

Forum:[Hack Forums](#)

Thread: [Harden Firefox \(Make firefox Secure\)](#)

MoonP - October 17, 2022, 3:29 am

Firefox is arguably the best browser for private browsing but it is at least a good option.

But out of the box, it is lacking greatly.

So how do you improve your security and privacy online?

First we will go over the browser settings:

General

We do not want to open previous tabs on startup, when its gone it should be gone, important sites should be kept in your bookmarks bar. (I recommend setting it to always show)

How you navigate around etc does not really matter so I will not cover general settings.

Select whatever font you wish, keep in mind that a different/non default font will allow you to be fingerprinted easily....normally we can prevent this later.

We should enable automatic updates (when firefox is not running) as this allows us to access important privacy updates faster, such as Mozilla's anti-tracking icons update.

Network settings should be managed by your VPN of choice - MullVad is a solid choice due to their privacy features and attempts to improve anonymity for signup/purchase, I would recommend purchasing from one of their verified resellers who offer Bitcoin(BTC) payments or simply paying via Cash.

Home

The home page content should be removed to prevent unnecessary recommendations or ads - only the web search is recommended.

Search

Search Engine of preference, Searx,Qwant is recommended.

Disable search suggestions.

Privacy & Security

We want to use the maximum security setting, but this will be changed later anyway.

Always send a DNT signal.

Delete cookies and site data on close - We do not want any cookies to stay beyond browser close, this helps to avoid cross site tracking or building a profile of you. It will also prevent bypass of 2FA by malware that uses cookie grabbing and injection.

We do not want to save any passwords - storing passwords in your browser is always a bad idea and is very vulnerable to malware. Browsers have terrible security, storing your passwords in a file on disk.

Do not use a master password or microsoft sign in. (You shouldn't really even use a microsoft account.)

Clear all history when firefox closes - again this is vulnerable to malware and tracking, there is no need to have a log of everything you have ever done online.

Make sure no websites have automatic permission to use your microphone, camera etc, this should always need to be requested.

Block popups.

Warn about extension/add-on installs.

Disable all firefox data collection.

Block dangerous and deceptive content.

You don't really need to block dangerous downloads, you should be able to manage your own device security.

Query OCSP responder servers.

Enable HTTPS only in all windows.

Sync

Personal choice, it isn't needed but isn't incredibly dangerous.

Search for "about:config"

dom.event.contextmenu.enabled = false

Don't allow websites to prevent use of right-click,
or otherwise messing with the context menu.

media.peerconnection.enabled = false

Disable WebRTC leaking real IP

security.ssl.require_safe_negotiation = true

Require Safe Negotiation to optimize SSL

security.tls.enable_Ortt_data = false

plugin.scan.plid.all = false

Disable scanning for plugins for fingerprint or detecting adblock

browser.newtabpage.activity-stream.feeds.telemetry browser.newtabpage.activity-stream.telemetry
= false

browser.pingcentre.telemetry = false

devtools.onboarding.telemetry-logged = false

media.wmf.deblacklisting-for-telemetry-in-gpu-process = false

toolkit.telemetry.archive.enabled = false

toolkit.telemetry.bhrping.enabled = false

toolkit.telemetry.firstshutdownping.enabled = false

toolkit.telemetry.hybridcontent.enabled = false

toolkit.telemetry.newprofileping.enabled = false

toolkit.telemetry.unified = false

toolkit.telemetry.updateping.enabled = false

toolkit.telemetry.shutdownpingsender.enabled = false

Disable all mozilla telemetry

privacy.firstparty.isolate = true

Disable supercookies/cross site tracking

security.ssl.enable_false_start = false

Disable TLS false starting

browser.formfill.enable = false

Disable automatic formfilling such as logins, credit cards, shipping etc

browser.cache.disk.enable = false

browser.cache.disk_cache_ssl = false

browser.cache.memory.enable = false

browser.cache.offline.enable = false

browser.cache.insecure.enable = false

Disable disk caching

`dom.event.clipboardevents.enabled = false`

Don't allow websites to prevent copy and paste.

Disable notifications of copy, paste, or cut functions.

Stop webpage knowing which part of the page had been selected.

`network.IDN_show_punycode = true`

Show punycode. Help protect from character 'spoofing' or IDN Homograph attacks

`plugins.enumerable_names = blank`

Disable site reading installed plugins.

`network.http.sendRefererHeader = 0`

Tells website where you came from. Disabling may break some sites.

0 = Disable referrer headers.

1 = Send only on clicked links.

2 = (default) Send for links and image.

`network.http.sendSecureXSiteReferrer = false`

Disable referrer headers between https websites.

`network.http.referer.spoofSource = true`

Send fake referrer (if choose to send referrers).

`geo.enabled = false`

`geo.wifi.uri = blank`

`browser.search.geoip.url = blank`

Disables geolocation and firefox logging geolocation requests.

`browser.send_pings = false`

Prevent website tracking clicks.

`browser.send_pings.require_same_host = true`

Only send pings if send and receiving host match (same website).

`dom.battery.enabled = false`

Disable website reading how much battery your device has.

`network.cookie.alwaysAcceptSessionCookies = false`

Disables acceptance of session cookies.

Now that our firefox is configured properly, we have basic security, but some settings may seem annoying such as not saving passwords.

This is where we turn to extensions, while we can be fingerprinted by how many extensions we have etc, it is much more beneficial to use these than to not.

Adblock:

uBlock Origin - blocks ads

Tampermonkey with AntiAdblock Killer Script - prevents websites disabling ublock

FastForward - skip delays such as shortened url's + website loading delays + block IP loggers

Skip Redirect - prevent in site redirects

Anti-Grabify - blocks many popular IP logging links

Anti-Fingerprinting:

Chameleon - reports fake information about system and browser

Chameleon Settings:

Profile - Random Desktop Profile Every Minute

Headers - Yes/Yes/Yes/No/No/Default/Default

Injection - Enable all + spoof timezone and resolution

Standard - No/Yes/Yes/On/Block 3rd Party (Allow All to fix websites like Discord not loading)

Cookies - Yes/Reject 3rd Party

Anonyme - hide identifiable information such as profile pictures

Google Analytics Blocker - prevents participation in google analytics

Opt-Out for Analytics - say no to google analytics in case previous fails

WebGL Fingerprint Defender - reports fake values to prevent fingerprinting

Canvas Fingerprint Defender - reports fake values to prevent fingerprinting

AudioContext Fingerprint Defender - reports fake values to prevent fingerprinting

Font Fingerprint Defender - reports fake values to prevent fingerprinting

Decentraleyes - prevents centralized content delivery

DuckDuckGo Privacy Essentials - blocks trackers and provides privacy rating of sites

ClearURLs - shortens URLs to remove referral information

AmIUnique - evaluate your browsers privacy rating

Redirect to DuckDuckGo - changes links including other search engines to be sent via duckduckgo

Firefox Relay - create email forwarding inboxes to prevent giving out your true email /// AnonAddy - create email forwarding inboxes to prevent giving out your true email

Tab Anonymizer - prevent monitoring of websites visited by renaming tab titles (prevent software seeing tab names in process explorer)

With all of this, our firefox now has better fingerprint protection.

Cooligan - October 17, 2022, 3:40 am

This definitely isn't the typical first HF thread that people will normally make. Nice one [MoonP](#)

Welcome to HF, I hope to see many more HQ threads from you.

Oh and you should also go make a thread in Introductions, let us know a bit about you!

Bastille - October 17, 2022, 3:48 am

(Oct 17, 2022 03:40 AM)Cooligan Wrote: [\[CITE\]](#) This definitely isn't the typical first HF thread that people will normally make. Nice one [MoonP](#)

Welcome to HF, I hope to see many more HQ threads from you.

Oh and you should also go make a thread in Introductions, let us know a bit about you!

Mhhhh, looks like a lot what I've read in a book few months ago, but I think he skipped some parts and cut some paragraphs. The book is this one :

https://www.amazon.com/Open-Source-Intelligence-Techniques-Information/dp/B09PHL6Q4G/ref=sr_1_12?crid=11HRO0P53IP8Z&keywords=osint&qid=1666003561&qu=eyJxc2MiOiI1LjI0IiwicXNhIjo iNC41OCIsInFzcCI6IjQuMTcifQ%3D%3D&srefix=osin%2Caps%2C163&sr=8-12

Didn't finish it yet, need more time, but it's very interesting !

Welcome OP, hope we'll see you posting more often here, few members are really concerned about security, would be nice to add one member to our community.

Cooligan - October 17, 2022, 3:59 am

(Oct 17, 2022 03:48 AM)Yseurk Wrote: [\[CITE\]](#) Mhhhh, looks like a lot what I've read in a book few months ago, but I think he skipped some parts and cut some paragraphs. The book is this one :

https://www.amazon.com/Open-Source-Intelligence-Techniques-Information/dp/B09PHL6Q4G/ref=sr_1_12?crid=11HRO0P53IP8Z&keywords=osint&qid=1666003561&qu=eyJxc2MiOil1LjI0IiwicXNhIjo iNC41OCIsInFzcCI6IjQuMTcifQ%3D%3D&sprefix=osin%2Caps%2C163&sr=8-12

Didn't finish it yet, need more time, but it's very interesting !

Welcome OP, hope we'll see you posting more often here, few members are really concerned about security, would be nice to add one member to our community.

Ah damn. I tried Googling it to see if any matching results would pop up but couldn't find anything. Maybe I didn't search enough, I also didn't even try dorking it seeing how long it is lol.

Nonetheless like you said it'd be nice to see another security-minded, overall WHH type of member in the community.

Aveling - October 17, 2022, 4:04 am

Thank you for writing this guide, it's always great to see extra focus on FireFox nowadays.

MoonP - October 17, 2022, 5:46 am

(Oct 17, 2022 03:48 AM)Yseurk Wrote: [\[CITE\]](#) Mhhhh, looks like a lot what I've read in a book few months ago, but I think he skipped some parts and cut some paragraphs. The book is this one :

https://www.amazon.com/Open-Source-Intelligence-Techniques-Information/dp/B09PHL6Q4G/ref=sr_1_12?crid=11HRO0P53IP8Z&keywords=osint&qid=1666003561&qu=eyJxc2MiOil1LjI0IiwicXNhIjo iNC41OCIsInFzcCI6IjQuMTcifQ%3D%3D&sprefix=osin%2Caps%2C163&sr=8-12

Didn't finish it yet, need more time, but it's very interesting !

Welcome OP, hope we'll see you posting more often here, few members are really concerned about security, would be nice to add one member to our community.

Thank you! ?

Blockonome - October 18, 2022, 2:18 pm

This looks good, I have not read it all, but I am definitely saving this for later.

SIM-587985 - October 20, 2022, 8:25 am

Nice, Yall should check ["Browser in the box"](#) as well if you want to run Firefox through a virtual machine.