How to improve your web browser security - Better securing your personal identity privacy on the Net

Author : admin

Nowadays internet privacy has become a taboo. Many people do understand how vital is it to protect your privacy online.
Unfortunately not much has done much in order to improve their state of security whilst on the net.
In this article you're about to find out how trusted and secure is the browsing in the Internet and next to it you will find some possibleways and thoughts how you can improve your personal privacy and the amount of information your browser reveals about your (habits, interestest, and, lifestyle) while surfing online.
There are a lot of private information that can leak through a simple web serarch, let's say you decide to search for some kind of sickness and it's treatment.. just few minutes later the paid advertisement popping up will be showing up targetting ads related to your previous sickness google search.
This is tiny bit of information your browser reveals, however there is much much more. So let me give you a few more examples:
Let's say you visit a website with an **Adobe Flash** browser player enabled. It's very likely that the website will have flash advertisement this popular this day. If that is the scenario it's very likely that the flash application is built to use Ñ‚Ñ…Đµ so called **flash cookies** supported.
You might have never heard about flash cookies but anyways this one of cookies are one of the most malicious cookies ever invented.
One of the main reason they're so dubious is the fact THEY NEVER EXPIRE!
Though as with normal cookies flash cookies are used for storing user details, let's say your profile details or settings concerning your youtube video player etc. and this sound nice, market guys use the same features to track what you do online.
Using flash cookies for instance everybody who cratefted a **specific adobe flash page is able to list your flash cookies stored browser history!**
To partly setup the behaviour of your Flash player and change the defailt flash player settings for good use the flashplayer settings manager

It's really odd that the only way to configure flash is to configure it via adobe's webpage this is much sneaky since, God only knows what kind of information as well probably your whole flash browser history and flash cookies is being sent Adobe for later analysis.
Moreover the flash player is a propriatary software and this makes it even more likely to have included some extra spying software and stuff alike ..

To see all the stored information by flash about a websites you have visited check out:

flashplayer settings manager

Honestly I was quite shocked when I saw many websites I have visited for the rest 1.5+ year listed.

From hence since we know how "evil" flash storage manager cookies are, one sure step to increase your browser privacy is to periodically get rid of Flash Storage (Flash Cookies).
To achieve periodical flash cookies wipe out on Linux, below I provide you with a tiny .tcsh script which is tested and is working on Debian and Ubuntu. Get rid of Local Flash Storage shell script for Linux
(Stores data of the websites you have visited using your browser flash player)

To check your general Browser security The Electronic Frontier Foundation has developed a special website to test your browser anonymity visit penoptickclick.eff.org and click the > TEST ME button

In my case all my installed browser plugins were listed as well many information related to what kind of browser I use the version on the architecture I'm running on etc. etc.
Thereafter navigate to about:config and set the variable **dom.storage.enabled** to **false** . This will completely disable the DOM cookies which by the way never expire!
DOM cookies aren't so widely used yet but still it's possible that some websites online has stareted using them, since they're completely junky and bad designed for instance DOM a cookie can contant up to (100KB) of information. then it's best that you disable them completely.
Another recommendable thing to disable on your Iceweasel / Firefox that will tighten up your security is the **keyword.enabled** variable click twice on it and assure yourself it reads **false**
Disabling it will prevent the google word suggest to appear each time you type something in Google search box, albeit not every character you type will be sent to Google.

Also a really nice worthy reading is the article explaining dom cookies
Take some time and read it to get a better idea on DOM cookies what they are and why you don't want them.
Likewise take a look at Flash Cookie Forensics for a bit more insight on the **flash cookies**

After reading the article about flash cookies, I came to the conclusion that maybe it's best that they're completely enabled. Anyways if they're disabled then many websites won't work properly which is something we don't want.
It's rather strange that the only available way to control your flash and disable the flash cookies is via Flashplayer Web Based Setting Manager
Since it's **"Web Based Manager"** and it is hosted on Adobe's web site this probably means that everything you do through it gets logged by Adobe, not so nice (neither secure) heh ..

It's recommended also to install and configure the following list of extra Firefox plugins to ensure a bit more Anonimity while surfing on the Internet.

- Adblock Plus
- AntiSocial
- BeeFree
- Beef Taco
- BetterPrivacy
- DownloadHelper
- Download Statusbar
- Live HTTP Headers
- No FB Tracking
- NoScript
- RefControl

Now configure AdBlock plus to work with EasyPrivacy+EasyList (by default it works only with EasyList).
To subscribe for ABP EasyPrivacy click here

BeeFree Mozilla Addon .
Is under the GNU GPL license and it helps you defend a bit more your privacy. It's advantage use is to prevent search engines from knowing which links from their search results is most probably for you to check. Looks like a promising and great stuff
It is said in the add-on website that as a side effect of using the plugin it will probably increase your browser speed.
This post has highly adopted information from the Bulgarian Article by Anton Zinoviev, 2010 About your web browser and the inviolability of your personal life
Big thanks to Anton Zinoviev for the time and effort taken to research on the topic of browser security and write this wonderful thoroughful article.
To configure the **BeeFree Firefox security tightening browser addon** you will have to type in your browser *URL address bar* once again
about:config
Now you will have to look up for the following browser config keys:

extensions.beefree.websites.default.header.accept-charset.action
a
Set it's value to be **2** e.g. **extensions.beefree.websites.default.header.accept-charset.action = 2**
Now look for the key value **extensions.beefree.websites.default.header.accept-charset.value.text** and set it's value to:
/
Changing the **extensions.beefree.websites.default.header.accept-charset.action = */*** will make **BeeFree** compatible to some securing anti spam programs.
Last thing to do to complete the BeeFree configuration create the key value
extensions.beefree.website.generic.header.useragent.action
To create this one press on a random key the last mouse button and select **New -> Integer**
The value for the newly created **extensions.beefree.website.generic.header.useragent.action should**

be set to 4
Creating this key will instruct beefree to protect your browser from revealing it's browser version variable.
Interesting to say each restart of the browser will make **BeeFree** to select a random Firefox Linux or Windows version, dependant of the OS type you use.

The **AntiSocial** addon will prevent your browser from revealing information to **Facebook** about your personal interests. It blocks the facebook elements which are being embedded to your browser by some websites.

No FB Tracking stops facebook of keeping an eye on you through the buttons **"I like"**. Using this buttons facebook can track you even if you're not logged in or registered in the social network.

Installing all this plugins would take you time but considering the privacy is invaluable time shouldn't be a concern of you.
Also some of the plugins like **NoScript** make take some time until you're used to it but it's worth to learn using it.
BetterPrivacy is able and will delete all *flash cookies* when your browser exits, this will prevent that some sites pry on you through the shitty *flash cookies* technology, this type of cookies NEVER EXPIRE! Hard to swallow but a fact ...

In Linux this plugin is reported to work correctly however, in Windows there are dubious reports about it.
This is just a brief overview about how to improve your browsing privacy and therefore general personal data security, there is plenty much already red and said on topic, however I hope this could be some kind of basis for my dear reader for a later research on the topic.