Firefox Hardening Guide

2021/05/25

There are various similar guides on other sites, but many of these guides were partially incomplete, so I've tried to write the most complete guide as possible, which can be used by paranoid users like me.

This is the best way to enhance Firefox. I must remind you that **our goal here is privacy**. If you want to browse the web anonymously, I'd suggest you looking at Tor instead.

The easiest and fastest way to get the best configuration for Firefox is using Arkenfox's user.js. **The Arkenfox project provides an user.js template for configuration and hardening Firefox**, which gives us the perfect foundation for our privacy friendly browser.

Creating a new profile that uses Arkenfox's user.js

It's a simple process and I recommend you going to **Arkenfox's repo on Github** and read their Wiki. But I'll assume that you want the maximum level of privacy and guide you through the necessary steps.

You’ll have to go to about:profiles and create a new profile. I’ll name it “Arkenfox” but you can call it wathever you want. Then, download Arkenfox’s user.js from their repo and unzip it. The result should be a directory called “user.js-88.0” (NOTE: the name may vary in newer Firefox versions, but the procedure is exactly the same)

You’ll have to copy the resulting directory to /home/“your-user-name”/.mozilla/firefox . After that, go to your .mozilla/firefox directory and look for a directory that should be named something like “xxxxxxxx.arkenfox”, in my case it was “bvorhi84.arkenfox”. Now, copy that name and delete the directory.

The last step is to rename the directory “user.js-88.0” with the name of the previously deleted directory, “bvorhi84.arkenfox” for me.

Now you can open about:profiles again and select your recently created profile (“Arkenfox” in my case). Open it and you should set it as the default profile so it’s opened every time that you launch Firefox.

Congratulations! We have already completed the most difficult part of the process.

Use a privacy friendly search engine

This is the simplest part of the guide. You only have to replace Google with a privacy respectful search engine. I'll list you the options.

Searx

A privacy respecting, fully free (as in freedom), metasearch engine. It's selfhostable so you can use your own instance or one of the **public ones**.

Less recommendable options are:

- **Metager**: another free metasearch engine runned by a non-profit based in Germany. It's preferrable over Duckduckgo but not over SearX.
- **Duckduckgo Lite**: this is Duckduckgo but without JavaScript so they can track you as little as possible (Duckduckgo shouldn't be trusted).
- **Qwant**: a search engine which says that it doesn't track their users (non-free).
- **Mojeek**: independent search engine based in the UK that says that it doesn't track their users (non-free).
- **YaCy**: a libre, peer-to-peer search engine. It's powered by it's users and it doesn't have any central server. This is a unique and great idea, although it doesn't work great.

Privacy addons

This section is divided in two parts: the must-haves addons and some recommendations that will improve your privacy.

Must-haves

uBlock Origin

It’s **an efficient blocker that is easy on memory and it’s completely free software**. It also has various modes and it allows for extended blocking similar to NoScript and uMatrix.

Properly configured, uBlock will be our best aliased against ads, trackers and analytics.

I’d suggest you enabling the advanced mode. It’s highly recommended to turn off JavaScript by default. You can enable it for certain sites whenever you need it. **Blocking JavaScript is probably the best thing we can do to preserve our privacy**.

Learning how to use the advanced mode in uBlock is IMO worth it and highly rewarded if you want to gain privacy. It isn’t that hard and there are tons of tutorials, so that’s up to you.

LocalCDN

LocalCDN is a fork of the well-known Decentraleyes. It emaulates Content Delivery Networks locally by intercepting requests, serving them locally. It’s better than Decentraleyes in the sense that it provides custom rules to use inside uBlock Origin, so these addons work better together.

We can find these prepared rules clicking the addon icon, going to advanced and scrolling down. We select uBlock Origin and copy the rules. Then, we have to go to uBlock, enable “I am an advanced user”, then go to “My rules” and you have to paste the rules on the list at the right. Then save and commit the changes so they become permanent. You can now forget about LocalCDN, it’ll just work.

Password Manager

You should be using a trustable password manager for creating and storing your passwords.

My recommendation would be Bitwarden which is free as in freedom and free as in free beer! Yeah, it’s both “libre” and “gratis”. It has automatic sync between your devices and it’s really easy to use. If you like it and you can afford it, you should buy their premium membership, which doesn’t provide any essential feature (their free plan is so complete) but it’s important to support free software projects

For more paranoid people (like me, lol) **who don’t want their passwords to be stored on a server, we have KeePassXC** which is also free software and gratis. It has the advantage that **your passwords are only stored in a local, strongly encrypted database** so they won’t ever leave your computer if you don’t want to. You can use **Syncthing** to sync them between your different machines without any server.

The third option (for terminal wizards only) is **GNU Pass**, which is a **simple password manager that follows the Unix philosophy**. Passwords live in ~/.password-store **encrypted with your GPG key**.

Recommended addons

These are addons that are generally recommended but that in contrast with uBlock or LocalCDN, they require some maintenance (not so much, actually).

Take into account that some of these addons may be redundant with each other and that when you have JavaScript enabled, they could fingerprint you by the addons you use, so **I'd recommend to use the minimum number of addons as possible**, without sacrificing important privacy features. So you'll have to find the perfect balance between the number of addons and the advantages they provide.

Cookie AutoDelete

This addon deletes cookies everytime that we close a tab or we exit. But it can do much more, like **cleaning local storage, cleaning on domain change, deleting cache, white and greylisting, cleaning on domain change**, etc.

It's such a powerful tool that it can also be configured to be used with containers (you should enable a setting for that) and **it's especially helpful if you aren't using neither containers nor first party isolation** (later in the article).

ClearURLs

It will **automatically remove tracking elements from URLs** (this is a commonly used strategy to track you) and it's really simple to use. It isn't a must-have because very few times may break a site that won't work if you clean the URL. But if you notice this, you only have to temporarily disable the addon. Easy, isn't it?

Temporary Containers

This is possibly one of the greatest addons of all times. It allows you to open tabs, websites and links in automatically managed disposable containers. **Containers isolate data websites store (cookies, storage, and more) from each other**. You only have to enable automatic mode and the addon will do the magic for you. However, you can't use it on private mode and it may slow down your browser a bit (since it's creating a container for each new tab). If you want containers only for especific sites, I'd recommend **Multi-Account Containers**. Cookie AutoDelete may be unnecessary when using Temporary Containers.

ETag Stoppa

It prevents your browser from storing entity tags by removing ETag response headers without exceptions. It's only necessary if you aren't using Temporary Containers and it makes a great team with Cookie AutoDelete.

CanvasBlocker

CanvasBlocker is the perfect addon for those momments when you have to enable JavaScript. **It prevents websites from using some JavaScript APIs to fingerprint you**. It has various levels and it's really helpful if you want to spoof your fingerprint. They say that it may break some sites although I've never experienced any issue with this addon. It just works.

xBrowserSync

Bookmark sync as it should be: end-to-end encrypted and anonymous. There are different servers and you can even selfhost it yourself.

AdNauseam (alternative to uBlock)

AdNauseam not only blocks ads, it obfuscates browsing data to resist tracking by the online ad industry. To throw ad networks off your trail **AdNauseam "clicks" blocked and hidden ads, polluting your data profile and injecting noise into the economic system that drives online surveillance**. It uses uBlock as it's base, so you also get everything that uBlock is capable of.

It's the perfect addon if you want to shout a loud **"Google fuck you!"**.

Privacy Redirect

Redirects Twitter, YouTube, Instagram, Reddit & Google Maps requests **to privacy friendly and libre alternatives** (Nitter, Invidious, OpenStreetMap, Libreddit). It also supports custom servers so you can use it with your selfhosted instances!

Additional tweaks in the about:config

Although Arkenfox has given us a great template, I find that there are a few other settings that can enhance even more our privacy. You'll have to go to your about:config (In your new profile, of course!). Click that you accept the risks and continue. I'll list you some of my recommended tweaks, you can evaluate yourself if you need one of the features that we're disabling.

The following changes will be classified in **three tiers**: **basic tier** tweaks won't break anything, **standard tier** changes might cause minor inconvenience, while tweaks in the **advanced tier** may break certain sites, but don't worry since I provide an easy way to fix those sites for you.

Basic tier

Disable prefetching

Change network.dns.disablePrefetch to true and network.prefetch-next to false (Prefetching may speed loading times a bit, but it isn’t that visible and disabling it prevents your browser from connecting to servers without user intervention)

Disable Firefox account

Change identity.fxaccounts.enabled to false.

Disable JavaScript for PDF view

Change pdfjs.enableScripting to false (You’ll still be able to view PDF’s on Firefox)

Disable Pocket completely

Change browser.newtabpage.activity-stream.section.highlights.includePocket to false and extensions.pocket.enabled to false (Pocket should be disabled by Arkenfox, but it doesn’t appear to be disable in my browser, so I include this options just in case)

Standard tier

Disable geolocation support

Change geo.enabled to false

Disable WebRTC

Change media.peerconnection.enabled and media.navigator.enabled to false. (WARNING: turning this to false may break certain sites, especially a few popular videocalls programs.)

Disable DRM controlled HTML5 content

Change media.gmp-widevinecdm.enabled and media.eme.enabled to false (May break sites which require DRM)

Advanced tier

For users in the advanced tier, I highly recommend you the **Privacy Settings addon** which allows us to temporarily turn off some settings so you can fix broken sites without disabling a privacy setting permanently. It’s super useful once you learn how to use it.

Enable first party isolate

Change privacy.firstparty.isolate to true. This is an important tweak, since it isolates cookies and blocks cross-site tracking.

Enable Resist Fingerprinting

Change privacy.resistFingerprinting to true. It might result in some performance issues, but I like to enable it. I’ve been using it for a long time and I’ve never had any issue.

Disable referer headers

Change network.http.referer.XOriginPolicy to 2. It’ll break some sites, especially those that have forms and logins.

0 = Send Referer in all cases.

1 = Send Referer to same eTLD sites.

2 = Send Referer only when the full hostnames match.

End of the journey

If you’ve come this far, **I must give you my most sincere congratulations. You have successfully configured Firefox to maximize your privacy**. It isn’t the most comfortable web browsing experience, but **it’s by far the one that rewards you with the most satisfaction and feeling of security**. If you have any question, you can reach me on **Mastodon**.

>> Home

Made with Free Software | Fediverse |