(https://cyberinsider.com/)

If you buy through links on this site, we may earn a commission, which helps support our work (https://cyberinsider.com/about/).

Firefox Privacy — The Complete How-To Guide for 2025

January 19, 2025 *By* Alex Lekander (https://cyberinsider.com/author/alexlekander/) —

Mozilla Firefox is one of the best browsers available that combines strong privacy protection features, good security, active development, and regular updates. The newest version of Firefox is fast, light-weight, and packed full of privacy and security features.

It is for this reason that I consider Firefox to be the best all-around browser for privacy and security. It remains a solid alternative to some of the other options, such as Google Chrome, Microsoft Edge, and Safari.

Another great aspect of Firefox is that it is **highly customizable**, which is the point of this guide. Below we will go over how you can customize Firefox to give you the security and privacy you desire, while still working well for day-to-day browsing.

But before we jump in, let's cover some important details.

Important considerations before starting

There are many factors to consider when configuring Firefox to meet your needs, including your threat model and browsing preferences. In other words, there is no "one-size-fits-all" configuration that will work for everyone. This guide is a basic overview covering some of the different configurations options.

Before you start modifying Firefox and installing a bunch of add-ons, it's important to consider browser fingerprinting.

Browser fingerprinting

The issue of browser fingerprinting (https://cyberinsider.com/browser-fingerprinting/) (or device fingerprinting) is a big topic that covers all the different ways you can be tracked and identified by your system and various settings. All of the different add-ons you install and preference modifications you make to Firefox are inputs that can potentially be used to identify and track you.

Herein lies the catch-22: the more browser add-ons you install and settings you modify, the more likely you will stand out from the crowd and be easier to track. There are solutions for this and the latest version of Firefox does offer *some* fingerprinting protection. I discuss this problem and also provide solutions in the browser fingerprinting (https://cyberinsider.com/browser-fingerprinting/) guide.

And that leads us to the next point that…

More is not always better

When it comes to browser add-ons and modifications, you don't want to be like that kid who puts every topping imaginable on his ice cream. Similarly, more is not always better with Firefox browser add-ons.

Aside from the issue of browser fingerprinting, having too many add-ons may slow down performance and break things. Many of the popular Firefox add-ons also fulfill the same functions and are **redundant** when used together.

Therefore it is best to strike a balanced approach. Install and modify *only* what you think will be useful and necessary for your specific situation.

Proceed with caution

Modifying some of these settings may interfere with your browsing experience and break some websites (they won't load properly). Therefore taking an **incremental approach may be** the **best** way to proceed. You can continue to install add-ons and adjust your settings as you see what works best for your needs.

This allows you to modify the settings, create exceptions, or add sites to a whitelist.

Firefox privacy tweaks

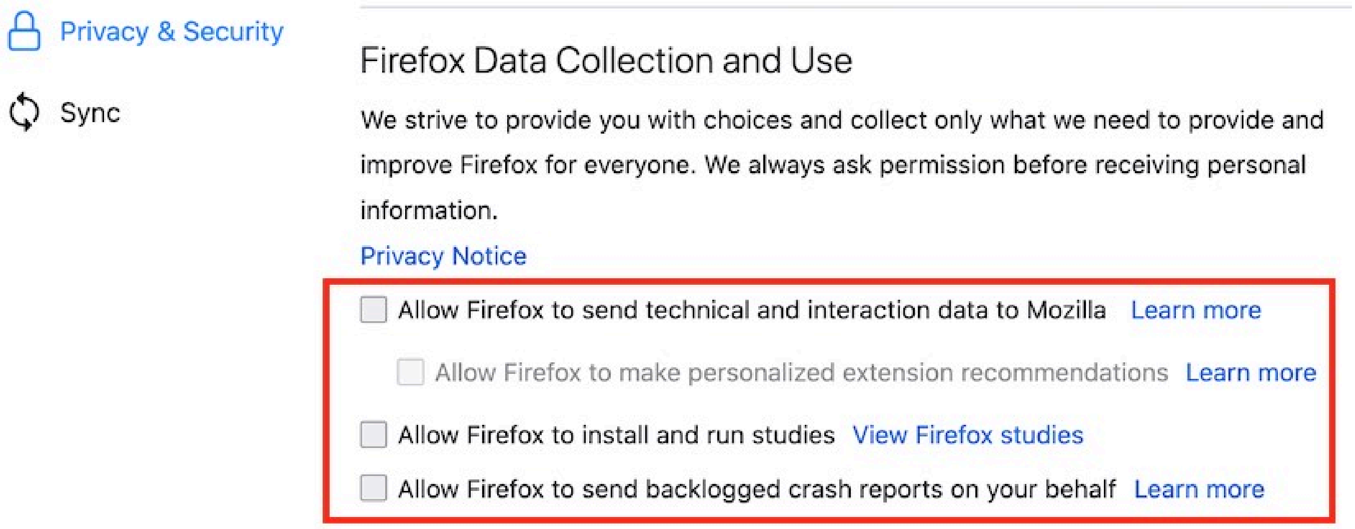
Before you get going with Firefox you may want to adjust the following settings for better privacy.

Note: if you are a Mac OS user, you will see the word “Preferences” in your menu rather than “Options” as it is listed below.

Disable Firefox telemetry

With the latest version of Firefox, it is configured to share “**technical and interaction data**” with Mozilla. This includes the ability to “**install and run studies**” on your computer. You can learn more about these studies (https://support.mozilla.org/en-US/kb/shield?as=u&utm_source=inproduct) and data collection (https://www.mozilla.org/en-US/privacy/firefox/#health-report) practices, but I'd recommend disabling these settings.

To disable go to **Open Menu** (three bars at the top right corner of the browser) > **Options** > **Privacy & Security** > **Firefox Data Collection and Use** and then uncheck the boxes as you see below:



Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.

Privacy Notice

- □ Allow Firefox to send technical and interaction data to Mozilla Learn more
  - □ Allow Firefox to make personalized extension recommendations Learn more
- □ Allow Firefox to install and run studies View Firefox studies
- □ Allow Firefox to send backlogged crash reports on your behalf Learn more

It is easy to disable telemetry in Firefox.

You can also disable data sharing with Firefox for Android by going to **Menu** > **Options** > **Privacy** > **Data Choices** and then uncheck all three categories for Telemetry, Crash Reporter, and Mozilla Location Service.

Note: You can also disable this in the About:Config settings with **toolkit.telemetry.enabled** set to **false**.

Change the default search engine in Firefox

Firefox now uses Google as the default search engine, but there are other private search engines (https://cyberinsider.com/private-search-engine/) you can use instead.

To do this, go to **Menu** > **Options** > **Search** > **Default Search Engine**. Firefox does not provide you with very many alternatives directly in the settings area. However, you can view more options by going down to **One-Click Search Engines** and then click **Find more search engines** to see the other alternatives.

See our guide on private search engines (https://cyberinsider.com/private-search-engine/) to dive into this topic more.

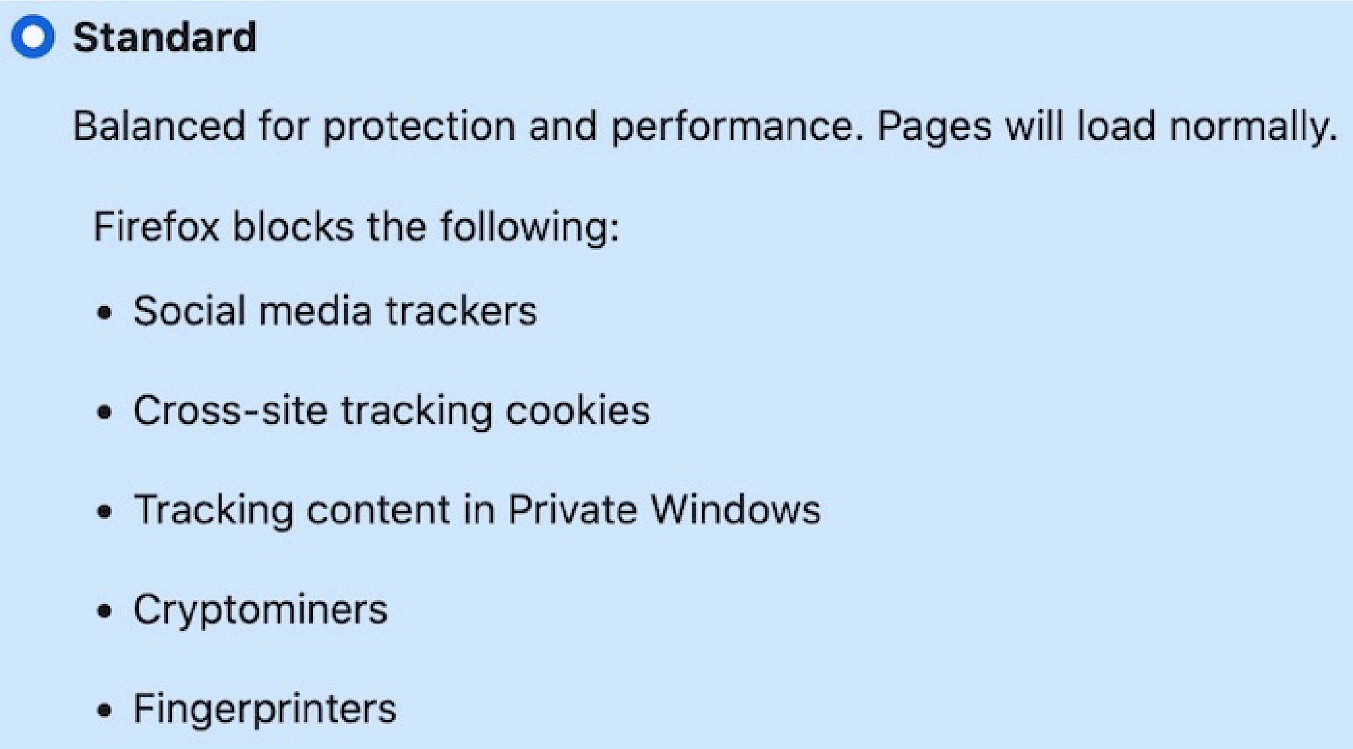
Firefox also has a guide (https://support.mozilla.org/en-US/kb/add-or-remove-search-engine-firefox) on modifying your search engine preferences.

Firefox Content Blocking

Another great new feature with Firefox is Content Blocking. This customizable feature (https://support.mozilla.org/en-US/kb/content-blocking) will automatically block "content that tracks the sites you visit and profiles you." You can choose between Standard, Strict, and Custom modes, which allow you to block:

- Cookies
- Tracking content
- Cyrptominers
- Fingerprinters

To adjust the Firefox Content Blocking settings, go to **Menu** > **Options** > **Privacy and Security** > **Content Blocking** and then select which mode you want to use.



○ **Standard**

Balanced for protection and performance. Pages will load normally.

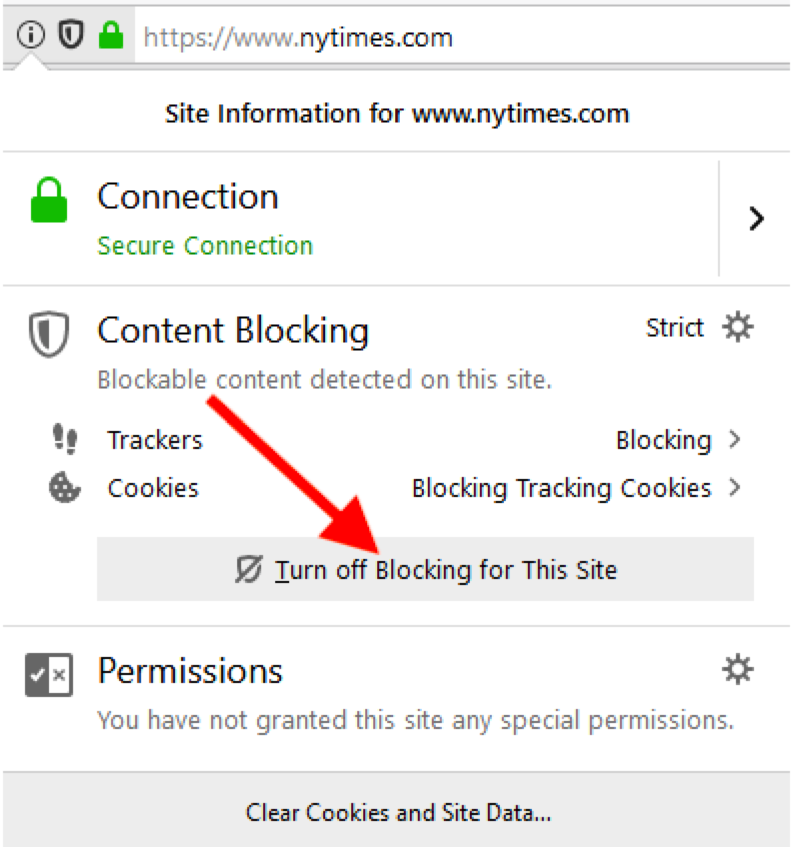
Firefox blocks the following:

- Social media trackers
- Cross-site tracking cookies
- Tracking content in Private Windows
- Cryptominers
- Fingerprinters

The **Standard** setting may be the best balance for regular users. Firefox warns that **Strict** mode may “cause some websites to break.” However, you can still…

Disable content blocking for specific sites

It's easy to disable content blocking for certain trusted sites. Simply enter the website URL, then click the “i” icon to the left of the address bar, then click the grey button to “**Turn off Blocking for This Site**.”



https://www.nytimes.com

Site Information for www.nytimes.com

Connection

Secure Connection

Content Blocking Strict

Blockable content detected on this site.

Trackers Blocking

Cookies Blocking Tracking Cookies

Turn off Blocking for This Site

Permissions

You have not granted this site any special permissions.

Clear Cookies and Site Data...

Another benefit of Firefox's Content Blocking feature is that it can save your data and improve page load speeds.

The “Do Not Track” request

Firefox also has an option to request that websites “do not track” you online. This is simply an HTTP header field (https://en.wikipedia.org/wiki/Do_Not_Track) that you can easily enable. However, the key word here is **request**, because this is not actually blocking anything. We have also learned that many websites simply **ignore these requests** (https://marketingland.com/hulu-joined-list-major-platforms-ignore-not-track-requests-185610).

In addition to being ignored by most sites, this is also a value that can be used for browser fingerprinting purposes, as explained here (https://www.intego.com/mac-security-blog/apple-to-remove-do-not-track-feature-from-safari/). Therefore I no longer recommend enabling or modifying the Do Not Track settings, which you'll find in the Content Blocking settings area.

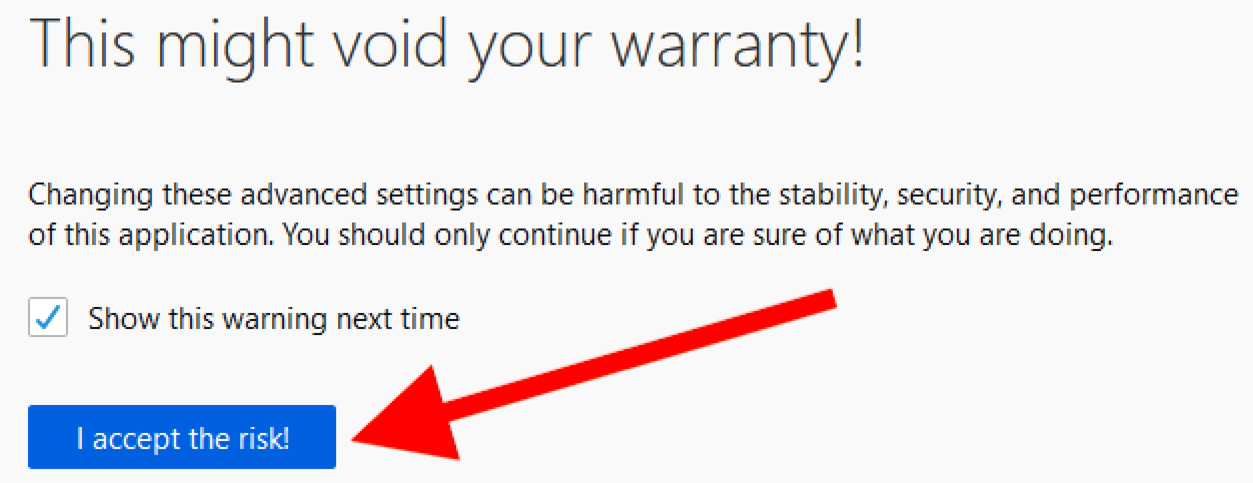
You can learn more about the Do Not Track feature here (https://support.mozilla.org/en-US/kb/how-do-i-turn-do-not-track-feature).

Firefox About:Config settings

Aside from the general Menu settings we used above, you can also make a number of different modifications using **about:config**.

Note: If you made all of the changes above, you may notice that some of these settings are already updated in about:config. We will still cover the different about:config since some people prefer to modify settings in this area, rather than through the general Menu.

To access these configuration settings, simply enter **about:config** into the URL bar and hit enter. You will then be prompted with a warning screen stating "This might void your warranty." Just click "**I accept the risk**" to continue.



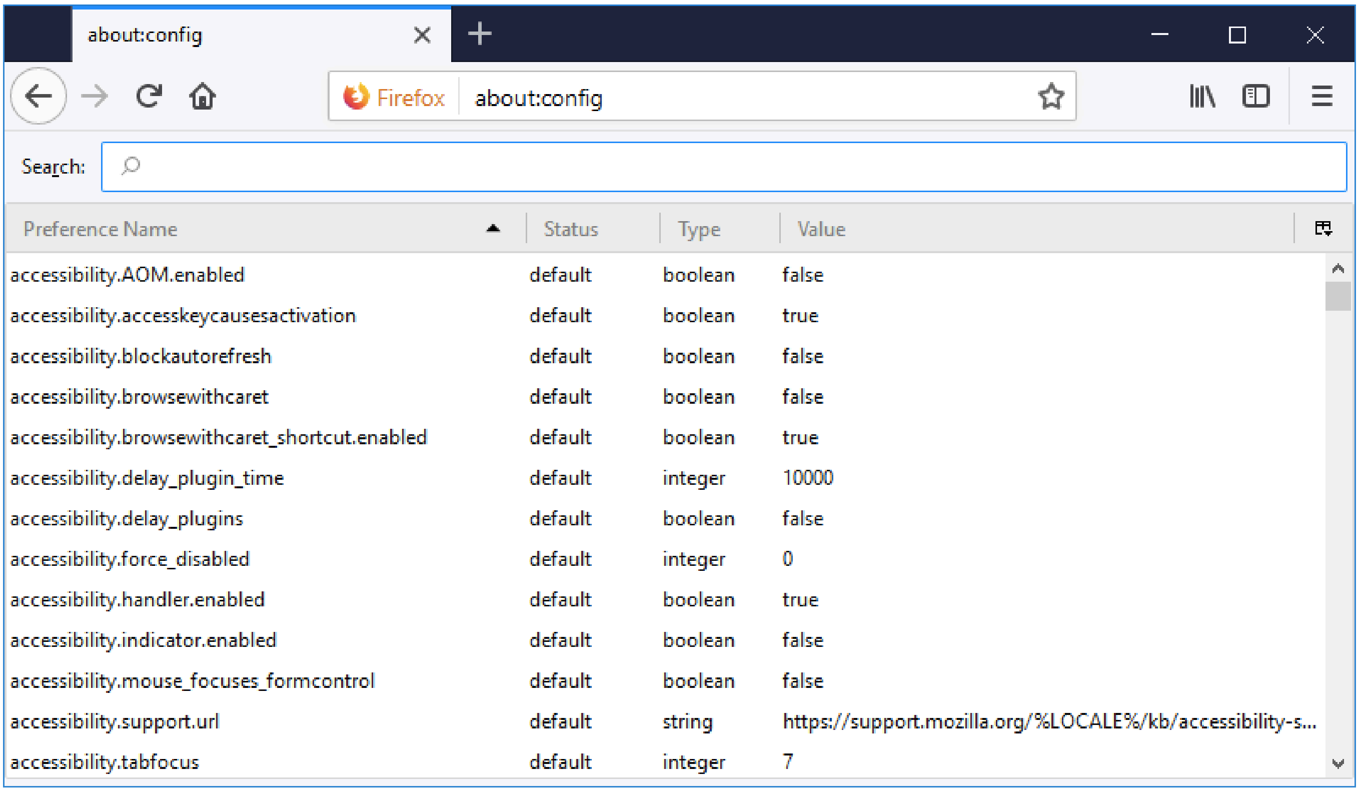
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

After proceeding, you will see a large list of preferences, which each include a status, type, and value.

These preferences will be listed in alphabetical order and are easily searchable from the search bar near the top.



Preference Name	Status	Type	Value
accessibility.AOM.enabled	default	boolean	false
accessibility.accesskeycausesactivation	default	boolean	true
accessibility.blockautorefresh	default	boolean	false
accessibility.browsewithcaret	default	boolean	false
accessibility.browsewithcaret_shortcut.enabled	default	boolean	true
accessibility.delay_plugin_time	default	integer	10000
accessibility.delay_plugins	default	boolean	false
accessibility.force_disabled	default	integer	0
accessibility.handler.enabled	default	boolean	true
accessibility.indicator.enabled	default	boolean	false
accessibility.mouse_focuses_formcontrol	default	boolean	false
accessibility.support.url	default	string	https://support.mozilla.org/%LOCALE%/kb/accessibility-s...
accessibility.tabfocus	default	integer	7

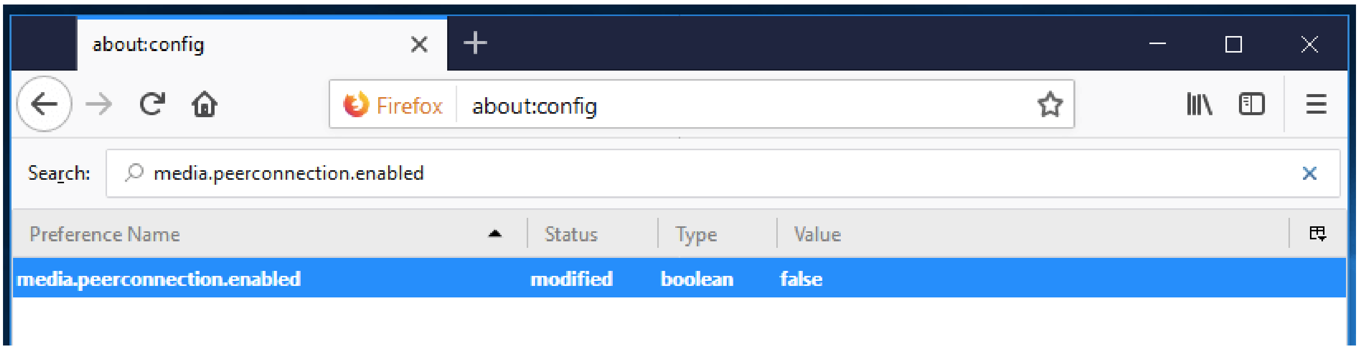
Modifying preferences – You can modify any of these Firefox preferences by simply **double clicking** the preference name. If the preference is a "boolean" type, then double clicking will change the value to true or false. If the preference is an "integer" or "string" type, double clicking will open a box to change the value.

Here are my recommended changes:

Disable WebRTC: media.peerconnection.enabled (WebRTC) = false

WebRTC stands for "Web Real-Time Communication" and it allows for voice, video chat, and P2P sharing through your browser. Unfortunately, this capability can also **expose your real IP address** through browser STUN requests, even if you are using a good VPN service. (This is called a WebRTC leak (https://cyberinsider.com/webrtc-leaks/).)

To disable WebRTC in Firefox simply enter **media.peerconnection.enabled** into the search bar and then double click the value to change it to **false**.



Search: media.peerconnection.enabled

Preference Name	Status	Type	Value
media.peerconnection.enabled	modified	boolean	false

Aside from Firefox, the WebRTC vulnerability also affects Chrome, Opera, Brave, and other Chromium-based browsers. Safari is also in the process of implementing WebRTC.

Note: If you disable WebRTC, services like Google Meet and Whereby may not work.

Resist Fingerprinting: privacy.resistFingerprinting = true

Changing this preference to **true** will help to make Firefox more resistant to browser fingerprinting.

Note: There are many factors that go into browser fingerprinting and the ability of an adversary to identify you. See the browser fingerprinting (https://cyberinsider.com/browser-fingerprinting/) guide for additional details.

privacy.trackingprotection.fingerprinting.enabled = true

This is a new preference with Firefox 67+ to block fingerprinting.

privacy.trackingprotection.cryptomining.enabled = true

Another new preference with Firefox 67+, this will block cryptominers.

First party isolate privacy.firstparty.isolate = true

Changing this to **true** will isolate cookies to the first party domain, which prevents tracking across multiple domains. First party isolation also does much more than isolating cookies, it affects: cookies, cache, HTTP Authentication, DOM Storage, Flash cookies, SSL and TLS session resumption, Shared Workers, blob URIs, SPDY and HTTP/2, automated cross-origin redirects, window.name, auto-form fill, HSTS and HPKP supercookies, broadcast channels, OCSP, favicons, mediasource URIs and Mediastream, speculative and prefetched connections.

This preference was added in late 2017 as part of the Tor Uplift Project (https://wiki.mozilla.org/Security/Tor_Uplift).

Tracking protection privacy.trackingprotection.enabled = true

Another new update, this is Mozilla’s built-in tracking protection feature. This will use a Disconnect.me filter list, but may be redundant if you are using uBlock Origin 3rd party filters.

Disable geolocation tracking geo.enabled = false

Setting this to **false** will **disable geolocation tracking**, which may be requested by a site you are visiting. As explained by Mozilla (https://support.mozilla.org/en-US/kb/does-firefox-share-my-location-websites?redirectlocale=en-US&redirectslug=does-firefox-share-my-location-web-sites), this preference is enabled by default and utilizes **Google Location Services** to pinpoint your location. In order to do that, Firefox sends Google:

1. your computer's IP address
2. information about nearby wireless access points
3. a random client identifier, which is assigned by Google (expires every two weeks)

Before this data is sent to Google, you would first get a request by the site you are visiting. Therefore you do have control over this, even if geo remains enabled.

media.navigator.enabled = false

Setting this preference to **false** will block websites from being able to track the microphone and camera status of your device.

network.cookie.cookieBehavior

This is an integer type preference with different values. Here are the cookie preference options:

- 0 = Accept all cookies by default
- 1 = Only accept from the originating site (block third-party cookies)
- 2 = Block all cookies by default
- 3 = Block cookies from unvisited sites

- 4 = New Cookie Jar policy (prevent storage access to trackers)

Any selection between 1 and 4 would improve privacy. The New Cookie Jar policy (value 4) offers more protection, but it may also break the functionality of some websites. Ghacks has a discussion of the New Cookie Jar policy here (https://www.ghacks.net/2018/09/23/firefox-65-new-cookie-jar-policy-to-block-tracking/).

network.cookie.lifetimePolicy = 2

This is another integer type preference that you should set to a **value of 2**. This preference determines when cookies are deleted. Here are the different options:

- 0 = Accept cookies normally
- 1 = Prompt for each cookie
- 2 = Accept for current session only
- 3 = Accept for N days

With a value of 2, websites you visit should work without any problems, and all cookies will be automatically deleted at the end of the session.

network.dns.disablePrefetch = true

Setting this preference to **true** will disable Firefox from “prefetching” DNS requests. While advanced domain name resolution may slightly improve page load speeds, this also comes with some risks, as described in this paper (https://www.usenix.org/legacy/events/leet10/tech/full_papers/Krishnan.pdf).

network.prefetch-next = false

Similar to prefetching DNS requests above, setting this preference to **false** will prevent pages from being prefetched by Firefox. Mozilla has deployed this feature to speed up web pages that you might visit. However, it will use up resources and poses a risk to privacy. This is another example of performance at the price of privacy.

Disable WebGL:
webgl.disabled = true

WebGL is a potential security risk (https://security.stackexchange.com/questions/13799/is-webgl-a-security-concern), which is why it is best disabled by setting **webgl.disabled** to **true**. Another issue with WebGL is that it can be used to fingerprint your device.

You can get more information on the WebGL issue here (https://www.contextis.com/blog/webgl-a-new-dimension-for-browser-exploitation) and here (https://www.khronos.org/webgl/security/).

dom.event.clipboardevents.enabled = false

This prevents websites from getting notifications if you copy, paste, or cut something from the page.

media.eme.enabled = false

This disables the playback of DRM-controlled HTML5 content. See details here (https://support.mozilla.org/en-US/kb/enable-drm#w_opt-out-of-cdm-playback-uninstall-cdms-and-stop-all-cdm-downloads).

Firefox “safe browsing” preferences

There are many recommendations to disable the Safe Browsing feature in Firefox due to privacy concerns and potential Google tracking. However, these concerns are based on an **older version** of the Safe Browsing feature, which would utilize “real-time lookup” of website URLs. This method has not been in use since 2011 – explained further here (https://feeding.cloud.geek.nz/posts/how-safe-browsing-works-in-firefox/).

If a URL is needed, Firefox takes the following precautions to protect user privacy, as explained by François Marier (https://feeding.cloud.geek.nz/posts/how-safe-browsing-works-in-firefox/), a security engineer for Mozilla:

- Query string parameters are stripped (https://dxr.mozilla.org/mozilla-central/rev/494289c72ba3997183e7b5beaca3e0447ecaf96d/toolkit/components/downloads/ApplicationReputation.cpp#684-710) from URLs we check as part of the download protection feature.
- Cookies set by the Safe Browsing servers to protect the service from abuse are stored in a separate cookie jar (https://bugzilla.mozilla.org/show_bug.cgi?id=897516) so that they are not mixed with regular browsing/session cookies.
- When requesting complete hashes for a 32-bit prefix, Firefox throws in a number of extra “noise” entries (https://dxr.mozilla.org/mozilla-central/rev/494289c72ba3997183e7b5beaca3e0447ecaf96d/toolkit/components/url-classifier/nsUrlClassifierDBService.cpp#283-289) to obfuscate the original URL further.

Therefore I would conclude that disabling Safe Browsing would give you no tangible privacy benefits, while also being a security risk. That being said, if you still want to disable this feature, here's how in the about:config area:

- **browser.safebrowsing.phishing.enabled = false**
- **browser.safebrowsing.malware.enabled = false**

Firefox privacy and security add-ons

There are some great Firefox browser add-ons that will give you more privacy and security. With that being said, many of the add-ons we previously recommended are **no longer necessary thanks to Firefox's upgraded privacy and security settings**.

Note: When looking for Firefox add-ons, be sure to consider what you need in relation to the preferences you modified above. Some add-ons will be **redundant** and not necessary depending on your Firefox preferences and the other add-ons you are using.

uBlock Origin

uBlock Origin (https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/) is an efficient, light-weight blocker that filters both ads and tracking. It has risen to popularity as a powerful alternative to Adblock Plus, which allows “acceptable ads” that many users disdain. One added benefit of uBlock Origin is that it can significantly improve performance and page load speed.

Another great feature with uBlock Origin is the ability to whitelist certain websites. Given that many sites will block access if they detect an ad-blocker, the ability to whitelist will come in handy. uBlock Origin is free and entirely open source (https://github.com/gorhill/uBlock/).

NoScript

NoScript (https://noscript.net) is a script-blocker that allows you to identify/block scripts running on websites. While it does give you control, NoScript can be a pain to get configured properly. It breaks many websites, which requires you to tweak and configure the options. If you are already using uBlock Origin, then you probably don't need to be using NoScript.

This is definitely not an add-on for the casual user or those who don't have the patience to devote some time into configuration.

Using a VPN with Firefox

Firefox currently offers a VPN (https://cyberinsider.com/vpn/) (virtual private network) called **Mozilla VPN**. However, this is just a rebranded version of Mullvad and I have seen many users complaining on various forums about the lack of support when things go wrong.

Note that while some VPNs offer browser extensions for Firefox, these are fundamentally different from a full VPN. A VPN will run on your operating system (not just your browser) and encrypt all internet traffic on your operating system. This is different from a browser extension that only wraps your browsing traffic inside an additional layer of encryption.

Additionally, some Firefox VPN extensions are actually just an extension of the desktop VPN application. These "extensions" literally just extend control of the VPN to a convenient browser interface. We discuss this and more in our guide on the best VPNs for Firefox (https://cyberinsider.com/vpn/best/vpn-for-firefox/).

Firefox DNS over HTTPS (DoH) is not a great idea

Just like with Firefox Private Network, the implementation of DNS over HTTPS also relies on Cloudflare infrastructure. In fact, it makes **Cloudflare the central processing point for all DNS requests** in the Firefox browser **by default**.

While DNS over HTTPS may sound advantageous in some respects, there are also potential concerns. Rather than going over why, you can read the article, ***Centralised DoH is bad for privacy, in 2019 and beyond*** (https://blog.powerdns.com/2019/09/25/centralised-doh-is-bad-for-privacy-in-2019-and-beyond/), which concludes:

> *Centralised DoH is currently a privacy net negative since anyone that could see your metadata can still see your metadata when DNS is moved to a third party. Additionally, that third party then gets a complete log per device of all DNS queries, in a way that can even be tracked across IP addresses.*
>
> *Even if further privacy leaks are plugged, DoH to a third party remains at best a partial solution, one that should not be relied upon as a serious security layer, since it will be hard to plug everything, especially if non-CDN content providers survive.*
>
> *Encrypting DNS is good, but if this could be done without involving additional parties, that would be better.*
>
> *And for actual privacy on untrusted networks, **nothing beats a VPN**, except possibly not using hostile networks.*

Many people also assume that encrypted third-party DNS will somehow offer privacy and anonymity. This is a false assumption. Your IP address and location remains exposed with everything you do online, while your ISP will still be able to see the websites you visit (IP addresses) even if it's no longer handling DNS requests. In conclusion, a good VPN will offer much more protection than DoH through Cloudflare.

To disable DNS over HTTPS (DoH) in Firefox go to **Menu** > **Options** > **General** and then scroll down to **Network Settings** and click the **Settings** button. In the box that opens, scroll down to **Enable DNS over HTTPS**, where it can be enabled or **disabled**.

user.js Firefox hardening

For more information and resources on Firefox hardening, see here: user.js Firefox hardening (https://github.com/ghacksuserjs/ghacks-user.js).

As explained on their GitHub page (https://github.com/ghacksuserjs/ghacks-user.js), this is a "*configuration file that can control hundreds of Firefox settings. For a more technical breakdown and explanation, you can read more on the overview (https://github.com/ghacksuserjs/ghacks-user.js/wiki/1.1-Overview) wiki page.*"

Their Wiki page (https://github.com/ghacksuserjs/ghacks-user.js/wiki) is also full of great information.

Firefox privacy conclusion

In my opinion, Firefox remains the best all-around, mainstream browser on the market for privacy when it is modified as recommended above.

While many of the configurations and add-ons discussed in this guide will go a long way to giving you more privacy, there is one issue that remains: concealing your IP address and location. To do this, a good VPN service (https://cyberinsider.com/vpn/best/) is necessary. The Tor network (https://cyberinsider.com/tor/) also achieves this end, but it comes with the drawbacks of slow speeds, risks, and limitations (only works in a browser).

For more options in addition to Firefox, see the secure browser (https://cyberinsider.com/browser/secure/) guide.

Want to continue on the journey of restoring your online privacy? Check out these guides:

- Private and Secure Email Services (https://cyberinsider.com/email/secure/)
- Secure Browsers That Respect Your Privacy (https://cyberinsider.com/browser/secure/)
- Private Search Engines (https://cyberinsider.com/private-search-engine/)
- Best Password Managers (https://cyberinsider.com/password-manager/best-password-manager/)
- Online Data Removal Services (https://cyberinsider.com/data-removal/best-data-removal-services/)
- Best VPN Services (https://cyberinsider.com/vpn/best/)

This Firefox Privacy article was last updated on January 19, 2025.

About Alex Lekander

Alex is the founder and Editor-in-Chief of CyberInsider.com. His background and expertise includes digital privacy, security, and tech journalism. When he's not working behind a screen, Alex is probably tinkering with a boat or enjoying the outdoors.

Comments

max johnson

February 14, 2025 (https://cyberinsider.com/firefox-privacy/#comment-95035)

Why have you neither mentioned arkenfox (github) nor yokoffing ??

Reply

Office Guy

January 24, 2025 (https://cyberinsider.com/firefox-privacy/#comment-85411)

OR . . . . you can just use Brave and have default privacy. Whose to say any changes won't revert back when FF is updated ? It's ridiculous that users have to apply a "user.js" patch to have proper privacy, and what happens if it breaks sites ? I'll bet that FF user-base is dropping cause it's a pain in the neck to do all these "tweaks", when their are way better browsers.

Reply

CONNECT

About Us (https://cyberinsider.com/about/)

Contact (https://cyberinsider.com/contact/)

Newsletter (https://cyberinsider.com/newsletter/)

𝕏 (https://twitter.com/CyberInsidercom)

(https://www.facebook.com/profile.php?
id=61557842931135)

NEWS TOPICS

- Security (https://cyberinsider.com/security/)
- Data Breach (https://cyberinsider.com/data-breach/)
- Ransomware (https://cyberinsider.com/ransomware/)
- Legal (https://cyberinsider.com/legal/)
- Software (https://cyberinsider.com/software/)
- Windows (https://cyberinsider.com/windows/)

- Privacy (https://cyberinsider.com/privacy/)
- Hardware (https://cyberinsider.com/hardware/)
- Android (https://cyberinsider.com/android/)
- iOS (https://cyberinsider.com/ios/)
- Phishing (https://cyberinsider.com/phishing/)
- Cloud (https://cyberinsider.com/cloud/)

REVIEWS

- Secure Email Services (https://cyberinsider.com/email/secure/)
- Password Managers (https://cyberinsider.com/password-manager/best-password-manager/)
- Secure Browsers (https://cyberinsider.com/browser/secure/)
- Best VPN Services (https://cyberinsider.com/vpn/best/)
- Identity Theft Protection (https://cyberinsider.com/identity-theft-protection/best/)
- Private Search Engines (https://cyberinsider.com/private-search-engine/)
- Best Data Removal Services (https://cyberinsider.com/data-removal/best-data-removal-services/)

· Privacy Policy (https://cyberinsider.com/privacy-policy/) · Terms of Use (https://cyberinsider.com//terms-of-use/) · Contact (https://cyberinsider.com/contact/)