

Forum:[Hack Forums](#)

Thread: [Stay Secure While Browsing! *HUGE* List Of Addons For Firefox That Keep You Safe!](#)

cyberducky - February 7, 2014, 7:53 pm

Hello HF this is Abide. I decided to post some addons for firefox that keep you safe! I hope you enjoy and browse safely!

NOTE: These are not listed in order of importance. I just listed them to make it easier to read.

1. [AdBlock Plus](#)

Info: Spoiler ([Click to View](#)) This can act as a privacy add-on by blocking some elements and cookies that can be used to track you around the web. Make sure you install all three blocklists from fanboy or both blocklists from EasyList. Ghostery offers much of this privacy protection and more, but is more difficult to set up and more likely to interfere with the functionality of some websites. Adblock Plus has a larger community and usually they will discover any problems and hopefully they can be fixed before you're affected.

2. [Web Of Trust - WOT](#)

Info: Spoiler ([Click to View](#)) If you were only going to install one add-on, in most cases I would suggest that it be this one (perhaps accompanied by VTzilla secondly if you like to download software). WOT warns (or can optionally block) sites rated "red" by other users, when you try to visit such a site, regardless of how you got there. It also shows its red-yellow-green ratings on the results in major search engines. It has a very large user base so there's very wide coverage of sites.

3. [HTTPS Everywhere](#)

Info: Spoiler ([Click to View](#)) Many sites on the web offer some limited support for encryption over HTTPS, but make it difficult to use. For instance, they may default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site. The HTTPS Everywhere extension fixes these problems by using a clever technology to rewrite requests to these sites to HTTPS.

4. [Flashblock](#)

Info: Spoiler ([Click to View](#)) I use this to block embedded Flash (& Silverlight) content on unknown sites, especially during periods of time in which Flash has a zero-day (unfixed) security vulnerability, as you might see in the press. You simply click on the Play triangle icon to activate/play the content. Or you can right-click to "whitelist" this site to automatically play such content in the future (then reload/refresh the page to make this effective immediately). An alternative to this addon is Enable Click to Play, which goes further in that it not only blocks Flash/Silverlight, but blocks all other plugin content, for example Java and various media players. But Enable Click to Play it isn't as intuitive to use.

5. [BetterPrivacy](#)

Info: Spoiler ([Click to View](#)) I'm not entirely certain that this is needed in recent versions of Firefox which are supposed to try to apply your "regular" cookie settings to your Flash cookies as well.

Basically the BetterPrivacy safeguard offers various ways to handle Flash-cookies set by Google, YouTube, Ebay and others.

6. [QuickJava](#)

Info: Spoiler ([Click to View](#)) This addon provides buttons to globally toggle Javascript, Images, CSS, and various plugins completely on or off individually. You can't make exceptions on a particular page or whitelist a site like you can in Enable Click To Play (or Flashblock, just for Flash/Silverlight). The benefit is that you can completely disable specific plugins (or non-plugin features like Images or CSS) independently of one another. You have to customize one of your toolbars to drag the buttons for the individual plugins/features of interest onto it. The number of buttons becomes unwieldy if you want this capability for more than a few plugins/features.

7. [Cookies Manager+](#)

Info: Spoiler ([Click to View](#)) Overkill for most of us for day-to-day use, but I've found it useful when I want to selectively "clean up" my cookies, sorting them by expiration date or creation date to either delete them or just change their expiration date.

8. [Google/Yandex search link fix](#)

Info: Spoiler ([Click to View](#)) This extension prevents Google Search from modifying result links when they are clicked.

9. [WorldIP - Geo Add-on with Security Features](#)

Info: Spoiler ([Click to View](#)) This addon shows country, city, & other info for current site. If it looks wrong for a familiar site then you could be on a phony/phishing site. This is a more compact alternative to "Website City + Country Info" (or you could use both). Shows a lot of info when you hover over it. Can only be placed in the address/location bar (flag icon only) or in the addon/status bar (chosen information). It can't be dragged to another toolbar (except using an addon like UI Fixer or MarMod 2 to make the entire set of unmovable addon bar items draggable together to another toolbar.) Doesn't show the Organization like Website City... does, though the "Provider" often gives similar information.

10. [Cookie Controller](#)

Info: Spoiler ([Click to View](#)) After installing this add-on, I suggest dragging only the Cookie Permissions button onto the toolbar -- this is the site-specific one. You can get to the other functions via the legacy Tools menu (Alt+t) --> CookieController. For starters you can use that menu to go into "about:config...". There, you can set `network.cookie.thirdparty.sessionOnly = true`, `network.cookie.lifetimePolicy = 3`, and `network.cookie.lifetime.days = 8`. This means by default each cookie will expire if you don't actually visit their site for 8 days (you can choose a different number of days). If they set the cookie via another site you visited (as a "third party"), then the cookie will expire as soon as you end your browser session (though see warning about this in my notes for the Select Tabs to Restore addon). This will reduce the chance of being tracked over long periods of time, without the risk of a site not working because of cookies you blocked completely. You can use Cookie Controller to easily set exceptions for sites that you want to recognize you for longer periods of time, e.g. if you don't want to have to login again every week or re-answer your security questions at a banking site: simply click on the Cookie Permissions toolbar button (right-click for more choices).

11. Looking for plugin to put here

12. [Webutation - Reputation & Security](#)

Info: Spoiler ([Click to View](#)) Another aggregator of website reputation services, although it has some of its own rating capability. This one doesn't do anything with search results or warning or blocking; in this respect it's less capable than WOT.

13. [BrowserProtect](#)

Info: Spoiler ([Click to View](#)) This addon is designed to help protect you against having your browser configuration changed (e.g. by an add-on) without your knowledge, which seems like a good idea if it works. I've been using it but I haven't tested it by trying to get a change that it should catch so I can't yet vouch for its effectiveness. It hasn't warned me yet, so at least it doesn't appear to be intrusive by giving a lot of false positives.

14. [Muter](#)

Info: Spoiler ([Click to View](#)) This is a "mute" button for the browser. It can protect you from intrusive audio (including the audio track of video and flash) that may start playing automatically and unexpectedly when you visit a site. It thus protects your privacy because it prevents others around you from accidentally hearing audio.

15. [Enable Click To Play](#)

Info: Spoiler ([Click to View](#)) Enabling this addon is an easy way to switch on Firefox's built-in but hidden "click to play" feature: it prevents plugin content (Flash, Java, etc) from playing (executing) by default until you click on it to activate it. Once you realize that there's a special puzzle-piece icon at the left of the location bar (left of URL & its icon/id) when you're on a page with unactivated (unclicked) content, you can click on the button to activate all plugins on the page at once. Or even pull down the button menu on its dialog, in order to permanently allow (whitelist) this particular site so its plugins will play in the future without clicking. Annoyingly, once you've whitelisted the site, you may not be able to remove it from the whitelist except by using Firefox's own unfriendly method: go to the URL "about:permissions" (no quotes) to click on the site and change Plugins to "Allow". FlashBlock is an alternative addon that's nicer in that activating the entire page or whitelisting the site is much more intuitive: just right click on the "blocked" addon itself or use a flashblock button that you can put on any toolbar. You can also use the button to easily remove the site from the whitelist. But see my comments on Flashblock -- it doesn't block all plugins. Flashblock pre-dates and doesn't use Firefox's own "click to play" feature. I've also read that Flashblock works at the domain level, so you don't have to separately whitelist every site in the same domain (e.g. site1.something.com, site2.something.com, etc.). If using Enable Click to Play, you simply disable this plugin if you want to disable this feature and play all content on all sites without clicking -- no restart is required when you enable or disable this plugin. Eventually (some time in 2013 or 2014?), Firefox might get features that let you more-easily control Click To Play, more like Flashblock.

16. [VTzilla](#)

Info: Spoiler ([Click to View](#)) Very useful for pre-screening downloads for badware -- especially if you like to download software !! Initially it just gives you information based on the site. But if you're sending the actual download file URL, you can then click "Downloaded File Analysis" in the result to get an actual multi-engine antivirus scan of the file itself before you download it yourself! Aside from

the obvious benefits of not having to download and then upload a file to VirusTotal, this also avoids the possibility that you might inadvertently upload a private file to VirusTotal. For example a file with your personal information that you were able to download from a site while logged into your account. By sending such a file to virustotal, you are in effect releasing it to a couple of dozen antimalware companies, which you might want to do. If using this extension, VirusTotal will only be able to access public URLs so you don't have that risk. Sometimes it doesn't work if the "download" URL merely redirects to the actual file URL, or if it uses parameters and/or no explicit file extension. It would be nice if it could be smarter about those. I hide the annoying toolbar. Unfortunately you can't drag its buttons or fields onto another toolbar, but I get the same functionality with two bookmarklets.

17. [Perspectives](#)

Info: Spoiler ([Click to View](#)) Just slightly intrusive with a red bar at the top when you visit a site that's identifying itself using a new or different certificate than it usually has been. This bar means you should use caution because you could be on a fake or phishing site. So then you could try re-typing the address by hand (rather than getting there via a link), or else check some of the other tools in this collection to see if they indicate a problem. May give quite a few "false positives" but it lets you whitelist them so it won't warn about the same site again. I strongly recommend setting its options so it does NOT "automatically override security errors" -- that setting is too dangerous!

18. [Padlock](#)

Info: Spoiler ([Click to View](#)) This extension will change the looks of Firefox whenever a website is secured by SSL, therefore you can easily tell whether you are safe to login to certain websites.

19. [FormFox](#)

Info: Spoiler ([Click to View](#)) When you hover over a form's Submit button, this add-on displays a tooltip with the address to which the form will be submitted. You can see whether it's https vs http and whether it's being submitted to the site you're on (vs a third party that has it in embedded content).

20. [Master Password Timeout](#)

Info: Spoiler ([Click to View](#)) In any case, with or without this add-on, if you save website passwords in Firefox it's essential to HAVE A MASTER PASSWORD (Options-->Security). Mainly because it's the only thing that prevents someone from going into the password manager and do "Show All Passwords" and steal ALL your stored passwords. Fortunately, when they try to show all passwords, Firefox will prompt for the master password (if you have one!) for this action even if you've already entered the master password. Beyond that, if you want to also prevent someone from sitting down at your computer when you walk away and logging into a site using your stored password, you should also install the Master Password Timeout (Updated) add-on -- otherwise you're only prompted for the master password once and then your stored passwords can be used for the rest of your session even if you walk away and leave it open for hours. This add-on doesn't make you re-enter your master password unless you've been inactive for a specified period of time. However, if you already have a screen saver password or similar auto-lock for your entire computer session, there may be little benefit to installing this add-on unless you want to use it to set a shorter timeout than your screen saver lock.

Thanks for reading the entire thread! And if you have chrome don't worry! I will be releasing another

thread specifically for google chrome users in the near future! Stay tuned!

Corso - February 7, 2014, 10:15 pm

Some are good, a few are borderline adware/junkware types... Over all each one is worth looking into and determining if it's usage fits your needs.

Capwne - February 8, 2014, 3:18 pm

This is very helpful I just converted from Google chrome to Firefox. Must say I'm enjoying Firefox much more than chrome.

Chief Keef. - February 8, 2014, 8:35 pm

This is quite useful, I may use some of these addons!

Gustav. - February 9, 2014, 7:00 am

This is indeed an informative thread. Good job.

Null Byte - February 9, 2014, 5:42 pm

Revised list for you:

1. NoScript
2. Adblock
3. VPN
4. (optional) HTTPS Everywhere
5. Set java security level to very high (via control panel)

That is all you need to stay secure. Seriously.