**user.js**

**Firefox configuration hardening**

A [user.js](http://kb.mozillazine.org/User.js_file) configuration file for [Mozilla Firefox](https://www.mozilla.org/en-US/firefox/new/) designed to harden browser settings and make it more secure.

**This is a default template with every possible hardening measure enforced. See the**[**relaxed branch**](https://github.com/pyllyukko/user.js/tree/relaxed)**for a variant providing more usability**

**Main goals**

* Limit the possibilities to track the user through [web analytics](https://en.wikipedia.org/wiki/Web_analytics).
* Harden the browser against known data disclosure or code execution vulnerabilities.
* Limit the browser from storing anything even remotely sensitive persistently.
* Make sure the browser doesn't reveal too much information to [shoulder surfers](https://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29).
* Harden the browser's encryption (cipher suites, protocols, trusted CAs).
* Limit possibilities to uniquely identify the browser/device using [browser fingerprinting](https://en.wikipedia.org/wiki/Device_fingerprint).
* Hopefully limit the attack surface by disabling various features.
* Still be usable in daily use.

**How to achieve this?**

There are several parts to all this and they are:

* [Downloading](https://github.com/pyllyukko/user.js#download) and [installing](https://github.com/pyllyukko/user.js#installation) the user.js file.
* Reading about and applying [further hardening](https://github.com/pyllyukko/user.js#further-hardening) techniques.
* *Optional:* Modifying user.js to adapt it to your web browser usage.
* [Download](https://github.com/pyllyukko/user.js#download)
* [Installation](https://github.com/pyllyukko/user.js#installation)
* [What does it do?](https://github.com/pyllyukko/user.js#what-does-it-do)
* [Further hardening](https://github.com/pyllyukko/user.js#further-hardening)
* [Known problems and limitations](https://github.com/pyllyukko/user.js#known-problems-and-limitations)
* [FAQ](https://github.com/pyllyukko/user.js#faq)
* [Contributing](https://github.com/pyllyukko/user.js#contributing)
* [Online tests](https://github.com/pyllyukko/user.js#online-tests)
* [References](https://github.com/pyllyukko/user.js#references)

**Download**

Different download methods are available:

* Clone using git: git clone https://github.com/pyllyukko/user.js
* Download and extract the [ZIP file](https://github.com/pyllyukko/user.js/archive/master.zip) containing the latest version.
* Download the latest user.js [directly](https://raw.githubusercontent.com/pyllyukko/user.js/master/user.js)

**Installation**

**Backups**

Do note that these settings alter your browser behaviour quite a bit, so it is recommended to either create a completely new [profile](https://mzl.la/NYhKHH) for Firefox or backup your existing [profile directory](http://kb.mozillazine.org/Profile_folder_-_Firefox) before putting the user.js file in place.

To enable the Profile Manager, run Firefox with [command-line arguments](http://kb.mozillazine.org/Command_line_arguments): firefox --no-remote -P

**Single profile installation**

Copy user.js in your current user profile directory, or (recommended) to a fresh, newly created Firefox profile directory.

The file should be located at:

| **OS** | **Path** |
| --- | --- |
| Windows 7 | %APPDATA%\Mozilla\Firefox\Profiles\XXXXXXXX.your\_profile\_name\user.js |
| Linux | ~/.mozilla/firefox/XXXXXXXX.your\_profile\_name/user.js |
| OS X | ~/Library/Application Support/Firefox/Profiles/XXXXXXXX.your\_profile\_name |
| Android | /data/data/org.mozilla.firefox/files/mozilla/XXXXXXXX.your\_profile\_name and see [issue #14](https://github.com/pyllyukko/user.js/issues/14) |
| Sailfish OS + Alien Dalvik | /opt/alien/data/data/org.mozilla.firefox/files/mozilla/XXXXXXXX.your\_profile\_name |
| Windows (portable) | [firefox directory]\Data\profile\ |

With this installation method, if you change any of user.js settings through [about:config](http://kb.mozillazine.org/About:config) or Firefox preferences dialogs, they will be reset to the user.js defined values after you restart Firefox. This makes sure they're always back to secure defaults when starting the browser. However this prevents persistently changing settings you don't consider appropriate. Either edit user.js directly, or use the system-wide installation method described below.

**System-wide installation (all platforms)**

Generate a file suitable for system-wide installation, by running make with one of the following targets:

* systemwide\_user.js: (the value will be used as default value for all Firefox Profiles where it is not explicitly set, it can be changed in about:config and is kept across browser sessions)
* locked\_user.js: (the value will be used as default value on Firefox profile creation, will be locked and can't be changed) in user.js or in Firefox's about:config or settings.
* debian\_locked.js: Debian specific. Users are not able to override preferences. See [#415](https://github.com/pyllyukko/user.js/issues/415).

Copy the produced file to the Firefox installation directory. The file should be located at:

| **OS** | **Path** |
| --- | --- |
| Windows | C:\Program Files (x86)\Mozilla Firefox\mozilla.cfg |
| Linux | /etc/firefox/syspref.js, for older versions: /etc/firefox/firefox.js |
| Linux (Debian) | /etc/firefox-esr/firefox-esr.js |
| Linux (Gentoo, Archlinux) | /usr/lib/firefox/mozilla.cfg, might also be /usr/lib32/ or /usr/lib64/ |
| OS X | /Applications/Firefox.app/Contents/Resources/mozilla.cfg |

**Additional installation steps for Windows / OS X / Gentoo / Archlinux**

Create local-settings.js in Firefox installation directory, with the following contents:

pref("general.config.obscure\_value", 0);

pref("general.config.filename", "mozilla.cfg");

This file should be located at:

| **OS** | **Path** |
| --- | --- |
| Windows | C:\Program Files (x86)\Mozilla Firefox\defaults\pref\ |
| OS X | /Applications/Firefox.app/Contents/Resources/defaults/pref |
| Linux (Gentoo, Archlinux) | /usr/lib/firefox/defaults/pref/, might also be /usr/lib32/ or /usr/lib64/ |

If mozilla.cfg still fails to load, you must add a blank comment to the top of mozilla.cfg like so:

//

**Updating using git**

For any of the above methods, you can keep your browser's user.js with the latest version available here: Clone the repository, and create a symbolic link from the appropriate location to the user.js file in the repository. Just run git pull in the repository when you want to update, then restart Firefox:

cd ~/.mozilla/firefox

git clone 'https://github.com/pyllyukko/user.js.git'

cd XXXXXXXX.your\_profile\_name

ln -s ../user.js/user.js user.js

**Verifying**

Verify that the settings are effective from [about:support](http://kb.mozillazine.org/Troubleshooting_Information_report#Modified_Preferences) (check the "Important Modified Preferences" and "user.js Preferences" sections).

**What does it do?**

There's a whole lot of settings that this modifies and they are divided in the following sections.

Some of the settings in this user.js file might seem redundant, as some of them are already set to the same values by default. We chose to explicitely set their values, which ensures these settings are enforced if a future Firefox update changes the default value.

**HTML5 / APIs / DOM**

HTML5 / [APIs](https://wiki.mozilla.org/WebAPI) / [DOM](https://en.wikipedia.org/wiki/Document_Object_Model) related settings. Mozilla is keen to implement every new HTML5 feature, which have had unforeseen security or privacy implications. This section disables many of those new and yet to be proven technologies.

* Disable Service Workers [ [1](https://developer.mozilla.org/en-US/docs/Web/API/Worker) [2](https://developer.mozilla.org/en-US/docs/Web/API/ServiceWorker_API) [3](https://wiki.mozilla.org/Firefox/Push_Notifications#Service_Workers) ]
* Disable web notifications [ [1](https://support.mozilla.org/en-US/questions/1140439) ]
* Disable DOM timing API [ [1](https://wiki.mozilla.org/Security/Reviews/Firefox/NavigationTimingAPI) [2](https://www.w3.org/TR/navigation-timing/#privacy) ]
* Make sure the User Timing API does not provide a new high resolution timestamp [ [1](https://trac.torproject.org/projects/tor/ticket/16336) [2](https://www.w3.org/TR/2013/REC-user-timing-20131212/#privacy-security) ]
* Disable Web Audio API [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1288359) ]
* Disable Location-Aware Browsing (geolocation) [ [1](https://www.mozilla.org/en-US/firefox/geolocation/) ]
* When geolocation is enabled, use Mozilla geolocation service instead of Google [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=689252) ]
* When geolocation is enabled, don't log geolocation requests to the console
* Disable raw TCP socket support (mozTCPSocket) [ [1](https://trac.torproject.org/projects/tor/ticket/18863) [2](https://www.mozilla.org/en-US/security/advisories/mfsa2015-97/) [3](https://developer.mozilla.org/docs/Mozilla/B2G_OS/API/TCPSocket) ]
* Disable leaking network/browser connection information via Javascript
* Disable network API [ [1](https://developer.mozilla.org/en-US/docs/Web/API/Connection/onchange) [2](https://www.torproject.org/projects/torbrowser/design/#fingerprinting-defenses) ]
* Disable WebRTC entirely to prevent leaking internal IP addresses (Firefox < 42)
* Don't reveal your internal IP when WebRTC is enabled (Firefox >= 42) [ [1](https://wiki.mozilla.org/Media/WebRTC/Privacy) [2](https://github.com/beefproject/beef/wiki/Module%3A-Get-Internal-IP-WebRTC) ]
* Disable WebRTC getUserMedia, screen sharing, audio capture, video capture [ [1](https://wiki.mozilla.org/Media/getUserMedia) [2](https://blog.mozilla.org/futurereleases/2013/01/12/capture-local-camera-and-microphone-streams-with-getusermedia-now-enabled-in-firefox/) [3](https://developer.mozilla.org/en-US/docs/Web/API/Navigator) ]
* Disable battery API (Firefox < 52) [ [1](https://developer.mozilla.org/en-US/docs/Web/API/BatteryManager) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1313580) ]
* Disable telephony API [ [1](https://wiki.mozilla.org/WebAPI/Security/WebTelephony) ]
* Disable "beacon" asynchronous HTTP transfers (used for analytics) [ [1](https://developer.mozilla.org/en-US/docs/Web/API/navigator.sendBeacon) ]
* Disable clipboard event detection (onCut/onCopy/onPaste) via Javascript
* Disable "copy to clipboard" functionality via Javascript (Firefox >= 41)
* Disable speech recognition [ [1](https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html) [2](https://developer.mozilla.org/en-US/docs/Web/API/SpeechRecognition) [3](https://wiki.mozilla.org/HTML5_Speech_API) ]
* Disable speech synthesis [ [1](https://developer.mozilla.org/en-US/docs/Web/API/SpeechSynthesis) ]
* Disable sensor API [ [1](https://wiki.mozilla.org/Sensor_API) ]
* Disable pinging URIs specified in HTML ping= attributes [ [1](http://kb.mozillazine.org/Browser.send_pings) ]
* When browser pings are enabled, only allow pinging the same host as the origin page [ [1](http://kb.mozillazine.org/Browser.send_pings.require_same_host) ]
* Disable gamepad API to prevent USB device enumeration [ [1](https://www.w3.org/TR/gamepad/) [2](https://trac.torproject.org/projects/tor/ticket/13023) ]
* Disable virtual reality devices APIs [ [1](https://developer.mozilla.org/en-US/Firefox/Releases/36#Interfaces.2FAPIs.2FDOM) [2](https://developer.mozilla.org/en-US/docs/Web/API/WebVR_API) ]
* Disable vibrator API
* Disable resource timing API [ [1](https://www.w3.org/TR/resource-timing/#privacy-security) ]
* Disable Archive API (Firefox < 54) [ [1](https://wiki.mozilla.org/WebAPI/ArchiveAPI) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1342361) ]
* Disable webGL [ [1](https://en.wikipedia.org/wiki/WebGL) [2](https://www.contextis.com/resources/blog/webgl-new-dimension-browser-exploitation/) ]
* When webGL is enabled, use the minimum capability mode
* When webGL is enabled, disable webGL extensions [ [1](https://developer.mozilla.org/en-US/docs/Web/API/WebGL_API#WebGL_debugging_and_testing) ]
* When webGL is enabled, force enabling it even when layer acceleration is not supported [ [1](https://trac.torproject.org/projects/tor/ticket/18603) ]
* When webGL is enabled, do not expose information about the graphics driver [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1171228) [2](https://developer.mozilla.org/en-US/docs/Web/API/WEBGL_debug_renderer_info) ]
* Spoof dual-core CPU [ [1](https://trac.torproject.org/projects/tor/ticket/21675) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1360039) ]
* Disable WebAssembly [ [1](https://webassembly.org/) [2](https://en.wikipedia.org/wiki/WebAssembly) [3](https://trac.torproject.org/projects/tor/ticket/21549) ]

**Misc**

Settings that do not belong to other sections or are user specific preferences.

* Disable face detection
* Disable GeoIP lookup on your address to set default search engine region [ [1](https://trac.torproject.org/projects/tor/ticket/16254) [2](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections#w_geolocation-for-default-search-engine) ]
* Set Accept-Language HTTP header to en-US regardless of Firefox localization [ [1](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Accept-Language) ]
* Set Firefox locale to en-US [ [1](http://kb.mozillazine.org/General.useragent.locale) ]
* Don't use OS values to determine locale, force using Firefox locale setting [ [1](http://kb.mozillazine.org/Intl.locale.matchOS) ]
* Don't use Mozilla-provided location-specific search engines
* Do not automatically send selection to clipboard on some Linux platforms [ [1](http://kb.mozillazine.org/Clipboard.autocopy) ]
* Prevent leaking application locale/date format using JavaScript [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=867501) [2](https://hg.mozilla.org/mozilla-central/rev/52d635f2b33d) ]
* Do not submit invalid URIs entered in the address bar to the default search engine [ [1](http://kb.mozillazine.org/Keyword.enabled) ]
* Don't trim HTTP off of URLs in the address bar. [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=665580) ]
* Don't try to guess domain names when entering an invalid domain name in URL bar [ [1](http://www-archive.mozilla.org/docs/end-user/domain-guessing.html) ]
* When browser.fixup.alternate.enabled is enabled, strip password from 'user:password@...' URLs [ [1](https://github.com/pyllyukko/user.js/issues/290#issuecomment-303560851) ]
* Send DNS request through SOCKS when SOCKS proxying is in use [ [1](https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO/WebBrowsers) ]
* Don't monitor OS online/offline connection state [ [1](https://trac.torproject.org/projects/tor/ticket/18945) ]
* Enforce Mixed Active Content Blocking [ [1](https://support.mozilla.org/t5/Protect-your-privacy/Mixed-content-blocking-in-Firefox/ta-p/10990) [2](https://developer.mozilla.org/en-US/docs/Site_Compatibility_for_Firefox_23#Non-SSL_contents_on_SSL_pages_are_blocked_by_default) [3](https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/) ]
* Enforce Mixed Passive Content blocking (a.k.a. Mixed Display Content)
* Disable JAR from opening Unsafe File Types [ [1](http://kb.mozillazine.org/Network.jar.open-unsafe-types) ]
* Set File URI Origin Policy [ [1](http://kb.mozillazine.org/Security.fileuri.strict_origin_policy) ]
* Disable Displaying Javascript in History URLs [ [1](http://kb.mozillazine.org/Browser.urlbar.filter.javascript) ]
* Disable asm.js [ [1](http://asmjs.org/) [2](https://www.mozilla.org/en-US/security/advisories/mfsa2015-29/) [3](https://www.mozilla.org/en-US/security/advisories/mfsa2015-50/) [4](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2712) ]
* Disable SVG in OpenType fonts [ [1](https://wiki.mozilla.org/SVGOpenTypeFonts) [2](https://github.com/iSECPartners/publications/tree/master/reports/Tor%20Browser%20Bundle) ]
* Disable video stats to reduce fingerprinting threat [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=654550) [2](https://github.com/pyllyukko/user.js/issues/9#issuecomment-100468785) [3](https://github.com/pyllyukko/user.js/issues/9#issuecomment-148922065) ]
* Don't reveal build ID
* Don't use document specified fonts to prevent installed font enumeration (fingerprinting) [ [1](https://github.com/pyllyukko/user.js/issues/395) [2](https://browserleaks.com/fonts) [3](https://github.com/pyllyukko/user.js/issues/120) ]
* Enable only whitelisted URL protocol handlers [ [1](http://kb.mozillazine.org/Network.protocol-handler.external-default) [2](http://kb.mozillazine.org/Network.protocol-handler.warn-external-default) [3](http://kb.mozillazine.org/Network.protocol-handler.expose.%28protocol%29) [4](https://news.ycombinator.com/item?id=13047883) [5](https://bugzilla.mozilla.org/show_bug.cgi?id=167475) [6](https://github.com/pyllyukko/user.js/pull/285#issuecomment-298124005) ]

**Extensions / plugins**

Harden preferences related to external plugins

* Ensure you have a security delay when installing add-ons (milliseconds) [ [1](http://kb.mozillazine.org/Disable_extension_install_delay_-_Firefox) [2](http://www.squarefree.com/2004/07/01/race-conditions-in-security-dialogs/) ]
* Require signatures [ [1](https://wiki.mozilla.org/Addons/Extension_Signing) ]
* Opt-out of add-on metadata updates [ [1](https://blog.mozilla.org/addons/how-to-opt-out-of-add-on-metadata-updates/) ]
* Opt-out of themes (Persona) updates [ [1](https://support.mozilla.org/t5/Firefox/how-do-I-prevent-autoamtic-updates-in-a-50-user-environment/td-p/144287) ]
* Disable Flash Player NPAPI plugin [ [1](http://kb.mozillazine.org/Flash_plugin) ]
* Disable Java NPAPI plugin
* Disable sending Flash Player crash reports
* When Flash crash reports are enabled, don't send the visited URL in the crash report
* When Flash is enabled, download and use Mozilla SWF URIs blocklist [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1237198) [2](https://github.com/mozilla-services/shavar-plugin-blocklist) ]
* Disable Shumway (Mozilla Flash renderer) [ [1](https://developer.mozilla.org/en-US/docs/Mozilla/Projects/Shumway) ]
* Disable Gnome Shell Integration NPAPI plugin
* Enable plugins click-to-play [ [1](https://wiki.mozilla.org/Firefox/Click_To_Play) [2](https://blog.mozilla.org/security/2012/10/11/click-to-play-plugins-blocklist-style/) ]
* Updates addons automatically [ [1](https://blog.mozilla.org/addons/how-to-turn-off-add-on-updates/) ]
* Enable add-on and certificate blocklists (OneCRL) from Mozilla [ [1](https://wiki.mozilla.org/Blocklisting) [2](https://blocked.cdn.mozilla.net/) [3](http://kb.mozillazine.org/Extensions.blocklist.enabled) [4](http://kb.mozillazine.org/Extensions.blocklist.url) [5](https://blog.mozilla.org/security/2015/03/03/revoking-intermediate-certificates-introducing-onecrl/) ]
* Decrease system information leakage to Mozilla blocklist update servers [ [1](https://trac.torproject.org/projects/tor/ticket/16931) ]
* Disable system add-on updates (hidden & always-enabled add-ons from Mozilla) [ [1](https://firefox-source-docs.mozilla.org/toolkit/mozapps/extensions/addon-manager/SystemAddons.html) [2](https://blog.mozilla.org/data/2018/08/20/effectively-measuring-search-in-firefox/) [3](https://github.com/pyllyukko/user.js/issues/419) [4](https://dxr.mozilla.org/mozilla-central/source/toolkit/mozapps/extensions/AddonManager.jsm#1248-1257) ]

**Firefox (anti-)features / components**

Disable Firefox integrated metrics/reporting/experiments, disable potentially insecure/invasive/[undesirable](https://en.wikipedia.org/wiki/Feature_creep) features

* Disable Extension recommendations (Firefox >= 65) [ [1](https://support.mozilla.org/en-US/kb/extension-recommendations) ]
* Disable WebIDE [ [1](https://trac.torproject.org/projects/tor/ticket/16222) [2](https://developer.mozilla.org/docs/Tools/WebIDE) ]
* Disable remote debugging [ [1](https://developer.mozilla.org/en-US/docs/Tools/Remote_Debugging/Debugging_Firefox_Desktop) [2](https://developer.mozilla.org/en-US/docs/Tools/Tools_Toolbox#Advanced_settings) ]
* Disable Mozilla telemetry/experiments [ [1](https://wiki.mozilla.org/Platform/Features/Telemetry) [2](https://wiki.mozilla.org/Privacy/Reviews/Telemetry) [3](https://wiki.mozilla.org/Telemetry) [4](https://www.mozilla.org/en-US/legal/privacy/firefox.html#telemetry) [5](https://support.mozilla.org/t5/Firefox-crashes/Mozilla-Crash-Reporter/ta-p/1715) [6](https://wiki.mozilla.org/Security/Reviews/Firefox6/ReviewNotes/telemetry) [7](https://gecko.readthedocs.io/en/latest/browser/experiments/experiments/manifest.html) [8](https://wiki.mozilla.org/Telemetry/Experiments) [9](https://support.mozilla.org/en-US/questions/1197144) [10](https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/telemetry/internals/preferences.html#id1) ]
* Disallow Necko to do A/B testing [ [1](https://trac.torproject.org/projects/tor/ticket/13170) ]
* Disable sending Firefox crash reports to Mozilla servers [ [1](https://wiki.mozilla.org/Breakpad) [2](http://kb.mozillazine.org/Breakpad) [3](https://dxr.mozilla.org/mozilla-central/source/toolkit/crashreporter) [4](https://bugzilla.mozilla.org/show_bug.cgi?id=411490) ]
* Disable sending reports of tab crashes to Mozilla (about:tabcrashed), don't nag user about unsent crash reports [ [1](https://hg.mozilla.org/mozilla-central/file/tip/browser/app/profile/firefox.js) ]
* Disable FlyWeb (discovery of LAN/proximity IoT devices that expose a Web interface) [ [1](https://wiki.mozilla.org/FlyWeb) [2](https://wiki.mozilla.org/FlyWeb/Security_scenarios) [3](https://docs.google.com/document/d/1eqLb6cGjDL9XooSYEEo7mE-zKQ-o-AuDTcEyNhfBMBM/edit) [4](http://www.ghacks.net/2016/07/26/firefox-flyweb) ]
* Disable the UITour backend [ [1](https://trac.torproject.org/projects/tor/ticket/19047#comment:3) ]
* Enable Firefox Tracking Protection [ [1](https://wiki.mozilla.org/Security/Tracking_protection) [2](https://support.mozilla.org/en-US/kb/tracking-protection-firefox) [3](https://support.mozilla.org/en-US/kb/tracking-protection-pbm) [4](https://kontaxis.github.io/trackingprotectionfirefox/) [5](https://feeding.cloud.geek.nz/posts/how-tracking-protection-works-in-firefox/) ]
* Enable contextual identity Containers feature (Firefox >= 52)
* Enable Firefox's anti-fingerprinting mode ("resist fingerprinting" or RFP) (Tor Uplift project) [ [1](https://wiki.mozilla.org/Security/Tor_Uplift/Tracking) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1333933) [3](https://wiki.mozilla.org/Security/Fingerprinting) ]
* disable mozAddonManager Web API [FF57+] [ [1](https://bugzilla.mozilla.org/buglist.cgi?bug_id=1384330) [2](https://bugzilla.mozilla.org/buglist.cgi?bug_id=1406795) [3](https://bugzilla.mozilla.org/buglist.cgi?bug_id=1415644) [4](https://bugzilla.mozilla.org/buglist.cgi?bug_id=1453988) [5](https://trac.torproject.org/projects/tor/ticket/26114) ]
* disable showing about:blank/maximized window as soon as possible during startup [FF60+] [ [1](https://bugzilla.mozilla.org/1448423) ]
* Disable the built-in PDF viewer [ [1](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2743) [2](https://blog.mozilla.org/security/2015/08/06/firefox-exploit-found-in-the-wild/) [3](https://www.mozilla.org/en-US/security/advisories/mfsa2015-69/) ]
* Disable collection/sending of the health report (healthreport.sqlite\*) [ [1](https://support.mozilla.org/en-US/kb/firefox-health-report-understand-your-browser-perf) [2](https://gecko.readthedocs.org/en/latest/toolkit/components/telemetry/telemetry/preferences.html) ]
* Disable Shield/Heartbeat/Normandy (Mozilla user rating telemetry) [ [1](https://wiki.mozilla.org/Advocacy/heartbeat) [2](https://trac.torproject.org/projects/tor/ticket/19047) [3](https://trac.torproject.org/projects/tor/ticket/18738) [4](https://wiki.mozilla.org/Firefox/Shield) [5](https://github.com/mozilla/normandy) [6](https://support.mozilla.org/en-US/kb/shield) [7](https://bugzilla.mozilla.org/show_bug.cgi?id=1370801) ]
* Disable Firefox Hello metrics collection [ [1](https://groups.google.com/d/topic/mozilla.dev.platform/nyVkCx-_sFw/discussion) ]
* Enforce checking for Firefox updates [ [1](http://kb.mozillazine.org/App.update.enabled) ]
* Enable blocking reported web forgeries [ [1](https://wiki.mozilla.org/Security/Safe_Browsing) [2](http://kb.mozillazine.org/Safe_browsing) [3](https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work) [4](http://forums.mozillazine.org/viewtopic.php?f=39&t=2711237&p=12896849#p12896849) ]
* Enable blocking reported attack sites [ [1](http://kb.mozillazine.org/Browser.safebrowsing.malware.enabled) ]
* Disable querying Google Application Reputation database for downloaded binary files [ [1](https://www.mozilla.org/en-US/firefox/39.0/releasenotes/) [2](https://wiki.mozilla.org/Security/Application_Reputation) ]
* Disable Pocket [ [1](https://support.mozilla.org/en-US/kb/save-web-pages-later-pocket-firefox) [2](https://github.com/pyllyukko/user.js/issues/143) ]
* Disable "Recommended by Pocket" in Firefox Quantum

**Automatic connections**

Prevents the browser from [auto-connecting](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections) to some Mozilla services, and from predictively opening connections to websites during browsing.

* Disable prefetching of URLs [ [1](http://kb.mozillazine.org/Network.prefetch-next) [2](https://developer.mozilla.org/en-US/docs/Web/HTTP/Link_prefetching_FAQ#Is_there_a_preference_to_disable_link_prefetching.3F) ]
* Disable DNS prefetching [ [1](http://kb.mozillazine.org/Network.dns.disablePrefetch) [2](https://developer.mozilla.org/en-US/docs/Web/HTTP/Controlling_DNS_prefetching) ]
* Disable the predictive service (Necko) [ [1](https://wiki.mozilla.org/Privacy/Reviews/Necko) ]
* Reject .onion hostnames before passing the to DNS [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1228457) ]
* Disable search suggestions in the search bar [ [1](http://kb.mozillazine.org/Browser.search.suggest.enabled) ]
* Disable "Show search suggestions in location bar results"
* When using the location bar, don't suggest URLs from browsing history
* Disable SSDP [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1111967) ]
* Disable automatic downloading of OpenH264 codec [ [1](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections#w_media-capabilities) [2](https://andreasgal.com/2014/10/14/openh264-now-in-firefox/) ]
* Disable speculative pre-connections [ [1](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections#w_speculative-pre-connections) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=814169) ]
* Disable downloading homepage snippets/messages from Mozilla [ [1](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections#w_mozilla-content) [2](https://wiki.mozilla.org/Firefox/Projects/Firefox_Start/Snippet_Service) ]
* Never check updates for search engines [ [1](https://support.mozilla.org/en-US/kb/how-stop-firefox-making-automatic-connections#w_auto-update-checking) ]
* Disable automatic captive portal detection (Firefox >= 52.0) [ [1](https://support.mozilla.org/en-US/questions/1157121) ]

**HTTP**

HTTP protocol related entries. This affects cookies, the user agent, referer and others.

* Disallow NTLMv1 [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=828183) ]
* Enable CSP 1.1 script-nonce directive support [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=855326) ]
* Enable Content Security Policy (CSP) [ [1](https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy) [2](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) ]
* Enable Subresource Integrity [ [1](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity) [2](https://wiki.mozilla.org/Security/Subresource_Integrity) ]
* Don't send referer headers when following links across different domains [ [1](https://github.com/pyllyukko/user.js/issues/227) [2](https://github.com/pyllyukko/user.js/issues/328) [3](https://feeding.cloud.geek.nz/posts/tweaking-referrer-for-privacy-in-firefox/) ]
* Accept Only 1st Party Cookies [ [1](http://kb.mozillazine.org/Network.cookie.cookieBehavior#1) ]
* Enable first-party isolation [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1299996) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1260931) [3](https://wiki.mozilla.org/Security/FirstPartyIsolation) ]
* Make sure that third-party cookies (if enabled) never persist beyond the session. [ [1](https://feeding.cloud.geek.nz/posts/tweaking-cookies-for-privacy-in-firefox/) [2](http://kb.mozillazine.org/Network.cookie.thirdparty.sessionOnly) [3](https://developer.mozilla.org/en-US/docs/Cookies_Preferences_in_Mozilla#network.cookie.thirdparty.sessionOnly) ]

**Caching**

Enable and configure private browsing mode, don't store information locally during the browsing session

* Permanently enable private browsing mode [ [1](https://support.mozilla.org/en-US/kb/Private-Browsing) [2](https://wiki.mozilla.org/PrivateBrowsing) ]
* Do not download URLs for the offline cache [ [1](http://kb.mozillazine.org/Browser.cache.offline.enable) ]
* Clear history when Firefox closes [ [1](https://support.mozilla.org/en-US/kb/Clear%20Recent%20History#w_how-do-i-make-firefox-clear-my-history-automatically) ]
* Set time range to "Everything" as default in "Clear Recent History"
* Clear everything but "Site Preferences" in "Clear Recent History"
* Don't remember browsing history
* Disable disk cache [ [1](http://kb.mozillazine.org/Browser.cache.disk.enable) ]
* Disable Caching of SSL Pages
* Disable download history
* Disable password manager (use an external password manager!)
* Disable form autofill, don't save information entered in web page forms and the Search Bar
* Cookies expires at the end of the session (when the browser closes) [ [1](http://kb.mozillazine.org/Network.cookie.lifetimePolicy#2) ]
* Require manual intervention to autofill known username/passwords sign-in forms [ [1](http://kb.mozillazine.org/Signon.autofillForms) [2](https://www.torproject.org/projects/torbrowser/design/#identifier-linkability) ]
* Disable formless login capture [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1166947) ]
* When username/password autofill is enabled, still disable it on non-HTTPS sites [ [1](https://hg.mozilla.org/integration/mozilla-inbound/rev/f0d146fe7317) ]
* Show in-content login form warning UI for insecure login fields [ [1](https://hg.mozilla.org/integration/mozilla-inbound/rev/f0d146fe7317) ]
* Delete Search and Form History
* Clear SSL Form Session Data [ [1](http://kb.mozillazine.org/Browser.sessionstore.privacy_level#2) ]
* Delete temporary files on exit [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=238789) ]
* Do not create screenshots of visited pages (relates to the "new tab page" feature) [ [1](https://support.mozilla.org/en-US/questions/973320) [2](https://developer.mozilla.org/en-US/docs/Mozilla/Preferences/Preference_reference/browser.pagethumbnails.capturing_disabled) ]
* Don't fetch and permanently store favicons for Windows .URL shortcuts created by drag and drop
* Disable bookmarks backups (default: 15) [ [1](http://kb.mozillazine.org/Browser.bookmarks.max_backups) ]

**UI related**

Improve visibility of security-related elements, mitigate shoulder-surfing

* Enable insecure password warnings (login forms in non-HTTPS pages) [ [1](https://blog.mozilla.org/tanvi/2016/01/28/no-more-passwords-over-http-please/) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1319119) [3](https://bugzilla.mozilla.org/show_bug.cgi?id=1217156) ]
* Disable "Are you sure you want to leave this page?" popups on page close [ [1](https://support.mozilla.org/en-US/questions/1043508) ]
* Disable Downloading on Desktop
* Always ask the user where to download [ [1](https://developer.mozilla.org/en/Download_Manager_preferences) ]
* Disable the "new tab page" feature and show a blank tab instead [ [1](https://wiki.mozilla.org/Privacy/Reviews/New_Tab) [2](https://support.mozilla.org/en-US/kb/new-tab-page-show-hide-and-customize-top-sites#w_how-do-i-turn-the-new-tab-page-off) ]
* Disable Snippets [ [1](https://wiki.mozilla.org/Firefox/Projects/Firefox_Start/Snippet_Service) [2](https://support.mozilla.org/en-US/kb/snippets-firefox-faq) ]
* Disable Activity Stream [ [1](https://wiki.mozilla.org/Firefox/Activity_Stream) ]
* Disable new tab tile ads & preload [ [1](http://www.thewindowsclub.com/disable-remove-ad-tiles-from-firefox) [2](http://forums.mozillazine.org/viewtopic.php?p=13876331#p13876331) [3](https://wiki.mozilla.org/Tiles/Technical_Documentation#Ping) [4](https://gecko.readthedocs.org/en/latest/browser/browser/DirectoryLinksProvider.html#browser-newtabpage-directory-source) [5](https://gecko.readthedocs.org/en/latest/browser/browser/DirectoryLinksProvider.html#browser-newtabpage-directory-ping) ]
* Enable Auto Notification of Outdated Plugins (Firefox < 50) [ [1](https://wiki.mozilla.org/Firefox3.6/Plugin_Update_Awareness_Security_Review) ]
* Force Punycode for Internationalized Domain Names [ [1](http://kb.mozillazine.org/Network.IDN_show_punycode) [2](https://www.xudongz.com/blog/2017/idn-phishing/) [3](https://wiki.mozilla.org/IDN_Display_Algorithm) [4](https://en.wikipedia.org/wiki/IDN_homograph_attack) [5](https://www.mozilla.org/en-US/security/advisories/mfsa2017-02/) ]
* Disable inline autocomplete in URL bar [ [1](http://kb.mozillazine.org/Inline_autocomplete) ]
* Disable CSS :visited selectors [ [1](https://blog.mozilla.org/security/2010/03/31/plugging-the-css-history-leak/) [2](https://dbaron.org/mozilla/visited-privacy) ]
* Disable URL bar autocomplete and history/bookmarks suggestions dropdown [ [1](http://kb.mozillazine.org/Disabling_autocomplete_-_Firefox#Firefox_3.5) ]
* Do not check if Firefox is the default browser
* When password manager is enabled, lock the password storage periodically
* Lock the password storage every 1 minutes (default: 30)
* Display a notification bar when websites offer data for offline use [ [1](http://kb.mozillazine.org/Browser.offline-apps.notify) ]

**Cryptography**

[TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) protocol related settings

* Enable HSTS preload list (pre-set HSTS sites list provided by Mozilla) [ [1](https://blog.mozilla.org/security/2012/11/01/preloading-hsts/) [2](https://wiki.mozilla.org/Privacy/Features/HSTS_Preload_List) [3](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) ]
* Enable Online Certificate Status Protocol [ [1](https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol) [2](https://www.imperialviolet.org/2014/04/19/revchecking.html) [3](https://www.maikel.pro/blog/current-state-certificate-revocation-crls-ocsp/) [4](https://wiki.mozilla.org/CA:RevocationPlan) [5](https://wiki.mozilla.org/CA:ImprovingRevocation) [6](https://wiki.mozilla.org/CA:OCSP-HardFail) [7](https://news.netcraft.com/archives/2014/04/24/certificate-revocation-why-browsers-remain-affected-by-heartbleed.html) [8](https://news.netcraft.com/archives/2013/04/16/certificate-revocation-and-the-performance-of-ocsp.html) ]
* Enable OCSP Stapling support [ [1](https://en.wikipedia.org/wiki/OCSP_stapling) [2](https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/) [3](https://www.digitalocean.com/community/tutorials/how-to-configure-ocsp-stapling-on-apache-and-nginx) ]
* Enable OCSP Must-Staple support (Firefox >= 45) [ [1](https://blog.mozilla.org/security/2015/11/23/improving-revocation-ocsp-must-staple-and-short-lived-certificates/) [2](https://www.entrust.com/ocsp-must-staple/) [3](https://github.com/schomery/privacy-settings/issues/40) ]
* Require a valid OCSP response for OCSP enabled certificates [ [1](https://groups.google.com/forum/#!topic/mozilla.dev.security/n1G-N2-HTVA) ]
* Disable TLS Session Tickets [ [1](https://www.blackhat.com/us-13/briefings.html#NextGen) [2](https://media.blackhat.com/us-13/US-13-Daigniere-TLS-Secrets-Slides.pdf) [3](https://media.blackhat.com/us-13/US-13-Daigniere-TLS-Secrets-WP.pdf) [4](https://bugzilla.mozilla.org/show_bug.cgi?id=917049) [5](https://bugzilla.mozilla.org/show_bug.cgi?id=967977) ]
* Only allow TLS 1.[0-3] [ [1](http://kb.mozillazine.org/Security.tls.version.*) ]
* Disable insecure TLS version fallback [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1084025) [2](https://github.com/pyllyukko/user.js/pull/206#issuecomment-280229645) ]
* Enfore Public Key Pinning [ [1](https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning) [2](https://wiki.mozilla.org/SecurityEngineering/Public_Key_Pinning) ]
* Disallow SHA-1 [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=1302140) [2](https://shattered.io/) ]
* Warn the user when server doesn't support RFC 5746 ("safe" renegotiation) [ [1](https://wiki.mozilla.org/Security:Renegotiation#security.ssl.treat_unsafe_negotiation_as_broken) [2](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3555) ]
* Disable automatic reporting of TLS connection errors [ [1](https://support.mozilla.org/en-US/kb/certificate-pinning-reports) ]
* Pre-populate the current URL but do not pre-fetch the certificate in the "Add Security Exception" dialog [ [1](http://kb.mozillazine.org/Browser.ssl_override_behavior) [2](https://github.com/pyllyukko/user.js/issues/210) ]
* Encrypted SNI (when TRR is enabled) [ [1](https://www.cloudflare.com/ssl/encrypted-sni/) [2](https://wiki.mozilla.org/Trusted_Recursive_Resolver#ESNI) [3](https://en.wikipedia.org/wiki/Server_Name_Indication#Security_implications_(ESNI)) ]

**Cipher suites**

This section tweaks the cipher suites used by Firefox. The idea is to support only the strongest ones with emphasis on [forward secrecy](https://en.wikipedia.org/wiki/Forward_secrecy), but without compromising compatibility with all those sites on the internet. As new crypto related flaws are discovered quite often, the cipher suites can be [tweaked to mitigate these newly discovered threats](https://github.com/pyllyukko/user.js/pull/18).

* Disable null ciphers
* Disable SEED cipher [ [1](https://en.wikipedia.org/wiki/SEED) ]
* Disable 40/56/128-bit ciphers
* Disable RC4 [ [1](https://developer.mozilla.org/en-US/Firefox/Releases/38#Security) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=1138882) [3](https://rc4.io/) [4](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566) ]
* Disable 3DES (effective key size is < 128) [ [1](https://en.wikipedia.org/wiki/3des#Security) [2](http://en.citizendium.org/wiki/Meet-in-the-middle_attack) [3](http://www-archive.mozilla.org/projects/security/pki/nss/ssl/fips-ssl-ciphersuites.html) ]
* Disable ciphers with ECDH (non-ephemeral)
* Disable 256 bits ciphers without PFS
* Enable GCM ciphers (TLSv1.2 only) [ [1](https://en.wikipedia.org/wiki/Galois/Counter_Mode) ]
* Enable ChaCha20 and Poly1305 (Firefox >= 47) [ [1](https://www.mozilla.org/en-US/firefox/47.0/releasenotes/) [2](https://tools.ietf.org/html/rfc7905) [3](https://bugzilla.mozilla.org/show_bug.cgi?id=917571) [4](https://bugzilla.mozilla.org/show_bug.cgi?id=1247860) [5](https://cr.yp.to/chacha.html) ]
* Disable ciphers susceptible to the logjam attack [ [1](https://weakdh.org/) ]
* Disable ciphers with DSA (max 1024 bits)

**Further hardening**

**This is not enough!** Here's some other tips how you can further harden Firefox:

* By default **your browser trusts 100's of**[**Certificate Authorities**](https://en.wikipedia.org/wiki/Certificate_authority) (CAs) from various organizations to guarantee privacy of your encrypted communications with websites. Some CAs have been known for misusing or deliberately abusing this power in the past, and **a single malicious CA can compromise all** your encrypted communications! Follow [this document](https://github.com/pyllyukko/user.js/blob/master/CAs.md) to only trust a selected, trimmed-down list of CAs.
* Keep your browser updated! If you check [Firefox's security advisories](https://www.mozilla.org/security/known-vulnerabilities/firefox.html), you'll see that pretty much every new version of Firefox contains some security updates. If you don't keep your browser updated, you've already lost the game.
* Disable/uninstall all unnecessary extensions and plugins!
* Use long and **unique** passwords/passphrases for each website/service.
* Prefer open-source, reviewed and audited software and operating systems whenever possible.
* Do not transmit information meant to be private over unencrypted communication channels.
* Use a search engine that doesn't track its users, and set it as default search engine.
* If a plugin is absolutely required, [check for plugin updates](https://www.mozilla.org/en-US/plugincheck/)
* Create different [profiles](https://mzl.la/NYhKHH) for different purposes
* Change the Firefox's built-in tracking protection to use the [strict list](https://support.mozilla.org/en-US/kb/tracking-protection-pbm?as=u#w_change-your-block-list)
* Change the timezone for Firefox by using the TZ environment variable (see [here](https://wiki.archlinux.org/index.php/Firefox_privacy#Change_browser_time_zone)) to reduce it's value in browser fingerprinting
* If you are concerned about more advanced threats, use specialized hardened operating systems and browsers such as [Tails](https://tails.boum.org/) or [Tor Brower Bundle](https://www.torproject.org/projects/torbrowser.html.en)

**Add-ons**

Here is a list of the most essential security and privacy enhancing add-ons that you should consider using:

* [uBlock Origin](https://addons.mozilla.org/firefox/addon/ublock-origin/)
  + For additional protection, enable more blocklists in the addon dashboard.
  + For additional protection, set it to [Hard mode](https://github.com/gorhill/uBlock/wiki/Blocking-mode:-hard-mode) (experienced users) - the default is [Easy mode](https://github.com/gorhill/uBlock/wiki/Blocking-mode:-easy-mode)
* [HTTPS Everywhere](https://www.eff.org/https-everywhere)
  + For additional protection, enable Block all unencrypted requests in the toolbar button menu. This will break websites where HTTPS is not available.
* [Certificate Patrol](http://patrol.psyced.org/) (experienced users)
  + Setting Store certificates even when in Private Browsing mode improves usability. This will store information about sites you visit.
* [HTTPS by default](https://addons.mozilla.org/firefox/addon/https-by-default/)
* [NoScript](https://noscript.net/)
* [No Resource URI Leak](https://addons.mozilla.org/firefox/addon/no-resource-uri-leak/) [ [1](https://bugzilla.mozilla.org/show_bug.cgi?id=863246) [2](https://bugzilla.mozilla.org/show_bug.cgi?id=903959) [3](https://www.browserleaks.com/firefox) [4](https://cs1.ca/ttest/dump.html) [5](https://trac.torproject.org/projects/tor/ticket/8725) ]
* [Decentraleyes](https://addons.mozilla.org/firefox/addon/decentraleyes/)
* [Canvas Blocker](https://addons.mozilla.org/firefox/addon/canvasblocker/)

Additional add-ons that you might consider using or reading about:

* [uMatrix](https://addons.mozilla.org/en-US/firefox/addon/umatrix/) (experienced users)
* [Privacy Badger](https://www.eff.org/privacybadger)
* [Mozilla Lightbeam](https://www.mozilla.org/en-US/lightbeam/)
* [PRISM Break Web Browser Addons section](https://prism-break.org/en/subcategories/gnu-linux-web-browser-addons/)
* [Ghostery](https://www.ghostery.com/) (proprietary software, maintained by [an advertising company](https://en.wikipedia.org/wiki/Ghostery))

**Known problems and limitations**

Hardening your often implies a trade-off with ease-of-use and comes with reduced functionality. Here is a list of known problems/limitations:

* Disabling ServiceWorkers breaks functionality on some sites (Google Street View...)
* Disabling WebRTC breaks peer-to-peer file sharing tools (reep.io ...)
* Disabling clipboard events breaks Ctrl+C/X/V copy/cut/paste functionaility in JS-based web applications (Google Docs...)
* Disabling clipboard operations will break legitimate JS-based "copy to clipboard" functionality
* Enabling Mixed Display Content blocking can prevent images/styles... from loading properly when connection to the website is only partially secured
* Disabling nonessential protocols breaks all interaction with custom protocols such as mailto:, irc:, magnet: ... and breaks opening third-party mail/messaging/torrent/... clients when clicking on links with these protocols
* Disabling system add-on updates prevents Mozilla from "hotfixing" your browser to patch critical problems (one possible use case from the documentation)
* Containers are not available in Private Browsing mode
* RFP breaks some keyboard shortcuts used in certain websites (see #443)
* RFP changes your time zone
* Fully automatic updates are disabled and left to package management systems on Linux. Windows users may want to change this setting.
* Update check page might incorrectly report Firefox ESR as out-of-date
* Do No Track must be enabled manually
* Blocking 3rd-party cookies breaks a number of payment gateways
* First-party isolation breaks Microsoft Teams
* First-party isolation causes HTTP basic auth to ask for credentials for every new tab (see #425)
* You can not view or inspect cookies when in private browsing: <https://bugzilla.mozilla.org/show_bug.cgi?id=823941>
* When Javascript is enabled, Websites can detect use of Private Browsing mode
* Private browsing breaks Kerberos authentication
* Disables "Containers" functionality (see below)
* "Always use private browsing mode" (browser.privatebrowsing.autostart) disables the possibility to use password manager: <https://support.mozilla.org/en-US/kb/usernames-and-passwords-are-not-saved#w_private-browsing>
* Installing user.js will remove your browsing history, caches and local storage.
* Installing user.js **will remove your saved passwords** (<https://github.com/pyllyukko/user.js/issues/27>)
* Clearing open windows on Firefox exit causes 2 windows to open when Firefox starts <https://bugzilla.mozilla.org/show_bug.cgi?id=1334945>
* .URL shortcut files will be created with a generic icon
* disabling "beforeunload" events may lead to losing data entered in web forms
* OCSP leaks your IP and domains you visit to the CA when OCSP Stapling is not available on visited host
* OCSP is vulnerable to replay attacks when nonce is not configured on the OCSP responder
* OCSP adds latency (performance)
* Short-lived certificates are not checked for revocation (security.pki.cert\_short\_lifetime\_in\_days, default:10)
* Firefox falls back on plain OCSP when must-staple is not configured on the host certificate
* security.OCSP.require will make the connection fail when the OCSP responder is unavailable
* security.OCSP.require is known to break browsing on some [captive portals](https://en.wikipedia.org/wiki/Captive_portal)

In addition see the current [issues](https://github.com/pyllyukko/user.js/issues). You can use the [web console](https://developer.mozilla.org/en-US/docs/Tools/Web_Console) to investigate what causes websites to break.

**FAQ**

Does this user.js file fix all security problems?

No. Please read [Known problems and limitations](https://github.com/pyllyukko/user.js#known-problems-and-limitations), the project's [issue](https://github.com/pyllyukko/user.js/issues) tracker, and report new issues there. Please open separate issues for each individual problem/question you may have.

Why are obsolete/deprecated entries included in the user.js file?

This project is aimed at Firefox versions between the current [ESR](https://www.mozilla.org/en-US/firefox/organizations/) and the latest Firefox release. We will wait for widespread deployment of the current ESR (eg. adoption in major Linux distributions) before removing deprecated/obsolete preferences. Presence of deprecated entries causes no known problems.

Installing the user.js file breaks xyz plugin/addon/extension, how can I fix it?

See <https://github.com/pyllyukko/user.js/issues/100>

Will there be an official addon/an android version/feature xyz?

Search the project [issues](https://github.com/pyllyukko/user.js/issues?q=is%3Aissue).

How can I lock my preferences to prevent Firefox overwriting them?

See lockPref in [System-wide installation](https://github.com/pyllyukko/user.js#system-wide-installation).

**Contributing**

Yes please! All issues and pull requests are more than welcome. Please try to break down your pull requests or commits into small / manageable entities, so they are easier to process. All the settings in the user.js file should have some official references to them, so the effect of those settings can be easily verified from Mozilla's documentation.

Feel free to follow the latest commits [RSS feed](https://github.com/pyllyukko/user.js/commits/master.atom) and other interesting feeds from the [References](https://github.com/pyllyukko/user.js#references) section.

You may also reach other contributors through [IRC](http://webchat.freenode.net/?channels=%23user.js) (#user.js on Freenode) or [Gitter](https://gitter.im/user-js/Lobby).

For more information, see [CONTRIBUTING](https://github.com/pyllyukko/user.js/blob/master/CONTRIBUTING.md)

**Online tests**

**Version checks**

* [**Mozilla Plugin Check**](https://www.mozilla.org/en-US/plugincheck/)
* [Adobe Flash Player Version Check](https://www.adobe.com/software/flash/about/)
* [Java Version Check](https://www.java.com/en/download/installed.jsp)

**Fingerprinting tests**

* [BrowserSpy.dk](http://browserspy.dk/)
* [BrowserLeaks.com](https://www.browserleaks.com/firefox)
* [AmIUnique](https://amiunique.org/) [[1](https://github.com/DIVERSIFY-project/amiunique)]
* [Panopticlick](https://panopticlick.eff.org/)
* [Unique Machine](http://www.uniquemachine.org/)
* [Firefox Addon Detector](https://thehackerblog.com/addon_scanner/) [[1](https://thehackerblog.com/dirty-browser-enumeration-tricks-using-chrome-and-about-to-detect-firefox-plugins/)]
* [AudioContext Fingerprint Test Page](https://audiofingerprint.openwpm.com/)
* [Evercookie](https://samy.pl/evercookie/)
* [WebRTC Test Landing Page](https://mozilla.github.io/webrtc-landing/)
* [getUserMedia Test Page](https://mozilla.github.io/webrtc-landing/gum_test.html)
* [Onion test for CORS and WebSocket](https://cure53.de/leak/onion.php)
* [Official WebGL check](https://get.webgl.org/)
* [WebGL Report](http://webglreport.com/)
* [Battery API](https://robnyman.github.io/battery/) [[1](https://pstadler.sh/battery.js/)]
* [WebRTC LAN address leak test](http://net.ipcalf.com/)
* [IP Check](http://ip-check.info/?lang=en)
* [OONI Internet censorship tests](https://ooni.torproject.org/nettest/)

**SSL tests**

* [SSL Client Test](https://www.ssllabs.com/ssltest/viewMyClient.html)
* [How's My SSL](https://www.howsmyssl.com/)
* [Mixed content tests (Mozilla)](https://people.mozilla.org/~tvyas/mixedcontent.html)
* [Mixed content tests (Microsoft)](https://ie.microsoft.com/testdrive/browser/mixedcontent/assets/woodgrove.htm)
* [SSL Checker | Symantec CryptoReport](https://cryptoreport.websecurity.symantec.com/checker/views/sslCheck.jsp)
* [Bad SSL](https://badssl.com/)

**Other tests**

* [Test page for Firefox's built-in Tracking Protection](https://itisatrap.org/firefox/its-a-tracker.html)
* [Test page for Firefox's built-in Phishing Protection](https://itisatrap.org/firefox/its-a-trap.html) ("Web forgeries")
* [Test page for Firefox's built-in Malware Protection](https://itisatrap.org/firefox/its-an-attack.html) (attack page)
* [Test page for Firefox's built-in Malware Protection](https://itisatrap.org/firefox/unwanted.html) (unwanted software)
* [HTML5test](https://html5test.com/) - Comparison of supported HTML5 features in various browsers/versions
* [Filldisk](http://www.filldisk.com/)
* [BrowserAudit](https://browseraudit.com/)

**References**

**Mozilla documentation**

* [**Security Advisories for Firefox**](https://www.mozilla.org/security/known-vulnerabilities/firefox.html)
* [**Known Vulnerabilities for Firefox**](https://www.mozilla.org/en-US/security/known-vulnerabilities/firefox/)
* [**DXR - Firefox General preferences**](https://dxr.mozilla.org/mozilla-central/source/modules/libpref/init/all.js)**(**[**RSS**](https://hg.mozilla.org/mozilla-central/atom-log/tip/modules/libpref/init/all.js)**)**
* [DXR - Firefox Security preferences](https://dxr.mozilla.org/mozilla-central/source/security/manager/ssl/security-prefs.js) ([RSS](https://hg.mozilla.org/mozilla-central/atom-log/tip/security/manager/ssl/security-prefs.js))
* [DXR - Firefox Datareporting preferences](https://dxr.mozilla.org/mozilla-central/source/toolkit/components/telemetry/datareporting-prefs.js) ([RSS](https://hg.mozilla.org/mozilla-central/atom-log/tip/toolkit/components/telemetry/datareporting-prefs.js))
* [DXR - Firefox Healthreport preferences](https://dxr.mozilla.org/mozilla-central/source/toolkit/components/telemetry/healthreport-prefs.js) ([RSS](https://hg.mozilla.org/mozilla-central/atom-log/tip/toolkit/components/telemetry/healthreport-prefs.js))
* [**Mozilla Security Blog**](https://blog.mozilla.org/security/category/security/)**(**[**RSS**](https://blog.mozilla.org/security/feed/)**)**
* [Mozilla Firefox Release Plan](https://wiki.mozilla.org/RapidRelease/Calendar)
* [Mozilla Firefox developer release notes](https://developer.mozilla.org/en-US/Firefox/Releases)
* [Advices from Mozilla Firefox on privacy and government surveillance](https://www.mozilla.org/en-US/teach/smarton/surveillance/)
* [Polaris - advance privacy technology for the web](https://wiki.mozilla.org/Polaris)
* [Mozilla Privacy Principles](https://wiki.mozilla.org/Privacy/Principles)
* [List of Firefox "about:" URLs](https://developer.mozilla.org/en-US/Firefox/The_about_protocol)
* [Policy Templates for Firefox](https://github.com/mozilla/policy-templates)
* [A brief guide to Mozilla preferences](https://developer.mozilla.org/en-US/docs/Mozilla/Preferences/A_brief_guide_to_Mozilla_preferences)
* [Mozilla preferences for uber-geeks](https://developer.mozilla.org/en-US/docs/Mozilla/Preferences/Mozilla_preferences_for_uber-geeks)
* [Privacy & Security related add-ons](https://addons.mozilla.org/firefox/extensions/privacy-security/) ([RSS](https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/format:rss?sort=featured))

**Other documentation**

* [**User.js comparator**](https://jm42.github.io/compare-user.js/)
* [**CVEs for Firefox - mitre.org**](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=firefox)
* [CVEs for Firefox - cvedetails.com](https://www.cvedetails.com/vulnerability-list/vendor_id-452/product_id-3264/Mozilla-Firefox.html)
* [ghacksuserjs/ghacks-user.js](https://github.com/ghacksuserjs/ghacks-user.js): a similar project and great source of information, with different goals and methodology
* [About:config entries - MozillaZine](http://kb.mozillazine.org/About:config_entries)
* [Security and privacy-related preferences - MozillaZine](http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences)
* [Diff between various Firefox .js configurations in upcoming releases](https://cat-in-136.github.io/) **(**[**RSS**](https://cat-in-136.github.io/feed.xml)**)**
* [Center for Internet Security - Mozilla Firefox benchmarks](https://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.desktop.browsers.firefox) ([RSS](https://benchmarks.cisecurity.org/downloads/rss/))
* [iSEC Tor Browser evaluation](https://github.com/iSECPartners/publications/tree/master/reports/Tor%20Browser%20Bundle)
* [The Design and Implementation of the Tor Browser](https://www.torproject.org/projects/torbrowser/design/)
* [Browser Exploitation Framework](https://beefproject.com/) [[1](http://blog.beefproject.com/) [2](https://github.com/beefproject/beef/wiki) [3](https://github.com/beefproject/beef)]
* [shadow - Firefox jemalloc heap exploitation framework](https://github.com/CENSUS/shadow)

**TLS/SSL documentation**

* [Mozilla Included CA Certificate List](https://wiki.mozilla.org/CA:IncludedCAs)
* [Potentially problematic CA practices](https://wiki.mozilla.org/CA:Problematic_Practices)
* [Bulletproof SSL and TLS](https://www.feistyduck.com/books/bulletproof-ssl-and-tls/)
* [TLS Cipher Suite Discovery](https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/TLS_Cipher_Suite_Discovery)
* [Server-side TLS configuration](https://wiki.mozilla.org/Security/Server_Side_TLS)