

Essential privacy (and other) addons

- Introduction -
- Recommended privacy addons -
 - ηMatrix / uMatrix -
 - URL Rewriter -
 - Proxy Privacy Ruler -
 - Decentraleyes / deCDN -
- HTTPS enforcing addons -
- Inferior privacy addons -
 - uBlock Origin, AdBlock Plus, AdGuard, Disconnect, etc. -
 - NoScript -
 - Privacy Badger -
 - Ghostery -
 - LibreJS -
 - VPN addons -
- Other useful addons -
 - Reader View -
 - Vimium -
- I don't care about cookies -
 - Dorando Keyconfig -
 - Linkification -

Introduction

If you've read the article [How to choose a browser for everyday use](#), you know that most of their functionality comes from extensions. So much that, if you've had certain ones for a long time, a browser will seem unusable to you without them. But which ones should we choose, and which ones to avoid? That's exactly what you will learn in this article.

Recommended privacy addons

 [uMatrix](#) / [uMatrix](#) 

Simply THE most important addon out there, and one I won't go on the Internet without. To understand why, let's explore how the Web actually works. Every time you visit any website, you are making a **request** to it. A website can consist of many files, such as image, style files, or scripts (which can ALSO make their own requests). To complicate matters, it can also make connections to other websites (these are called **third-party requests**). So, by visiting one website you can end up with hundreds of all types of requests. Now, **most privacy issues in the end reduce to a browser making a request with the intention of data collection. The prevention of spying, then, would have to include disabling certain kinds of requests.** Okay, but what does uMatrix have to do with all that?

uMatrix divides all requests into eight categories: Cookies, CSS (style files), image, media

(audio and video files), scripts, XHR (requests made by scripts), frames (embedding other sites), and other (anything else). And then into another level of other categories: first and third party. What does this mean? Simply, **certain types of requests are much more likely to be privacy intruding** than others, and uMatrix **allows disabling them globally**, and then enabling them only on certain websites that you choose.

The requests most responsible for spying are the third party ones, especially scripts. So let's go and block them all. Now any website that contains a facebook script cannot spy on you anymore - but if you allow **first-party** scripts, you can still use Facebook - it just can't spy on you elsewhere. Another example - Google's ReCaptcha. You might want to globally allow it - OR, if you don't care about it except you need to access some website just once - allow it only for that website.

However, tracking prevention is not the only use of uMatrix. Removing clutter ("ads"), annoying popups pestering you to "sign up", video embeds, etc. are all possible. And if you realize you want video embeds on your favorite website - but not elsewhere - you can just allow them there. The best thing about uMatrix is that you can globally block everything with it, and only allow it when and where you need it. **It gives you almost complete control over your browsing**, and with an intuitive interface, too. Of course it will take a while to learn and configure it the way you want to, but for that level of power, it's worth it - and you can go gentle at first; just blocking third-party scripts and cookies will do a lot. Without this addon, that power would be in the hands of trackers and advertisers - you'd see what and when they want you to see. Now, there are other addons providing some of the same functionality, but they are hugely inferior, as we will see later. Available for both Chrome and Firefox based browsers (Pale Moon uses the nMatrix fork).

UPDATE January 2022: if you think the uBlock Origin Advanced Mode can replace uMatrix, look:



The screenshot shows the eMatrix 4.4.8 interface. At the top, the address bar displays 'duckduckgo.com'. Below it, a row of controls includes 'all', 'cookie', 'css', 'image', 'media', 'script', 'XHR', 'frame', and 'other'. The 'all' control is selected. Below this, a row of controls includes '1st-party', '2nd-party', '3rd-party', and 'other'. The '1st-party' control is selected. The bottom row shows the 'duckduckgo.com' domain with counts: 2 for 'cookie', 1 for 'css', and 2 for 'script'.

	all	cookie	css	image	media	script	XHR	frame	other
1st-party									
duckduckgo.com		2	1			2			



The screenshot shows the uBlock Origin grid mode. The top row has a dropdown menu set to 'all'. Below it, a row of controls includes 'images', '3rd-party', 'inline scripts', '1st-party scripts', '3rd-party scripts', '3rd-party frames', and '... duckduckgo.com'. The '... duckduckgo.com' control is selected. The bottom row shows the 'improving.duckduckgo.com' domain with a count of 1.

	all		
images			
3rd-party			
inline scripts			
1st-party scripts		+	
3rd-party scripts			
3rd-party frames			
... duckduckgo.com		++	
improving.duckduckgo.com			-

First is uMatrix, second is uBlock. We can see the latter has no way to control Cookies, CSS, Media, XHR, or Other AT ALL, as well as first-party frames and third party images. It has about 20% of the features uMatrix / ηMatrix do. The grid mode in uBlock Origin is just an afterthought compared to its lists. Yet I regularly see the claim that it can replace uMatrix entirely, even by so-called "security experts" - what a joke! **EDIT:** just in case someone accuses me of dishonesty: this is not the full uBlock screenshot, but only the relevant part, since I didn't

want to take up more space than necessary. The part left out does not replace the functionality of the uMatrix grid, but just provides things like element picking or blocking *“large media elements”* (uBlock still lacks separate blocking of images and video per domain), etc.

Hell, I've just looked more deeply at uBlock Origin, and **the situation is even worse than I initially thought**. If a website connects to a certain domain twice or thrice (e.g for a script and a CSS file), uBlock Origin's Advanced Mode can either block all of those requests, or none. On the other hand, with uMatrix, you choose exactly which ones you want to allow by their type. So, it was wrong for me to say that the uBlock grid has 20% functionality of the uMatrix one - the real figure is probably 10% or even less. And the "experts" who think uBlock can replace uMatrix look even funnier.

UPDATE February 2022: a surprising amount of people have bothered me about uMatrix supposedly being "deprecated". Nothing could be further from the truth! Just because the developer stopped updating it doesn't mean anything. During this time, the web didn't change in a way that would inhibit uMatrix functionality. The grid still covers all the requests. The idea that a software needs constant updates to stay useful really needs to die. It is what has got us into this whole privacy and bloat mess in the first place. My clock or drawer have not needed updates for decades, why would a program? BTW, uMatrix is still being updated, so if you really care about this "issue", use Pale Moon.

 [URL Rewriter](#) 

UPDATE May 2021: this used to be Redirector - a Classic Addons Archive extension. But then, a Pale Moon targeted fork was made (and ~~PM versions 29.2.0 and up disable CAA~~

extensions 30+ enables them again), so I've replaced the old one. Redirector was prettier, I guess - but as far as I can see, the functionality is exactly the same. URL Rewriter is a simple addon which enables the user to set automatic redirects by regular expressions. You can redirect privacy-hating, bloated services to user-respecting counterparts, switch regular domains to their onion versions, change languages, append parameters, etc. You need to know regex, of course - which is outside the scope ([MozArchive](#)) of this article. Here are some useful ones though:

Redirect: [^\(http|https\):/\(?:www.\)reddit.com\(.*\)](#) to [https://old.reddit.com\\$2](https://old.reddit.com$2)
Example: <https://www.reddit.com/u/test> becomes <https://old.reddit.com/u/test>
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/\(?:www.\)youtube.com\(.*\)](#) to [https://invidious.namazso.eu\\$2](https://invidious.namazso.eu$2)
Example: <https://www.youtube.com/watch?v=92384> becomes
<https://invidious.namazso.eu/watch?v=92384>
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/twitter.com\(.*\)](#) to [https://nitter.42l.fr\\$2](https://nitter.42l.fr$2)
Example: <https://twitter.com/i/web/status/1234102341328101376> becomes
<https://nitter.42l.fr/i/web/status/1234102341328101376>
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/yewtu.be\(.*\)](#) to [https://invidious.namazso.eu\\$2](https://invidious.namazso.eu$2)
Example: <https://yewtu.be/watch?v=CdVFIFnDcrU> becomes
<https://invidious.namazso.eu/watch?v=CdVFIFnDcrU>
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/invidio.us\(.*\)](#) to [https://invidious.namazso.eu\\$2](https://invidious.namazso.eu$2)
Example: <https://invidio.us/watch?v=CdVFIFnDcrU> becomes
<https://invidious.namazso.eu/watch?v=CdVFIFnDcrU>
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/youtu.be/\(.*\)](#) to [https://invidious.namazso.eu/watch?v=\\$2](https://invidious.namazso.eu/watch?v=$2)
Example: https://youtu.be/qQ_XFUyAV_A becomes
https://invidious.namazso.eu/watch?v=qQ_XFUyAV_A
[Edit](#) [Delete](#)

Redirect: [^\(http|https\):/mobile.twitter.com\(.*\)](#) to [https://nitter.42l.fr\\$2](https://nitter.42l.fr$2)
Example: <https://mobile.twitter.com/i/web/status/1234102341328101376>
becomes <https://nitter.42l.fr/i/web/status/1234102341328101376>
[Edit](#) [Delete](#)

Redirect: [https://imgur.com/\(.*\)](https://imgur.com/(.*)) to [https://i.imgur.com/\\$1.jpg](https://i.imgur.com/$1.jpg)
Example: <https://imgur.com/imageID> becomes <https://i.imgur.com/imageID.jpg>
[Edit](#) [Delete](#)

⚙️ Proxy Privacy Ruler ⚙️

In my fake initiatives report I've criticized the “*Private Browsing*” mode in web browsers as being misleading and not very useful. Well - here's an addon that allows you to fix that. What it does is **take your existing proxy settings and apply them only to private windows**. Anyone who's ever tried TOR probably realized that it's barely usable for regular web browsing - I mean, just the amount of Cloudflared pages will destroy your attempts. With this addon, you can have one window open for surfing as usual - where you'll visit all the TOR-hating sites - and a second private one for the TOR-friendly ones. The Private Browsing mode blocks local data storage by default, which does prevent some tracking (e.g by cookies or JS history snooping) - but since your IP would still be known, it only makes sense in combination with TOR's IP-masking functionality. Another way to use this addon is to set a domain list for which TOR will be used; amazingly, this allows the **seamless browsing of onion domains** without fiddling with proxy settings or using another browser - just type “**.onion*” in the Domain List field. You can also use this extension to work with I2P in a similar way. All in all, this is an excellent addon which bridges the gap between anonymity / privacy and convenience. Other proxy addons are either much more complicated, lack some of its functionality, or are not available for Pale Moon - so I don't recommend them. **Proxy Privacy Ruler is Pale Moon only.**

🌀 Decentraleyes / deCDN 🛡️

Another simple addon. There are certain scripts that are required for many websites to work (jQuery, some google scripts, etc..), but they also spy on you. How to get out of this? Store them locally and connect to those instead! And that's all Decentraleyes does. **Can conflict with uMatrix**. How to solve this? Briefly, you can't allow uMatrix to "steal" the requests that

Decentraleyes replaces, so allow those domains in uMatrix (these rules should work). The HTTPs enforcing addons can also try to steal its requests - installing Decentraleyes AFTER them will prevent that. Available for both Chrome and Firefox based browsers, as well as Pale Moon. **UPDATE May 2026:** deCDN now does the same, but better. Only works in the newest Pale Moon versions though.

HTTPS enforcing addons

UPDATE November 2024: Pale Moon - just like the Chrome- and Firefox- based browsers, now contains the option to *Upgrade Insecure Requests*, which might seem to deprecate the HTTPs enforcing addons at first glance. Yet I've done some testing and can confidently say that it does **not**:

- If the server doesn't support Upgrade Insecure Requests, then the browser option will do nothing whatsoever. Inquirer, somehow, still detects HTTPs availability on non-UIR supporting servers (I think it's because it additionally has the “*Fall back to GET*” option of HTTPs detection, if the UIR header is not sent back by the server).
- The browser option will always send an unencrypted request first, which could be attacked by a MitM. A saved HTTPS Always rule will skip the unencrypted request and prevent this type of attack. The default list contains quite a lot of sites, and you can always copy the rules you've already saved to another installation.
- If - for some reason - you want to connect to a certain website using HTTP (eg. for testing purposes), you can just disable the rule in HTTPS Always and still be able to use HTTPs everywhere else. The browser option does not allow this - it's all or nothing.

Therefore, I still recommend the HTTPS Inquirer+HTTPS Always setup.

Inferior privacy addons

 uBlock Origin, AdBlock Plus, AdGuard, Disconnect, etc. 

A huge, constantly updated, list of blocked elements is required for these to work. For example, AdGuard prides itself on having *“more than 1,800,000 malicious websites on record.”* Not something I would brag about, when it's so simple to just block entire classes of requests via uMatrix, rendering most of these adblockers irrelevant. By using them, you are also **relying on someone else to provide you with the lists**, instead of taking your web browsing into your own hands. **If something isn't on these lists, it will not be blocked**, and you cannot possibly make a list that will capture everything ever. **UPDATE May 2022:** remember that **the lists can also be malicious!** They can let trackers through (maybe with a bribe) or block a site with a "misinformation" or "fake news" label - as some lists (archive) (MozArchive) did to me. So, you are putting the control of your browsing into the hands of a few list maintainers - which, I guess, is still better than the hands of trackers or advertisers. Who incidentally have been ferociously fighting these lists for a long time now (BlockAdBlock, etc.). This has then spawned userscripts and such that block BlockAdBlock, which the advertisers have again responded to...uMatrix just sidesteps this whole dumb war. **With a properly configured uMatrix, you don't need to care about what tricks the trackers or advertisers have got up their sleeves**, since it will all be blocked until you choose otherwise ("default deny" versus "default allow" policy). Adblockers are easier to use (install and go), but in the end, outclassed by uMatrix, if you take the time to learn it. If you really want a list-based extension, Disconnect is the least worst. It has a nice UI and shows you the saved bandwidth and time, as well as a tracker

visualization mode. But really, **learn uMatrix**. Note on uBlock Origin: it has some additional features like element hiding and disabling WebRTC (irrelevant for Pale Moon) - but for basic content blocking, uMatrix is king.

NoScript

UPDATE August 2022: this extension used to be extremely inferior to uMatrix, with the ability to only block scripts per site. This had persisted for about a decade. But the newer versions received a complete overhaul, and the functionality came much closer to uMatrix's:



However, NoScript still lacks controls for cookies, CSS (do not get confused by the

“unrestricted CSS” category, it only blocks certain CSS-based attacks, instead of all CSS requests), or images. And the interface is a lot more intuitive in uMatrix. I also did not confirm if everything else actually works the way it's supposed to, as this extension **is not available for Pale Moon** and I don't care to install the browsers that it supports (Firefox and Chrome-based). A whitelist is also included:



General

Per-site Permissions

Appearance

Advanced

Search or add a web site: [https://noscript.net]



		TRUSTED				...afx.ms
		TRUSTED				...ajax.googleapis.com
		TRUSTED				ajax.aspnetcdn.com
		TRUSTED				...bootstrapcdn.com
		TRUSTED				tinymce.cachefly.net
		TRUSTED				...firstdata.com
		TRUSTED				...firstdata.lv
		TRUSTED				...gfx.ms
		TRUSTED				...google.com
		TRUSTED				...googlevideo.com
		TRUSTED				...gstatic.com
		TRUSTED				...hotmail.com
		TRUSTED				code.jquery.com
		TRUSTED				...live.com
		TRUSTED				...live.net
		TRUSTED				...maps.googleapis.com
		TRUSTED				...mozilla.net
		TRUSTED				addons.mozilla.org
		TRUSTED				...netflix.com
		TRUSTED				...nfixext.com
		TRUSTED				...nfiximg.com
		TRUSTED				...nfixvideo.net
		TRUSTED				...noscript.net
		TRUSTED				...outlook.com
		TRUSTED				...passport.com
		TRUSTED				...passport.net
		TRUSTED				...passportimages.com
		TRUSTED				...paypal.com
		TRUSTED				...paypalobjects.com
		TRUSTED				...securecode.com
		TRUSTED				...securesuite.net
		TRUSTED				...sfx.ms
		TRUSTED				...wlxrs.com
		TRUSTED				...yahoo.com
		TRUSTED				...yahooapis.com
		TRUSTED				...yimg.com
		TRUSTED				...youtube.com
		TRUSTED				...yting.com

This can be disabled, but it shows NoScript is still at its heart an extension designed to make sites "just work" while preventing most attack vectors. It is not like uMatrix, which is like an archer tirelessly shooting down every enemy that's trying to enter the castle - while NoScript lets through a bunch of Trojan horses. There is also some [unethical history \(archive\)](#) ([MozArchive](#)) with this extension; you decide if it is still relevant.

Privacy Badger

Probably the **worst of all the "privacy protecting" extensions**, even though it appears the most advanced, using AI to detect trackers. However, it requires a really long time to find anything (you'd learn uMatrix three times over...), and most of them will still go unnoticed. As it says, *"Privacy Badger looks for tracking techniques like uniquely identifying cookies, local storage "supercookies," and canvas fingerprinting"*. But these are three out of many more tracking ways, and PB will miss the rest. Also, PB only cares about tracking, but there are many other things you may want to block. Maybe you don't want random Twitter images on the sites you're browsing (and you can be tracked by those anyway). The funny thing is, PB enforces the sending of the Do Not Track header, which actually provides a way to track you (worsens your fingerprint). **Ignore the fancy stuff and use uMatrix**, the only content blocking extension you need.

Ghostery

Another really poor addon. It displays the amount of trackers a website contains, and then uses an algorithm to block **only some of them**. It leaves alone, for example, DoubleClick, social media buttons, Google AdSense, many analytics sites, and others. You can choose to block

some or all of these on certain or all sites, but by default, only the ones chosen by the algorithm are blocked. Another function of Ghostery is adblocking, which works the same way, but this time it **doesn't even tell you which ones were blocked**. You can “*restrict site*” so that all trackers on it will be blocked, but that option does not work for ads, so some will get through regardless. And you have to do that separately for every site. Ghostery also shares something called “*Human Web Data*” with its parent company Cliqz by default. No matter, uMatrix is superior.

🇯🇸 LibreJS 🇯🇸

Now let's be clear here - this addon has nothing whatsoever to do with privacy, functionality, convenience, or anything benefiting the user. **It only serves to satisfy a particular brand of autism called freetardism**. So what even is this addon? Well, it was supposed to block “*nonfree and nontrivial*” JavaScript on sites, but the criteria are confusing and imprecise. LibreJS will check whether a "free license" has been applied to a script, and if not, whether it is "trivial" enough for the license to be ignored. **This heavily slows down your browsing**, since it has to check every script on the site according to a bunch of rules for "triviality". And if you click on the LibreJS button, it will show you a barely human-readable dump of data allegedly showing which scripts are "nontrivial" and have been blocked by the addon. You can whitelist them then - a Sisyphean job if I ever saw one. Also, if a script has been blocked, a giant “*COMPLAIN*” overlay will appear to get you to contact the website devs so that they can remove the offending scripts (has that ever worked?). Sounds like a crusade I don't want to be a part of. uMatrix is so much cleaner, faster (actually significantly speeds up your browsing), more powerful, and actually serves the user instead of an ideology. Ditch the gimmicks, get uMatrix!

Like Browsec, Hola, PureVPN, ZenMate, Tunnelbear and many, many others. Not only are these leaky (archive) (MozArchive), but they are **not even real VPN**. This means only certain requests get tunneled (those you make through your browser). On top of that, they add other issues such as bandwidth limits, requiring payment after a free trial, pestering you with popups, or even operating like literal botnets (archive) (MozArchive) - therefore you don't want to use these, ever. Just get a real VPN - good free ones are available such as Snopyta (update: dead) or RiseUp.

Other useful addons

Reader View

Some websites insist on butchering their CSS in a way where half of the screen is blocked by a menu bar at all times, or there are random overlays inside the text, etc. This extension takes care of that by replacing the CSS with a custom one where just the text is visible. The use case doesn't come up often enough, and it doesn't work on all sites - but when one does come up, the extension easily justifies itself. At least when doing research efficiently is a goal, as it is for me. Following: the New York Post without RV, and with.

TRENDING NOW IN LIFESTYLE



How often should you change your underwear? Answer may surprise...



'Selfish' traveler refuses to give up airplane seat so dad can...



The over 150-year mystery of why urine is yellow has finally been...



Alarmed mom-to-be speaks out after 'unhinged' mother-in-law...



LIFE

Gl

ha

times in one day

Get seats. Earn rewards.

Glamorous heiress, 45, charged with having sex with 14-year-old boy four times in one day

Social Links for Andrew Court

4-5 minutes

An Australian horse heiress is saddled with charges after being accused of having sex with a 14-year-old boy four times in a single day.

Savannah Daisley, 45, faced Waverley Local Court in Sydney on Tuesday on child sex abuse allegations, with Judge Jaqueline Milledge denying her bail over the “quite disturbing” allegations.

The glamorous mother of two, who is the daughter of famed Aussie horse breeder [Ross Daisley](#), strongly denies the accusations and intends to plead not guilty.

Cops claim an unbridled Daisley molested the minor four times before 5 p.m. on May 20 last year. It’s unclear whether the pair were known to each other prior to the alleged acts.

An extension allowing mouseless navigation. The main reason to use it is the ability to **visit links by keyboard shortcuts** - press the *F* key, then whatever sequence appears over a particular link. Most other features are either available natively in browsers or don't work in Pale Moon - but that single one makes it worth it. Available for Firefox, Chrome and Pale Moon (through Classic Addons Archive).

🌐 I don't care about cookies 🌐

Some time ago, the EU came up with some bullshit requirement for websites to pester you with cookie "information" that you already know, which just so happens to cover a big part of the screen. This addon will remove those overlays. Of course, uMatrix also gets these if you disallow scripts on those sites, but if you need the functionality provided by scripts (for example on flashscore), then this addon is extremely useful. Available for both Chrome and Firefox based browsers, as well as Pale Moon. Note: can break sites too (Neocities delete button for example).

UPDATE September 2022: fucking AVAST claimed the extension ([MozArchive](#)). Turn off auto-updates now, and seek an alternative (apparently "EasyList Cookies" in uBlock Origin does it, though I've been told it does not get them all), I guess. Another FOSS privacy project bites the dust.

🛠️ Dorando Keyconfig 🛠️

Not much to say here - allows to modify default browser keyboard shortcuts - which for some reason isn't a native feature. Some keybinds not available by default can be found [here](#).

Dorando Keyconfig is Pale Moon only.

Linkification

Turns text links into actual ones. No more copying them into the address bar! Very convenient. Works on E-mail addresses, http(s), ftp, xmpp, file:// links and more - but unfortunately not IP addresses. Therefore, “*email@address.com*” will be made into a link, but “*127.0.0.1*” will not. Still, it's very useful. Pale Moon only - but Chrome and Firefox have alternatives such as Linkbot or Linkify Plus.

Stylus

A fork of an older Stylish version, before it became spyware (archive) (MozArchive). This extension allows you to create custom CSS for every website you visit, and enable or disable them at will. You can test it out on this site by downloading the styles I link to on the main page. Simply click the name of the theme, copy the contents, click the Stylus icon and “*Write style for digdeeper.club*”. Then paste the CSS there and click Save. Now visit my site again and you will see the look change; you can have all the styles installed at once and choose whichever you want at any time. Very convenient and available for both Chrome and Firefox based browsers (Pale Moon uses the Stylem fork). This extension can also double up as an adblocker that will get things even uMatrix can't (by way of element hiding). For example, StartPage ads can be blocked with the style:

```
@namespace url(http://www.w3.org/1999/xhtml);  
@-moz-document domain("startpage.com") {
```

```
#adBlock {  
display:none;  
}  
}
```

[Back to the front page](#)