

Recommended Addons

☐☐ RECOMMENDED

- [uBlock Origin](#) ✓ [privacy](#) | [github](#)
 - ☐ Setup your [blocking mode](#)
 - ☐ Enable [AdGuard URL Tracking Protection](#)
 - ☐ Import [Actually Legitimate URL Shortener Tool](#) ¹ | [github](#)

◦ “ ¹ [click me for details](#)

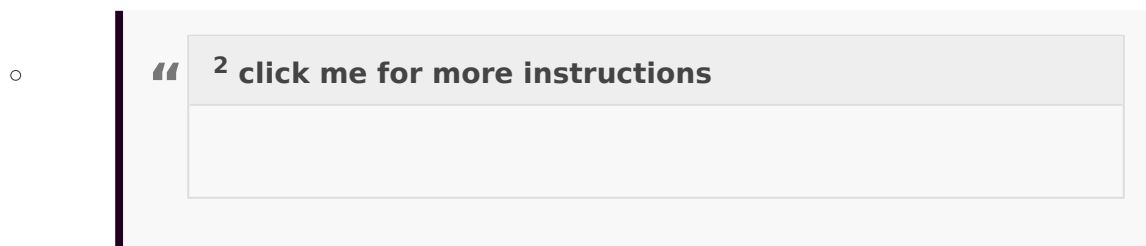
- [Skip Redirect](#) | [github](#)

note: images have been edited for simplicity

☐☐ OPTIONAL

- [CanvasBlocker](#) ✓ [privacy](#) | [github](#)
 - ☐ non-RFP users only - see [if RFP is for you](#)
 - Good protection against naive scripts, detectable and leaks with advanced scripts
 - Randomize canvas and audio, maybe webgl if you use that: the rest is not needed
- [Header Editor](#) | [github](#)
 - Allows you to run rules to modify the request header and response header, cancel a request and redirect a request. Be careful not to universally alter your passive fingerprint
- [Multi-Account Containers](#) (MAC) | [github](#) and [Temporary Containers](#) (TC) | ✓ [privacy](#) | [github](#)
 - While third parties are already partitioned with [Total Cookie Protection](#) (dFPI), leveraging containers can provide additional benefits, such as
 - an extra layer of isolation, see [bugzilla 1767271](#)

- signing in to multiple accounts on the same site
- MAC and Mozilla VPN adds advanced VPN and proxy settings
- While TC provides sanitizing, and uses a dFPI-compatible API, this is not why it is recommended as optional, see `Cookie extensions` in the `DON'T BOTHER` section below
- Request Control | [github](#) | [manual](#) | [testing links](#)
- Redirector ✓ [privacy](#) | [github](#)
- Smart Referer ✓ [privacy](#) | [gitlab](#) | [github: archived](#)
 - ☐ Only if `1601` `network.http.referer.XOriginPolicy` is too strict for you, and you override it to default `0` (so Smart Referer works)
 - Disable the whitelist ²



note: images have been edited for simplicity

☐☐ TOOLS

These extensions will not mask or alter any data sent or received, but may be useful depending on your needs

- Behave | [github](#)
 - Monitors and warns if a web page; performs DNS Rebinding attacks to Private IPs, accesses Private IPs, does Port Scans
- mozlz4-edit | [github](#)
 - Inspect and/or edit `*.lz4`, `*.mozlz4`, `*.jsonlz4`, `*.baklz4` and `*.json` files within FF
- CRX Viewer | [github](#)
- Compare-UserJS
 - Not an extension, but a tool to compare user.js files and output the diffs in detailed breakdown - thanks [claustromaniac](#) ☐☐

☐☐ DON'T BOTHER

- uMatrix
 - ⚠ No longer maintained, the last release was Sept 2019 except for a one-off patch to fix a vulnerability
 - Everything uMatrix did can be covered by prefs or other extensions: use uBlock Origin for any content blocking.
- NoScript
 - Redundant with uBlock Origin
- Ghostery, Disconnect, Privacy Badger, etc
 - Redundant with Total Cookie Protection (dFPI)
 - Note: Privacy Badger no longer uses heuristics by default, and enabling it makes you easily detected
- Neat URL, ClearURLs
 - Redundant with uBlock Origin's removeparam and added lists. Any potential extra coverage provided by additional extensions is going to be minimal
- HTTPS Everywhere
 - Redundant with HTTPS-Only Mode and scheduled for deprecation: maintenance mode only Sept 2021, sunsets Jan 2023
- CSS Exfil Protection
 - Practically zero threat and if the platform's CSS was compromised, you'd have bigger problems to worry about
- LocalCDN, Decentraleyeyes
 - Third parties are already partitioned if you use Total Cookie Protection (dFPI)
 - Replacing *some version specific* scripts on CDNs with local versions is not a comprehensive solution and is a form of enumerating badness. While it may work with some scripts that are included it doesn't help with most other third party connections
 - CDN extensions don't really improve privacy as far as sharing your IP address is concerned and their usage is fingerprintable as this Tor Project developer points out. They are the wrong tool for the job and are not a substitute for a good VPN or Tor Browser. Its worth noting the resources for Decentraleyeyes are over three years out of date and would not likely be used anyway
- Cookie extensions
 - ☐ Sanitizing in-session is a false sense of privacy. They do nothing for IP tracking. Even Tor Browser does not sanitize in-session e.g. when you request a new circuit. A new ID requires *both* full sanitizing *and* a new IP. The same applies to Firefox
 - ☐ Cookie extensions can lack APIs or implementation of them to properly sanitize
 - e.g. at the time of writing: Cookie Auto Delete
 - “ As of Firefox 86, strict mode is not supported at this time due to missing APIs to handle the Total Cookie Protection
- Anti-Fingerprinting Extensions

- Redundant with RFP which is the best solution
 - ☐ For non-RFP users, we recommend CanvasBlocker (see above) as your next best option
 - Most extensions cannot protect what they claim:
 - It's impossible (engine, OS, version)
 - It's not a lie (the sites expect and use a valid value)
 - It's dumb (randomizing is not very usable, and/or successfully spoofing is the same as setting that)
 - It's equivalency
 - It has too many methods (fonts: at least a dozen methods and counting)
 - ... and more
 - Web Extensions lack APIs to properly protect metrics (without breaking basic functionality)
 - Web Extensions are detectable, and often uniquely fingerprintable, when they touch the DOM (and sometimes when they don't)
-

Revision #1

Created 2 November 2022 12:07:02 by Admin

Updated 2 November 2022 12:20:48 by Admin