Параметры:

Язык интерфейса: -"-
Лицензия: -"-
Домашняя страница: -"-

Проверялось на *«Ubuntu» 14.04 LTS, Unity (64-bit.).*

Read more http://www.linux-info.ru/firefox-anonimnost.html