

In your Browser

- [Use Firefox forks.](#)
- [Recommended Addons](#)
- [Block Twitch ads with uBlock Origin](#)
- [ClearURLs](#)
- [SponsorBlock](#)

Use Firefox forks.

Librewolf

<https://www.youtube.com/embed/F7-bW2y6lcl>

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

- “ ² **click me for more instructions**

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)

Block Twitch ads with uBlock Origin

Link

- Navigate to the uBlock Origin Dashboard (the extension options)
- Under the `My filters` tab add `twitch.tv##+js(twitch-videoad)`.
- Under the `Settings` tab, enable `I am an advanced user`, then click the cog that appears. Modify the value of `userResourcesLocation` from `unset` to the full url of the solution you wish to use (if a url is already in use, add a space after the existing url). e.g.
`userResourcesLocation https://github.com/pixeltris/TwitchAdSolutions/raw/master/notify-strip/notify-strip-ublock-origin.js`
- To ensure uBlock Origin loads the script I recommend that you disable/enable the uBlock Origin extension (or restart your browser).

To stop using a script remove the filter and make the url `unset`.

ClearURLs

Link

ClearURLs is an add-on based on the new WebExtensions technology and is optimized for *Firefox* and *Chrome* based browsers.

This extension will automatically remove tracking elements from URLs to help protect your privacy when browsing through the internet.

Many websites use tracking elements in the URL to mark your online activity. All that tracking code is not necessary for a website to be displayed or work correctly and can therefore be removed — that is exactly what ClearURLs does.

Another common example are Amazon URLs. If you search for a product on Amazon you will see a very long URL, such as:

```
https://www.amazon.com/dp/exampleProduct/ref=sxin_0_pb?_mk_de_DE=ÅMÅŽÕÑ&keywords=tea&pd_rd_i=exampleProduct&pd_rd_r=8d39e4cd-1e4f-43db-b6e7-72e969a84aa5&pd_rd_w=1pcKM&pd_rd_wg=hYrNI&pf_rd_p=50bbfd25-5ef7-41a2-68d6-74d854b30e30&pf_rd_r=0GMWD0YYKA7XFGX55ADP&qid=1517757263&rnid=2914120011
```

Indeed most of the above URL is tracking code. Once ClearURLs has cleaned the address, it will look like this: `https://www.amazon.com/dp/exampleProduct`

- Removes tracking from URLs automatically in the background
- Blocks some common ad domains (optional)
- Has a built-in tool to clean up multiple URLs at once
- Supports redirection to the destination, without tracking services as a middleman
- Adds an entry to the context menu so that links can be copied quickly and cleanly
- Blocks hyperlink auditing, also known as *ping tracking* (see also [this article](#))
- Prevents ETag tracking
- Prevents tracking injection over history API (see also: [the replaceState\(\) method](#))
- Prevents Google from rewriting the search results (prevents the insertion of tracking code)
- Prevents Yandex from rewriting the search results (prevents the insertion of tracking code)

image-1648934719164.png

image-1648934759071.JPG

SponsorBlock

image-1648935286757.png

SponsorBlock is an open-source crowdsourced browser extension to skip sponsor segments in YouTube videos. Users submit when a sponsor happens from the extension, and the extension automatically skips sponsors it knows about. It also supports skipping other categories, such as intros, outros and reminders to subscribe.

It also supports Invidio.us.

image-1648935086122.png