

Better Web Browsing

1. Choosing a web browser
2. Adjust your settings
 1. Disable third-party cookies
 2. Clear cookies on exit
 3. Disable Java
 4. Change default search engine
3. Browser extensions
 1. Essential extensions
 2. Advanced extensions
 3. Harmful or not recommended
4. Verify Riseup's certificate fingerprints

Choosing a web browser

All four major web browsers, Firefox, Chrome, Microsoft Edge/IE, and Safari, have experienced severe security flaws in the recent past, so you should make sure you are using the most up-to-date version, whichever one you choose.

All four major browsers receive a failing grade in our Browser Privacy Scorecard (</en/security/network-security/better-web-browsing/browser-score-card>). However, these browsers can be made much better by installing certain extensions (see below).

Alternately, the Tor project provides a modified version of Firefox adapted to be more secure and anonymous called Tor Browser (<https://www.torproject.org/download/download-easy.html.en>).

Adjust your settings

Disable third-party cookies

Third-party cookies are tracking identifiers used by advertising networks to track your behavior as you browse from website to website. They are an abomination and serve no legitimate purpose.

- Firefox: Preferences > Privacy > Accept third-party cookies > Never.
- Chrome: Settings > Show advanced settings... > Content settings > Block third-party cookies and site data.

Clear cookies on exit

Most browsers keep cookies around much longer than necessary. It is best to configure your browser to delete cookies when you quit the browser.

- Firefox: Preferences > Privacy > Keep until > I close Firefox.
- Chrome: Settings > Show advanced settings... > Content settings > Keep local data only until you quit your browser.

Disable Java

Java also has many security problems and you probably have never used it. Remove or disable it with haste.

- Firefox: Add-ons > Plugins > Java > Never Activate.
- Chrome: Settings > Show advanced settings... > Content settings > Do not run plugins by default.

Change default search engine


While you are adjusting your setting, take the opportunity to change your default search engine to duckduckgo.com (<https://duckduckgo.com>). Riseup recommends DuckDuckGo over other privacy-respecting search engines. See instructions for desktop browsers (<https://duck.co/help/desktop/adding-duckduckgo-to-your-browser>) or mobile browsers (<https://duck.co/help/mobile>).


Browser extensions


The extensions in this list work for both Firefox and Chrome, unless otherwise noted.

Essential extensions

These are absolutely essential browser extensions that everyone should be using all the time. They are stable, open source, and rarely cause websites to break.

 **uBlock Origin** (<https://github.com/gorhill/uBlock>) (Chrome (<https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm>), Firefox (<https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/>)) prevents most advertisements and tracking networks. It is similar to Adblock Plus or Disconnect but works better and is much faster.

 **HTTPS Everywhere** (<https://www.eff.org/https-everywhere>) will automatically switch to secure TLS connections whenever the website supports it. This helps to protect against surveillance of the content of your web browsing, although it does not hide which websites you are visiting (unless you also run Onion Service configuration (</en/email/settings/tor>) or a VPN (</en/vpn>)).

 **Privacy Badger** (<https://www.eff.org/privacybadger>) dynamically detects attempts to track your browsing behavior and blocks content from these trackers. Privacy Badger is not designed to stop ads, so it is not a replacement for uBlock, but it includes some security features that uBlock (in default mode) does not have.

Usage notes:

- Leaking IP addresses: All browsers will leak your real IP address when using audio or video conferencing. If you use a VPN or Tor with audio or video chat, then you should open the uBlock settings and enable the option that prevents WebRTC from leaking your real IP address.
- uBlock advanced mode: If you run uBlock in advanced mode (<https://github.com/gorhill/uBlock/wiki/Advanced-user-features>), you should not also run Privacy Badger.

Advanced extensions

These extensions are for advanced users because they are complicated to use or cause many websites to malfunction.

These extensions attempt to overcome basic privacy flaws in how web browsers work. However, many websites rely on these privacy flaws for basic functionality, so attempts to fix these problems can often make a website stop working.

Some of these privacy flaws include:

- **HTTP Referrer:** When you click a link, your browser sends to the new website the location of the old website. Because sensitive or personally identifying information might be included in the URL of a particular page, the HTTP Referrer should be disabled. You can only do this with an extension.
- **HTTP User-Agent:** Your web browser sends a special “User-Agent” string to every website that it visits. This string contains a lot of uncommon information that can be used, in combination with other data, to uniquely identify your traffic. There is little point in this browser fingerprint these days, and it is better to use a generic value, such as the one used by the Tor Browser.
- **HTML5 Canvas:** Many websites have started to use the HTML5 Canvas to uniquely fingerprint your browser and track your behavior. There is currently no way to disable this, although some new extensions make a crude attempt.
- **JavaScript:** JavaScript is essential for most websites these days, but there are times when you may wish to disable it. When JavaScript is enabled, it is much easier for a website to fingerprint your browser and track your behavior. Also, most browser security vulnerabilities are caused by JavaScript.

For Firefox:

- Self Destructing Cookies (Firefox) (<https://addons.mozilla.org/en-US/firefox/addon/self-destructing-cookies/>) will clean out the cookies for a website when all the tabs for that site have been closed (rather than requiring that you restart the browser).
- µMatrix (<https://addons.mozilla.org/en-US/firefox/addon/umatrix/>) allows you to selectively block Javascript, plugins or other resources and control third-party resources. It also features extensive privacy features like user-agent masquerading, referer blocking and so on. It effectively replaces NoScript and RequestPolicy.
- User-Agent Switcher (<https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/>) will allow you to modify the HTTP User-Agent.
- Canvas Fingerprint Blocker (<https://addons.mozilla.org/en-US/firefox/addon/canvasblocker/>) will allow you to disable HTML5 canvas support for particular websites.

For Chrome:

- µMatrix (<https://chrome.google.com/webstore/detail/%C2%B5matrix/ogfcmafjalglgfnmanfmnieipoejdcf>) allows you to selectively block Javascript, plugins or other resources and control third-party resources. It also features extensive privacy features like user-agent masquerading, referer blocking and so on. It effectively replaces NoScript and RequestPolicy.
- User-Agent Switcher (<https://chrome.google.com/webstore/detail/user-agent-switcher/ffhkkpnpnpgnfaobgihpdblhhmmmbodake>) will allow you to modify the HTTP User-Agent.
- CanvasFingerPrintBlock (<https://chrome.google.com/webstore/detail/canvasfingerprintblock/ipmjngkmngdcdpmgmiebdmfbkcecdndc>) will block most HTML5 Canvas fingerprinting (not open source).

Harmful or not recommended

Despite their popularity, we recommend that you avoid the following extensions.

- Adblock Plus (<https://adblockplus.org/>) used to be the best extension to block ads and tracking. However, now they run a bribery scheme where advertisers can pay to bypass their filters. Also, uBlock is better technology anyway.

- Disconnect (<https://disconnect.me/disconnect>) works like uBlock, and is open source. If you are running uBlock, Disconnect is unnecessary, although it has some visualization features that uBlock does not.
- Ghostery (<https://www.ghostery.com>) works like uBlock, but has horrible defaults that allow most tracking, and the source code is proprietary.
- Flash Block (Firefox) is an extension which allows you to ‘click to play’ Flash. It is preferable to uninstall Flash. Also, this functionality is now built in.
- Better Privacy (<https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/>) was needed in the past to remove LSO or “Flash cookies”, but since the advent of ClearSiteData API (https://en.wikipedia.org/wiki/Local_shared_object#Browser_control), this is no longer needed.
- TrackMeNot will generate bogus search traffic. It is an interesting idea, but it is much better to just use DuckDuckGo.

Verify Riseup’s certificate fingerprints

On the internet, a certificate is needed in order to verify the identity of people or computers. These certificates are also called SSL certificates or identity certificates. We will just call them “certificates” here.

In particular, certificates are needed to establish secure connections. Without certificates, you would be able to ensure that no one else was listening, but you might be talking to the wrong computer altogether! All riseup.net servers and all riseup.net services allow or require secure connections.

To be certain you are communicating securely with Riseup, see how to verify Riseup’s certificates (</en/security/network-security/certificates>).