

Forum:[Hack Forums](#)

Thread: [The Complete Browser Security & Privacy Setup](#)

SecureOp - October 12, 2018, 5:05 pm

The Complete Browser Security & Privacy Setup

Over here I'm going to give you the direct instructions to setup the ideal browser, being modified Firefox. Now when I say 'ideal', this is in reference to Hack Forum members for a reason. This tutorial can be mixed and match with a lot of other different settings, so if your a user who doesn't need to take all that extreme precaution, you can choose what to adjust.

Every individual human has a unique fingerprint, if you'd like to track someone down you start with this. The same goes for the internet, except virtually. If you'd like to track someone down you'll need to combine information, and one of that vital piece of information is a browser fingerprint. Browser fingerprinting is a combination of details pulled from plugins, operating system, and other entities to uniquely identify and track with accuracy.

In certain situations, it becomes ironic as the user can use all means measurable to hide his identity via VPN, CookieHiders, InformationSpoofers, and all other addons/plugins.. Yet this would create an even more unique of a browser fingerprint. The argument here is there will always be a 'browser fingerprint', but it's up to the end user to modify and adjust it to their needs and capabilities.

We'll be using Firefox for this, so open it and type about:config

Disable Telemetry :-

Code `datareporting.healthreport.uploadEnabled`

Then set to false : This will not allow firefox to send browser's performance and stability reports back to them.

Disable Copy & Paste Log :-

Code `dom.event.clipboardevents.enabled`

Then set to false : This will not allow websites owners to read/modify/view this information, along with disable any scripts which prohibit of pasting in certain online forms (ex. verifying email). You will also be able to bypass anti-copy features on specific websites.

Disable Web Storage :-

Code `dom.storage.enabled`

Then set to false : This will prohibit web-application software methods and protocols used for

storing data in a web browser. Please note this can affect function or view of certain websites.

Disable Google Safe Browsing :-

Code `browser.safebrowsing.phishing.enabled` Code `browser.safebrowsing.malware.enabled`

Then set to false : Google Safe Browsing is a tool made to prevent phishing websites, but by enabling leaving this on you are accepting to give Google your browsing history. Phishing websites are identifiable by experienced users, however you can have the followed named extensions for prevention.

Change Homepage & Search Engine :-

Code `browser.startup.homepage`

Then set to <https://www.startpage.com/> : This will use a safe and recommend search engine when you first open Firefox (homepage), more available [here](#)

or

Visit : <https://www.startpage.com> & click “Add to Firefox”

Download > Click Add > Will ask to set as default Search Engine > Yes

Disable Geolocation :-

Code `geo.enabled`

Then set to false : This will automatically select preference to not share your location.

Disable Web Real-Time Communication :-

Code `media.peerconnection.enabled`

Then set to false : This will prevent websites being able to directly detect your computer's host IP when using features such as voice calling, video chat, or P2P connections directly in your browser. VPN users automatically assume that this is covered, however not all VPN Providers provide blocking of WebRCT leaks.

Disable DNS Prefetching :-

Code `network.dns.disablePrefetch`

Then set to true : This will prevent DNS resolvers from obtaining any data from prefetching leaks. To read more indepth about this click [here](#)

Disable Hyperlink Information :-

Code `network.http.sendRefererHeader`

Then set to 0 : This will prevent clicked hyperlinks from providing information about the page you clicked the link from, data of this sort can track you from one website to another.

&

Code `network.http.sendSecureXSiteReferrer`

Then set to false : Same as above.

Disable Prefetching :-

Code `network.prefetch-next`

Then set to false : This prevent algorithms assuming and predicting which resources are likely to be accessed by the browser user to speed up results, however has privacy implications. More information can be found [here](#)

Enable Tracking Protection :-

Code `privacy.trackingprotection.enabled`

Then set to true : This will enable a shield, helps prevent cross-site tracking and as an extra benefit load pages 44%, you can see why in this [following link...](#)

Extensions / Add-Ons

*[uBlock Origin](#) - A form of adblocker, with tweaked features to go the extra-mile in terms of anti-tracking.

*[Privacy Badger](#) - Privacy Badger blocks spying ads and invisible trackers.

*[NoScript](#) - Perfect tool to prevent malicious scripts in Javascript, Java and Flash.

*[uMatrix](#) - In the mix of uBlock + NoScript, for advance users who wish to work with source-code.

*[Chameleon](#) - Spoof your browser profile.

*[CookieAutoDelete](#) - To manage and delete cookies accordingly.

* = Best Together / * = Don't need together / * = Additional

Alternatives & Additional

Tor - Certain individuals would rather download a browser which does explains what's in the tutorial, in that case the popular Tor is there.

VPN - Highly recommended to always use with configured browsers, especially paid ones with reliable reviews and standards.

Proxies - Public or private proxies are a great way to shuffle more connects, and create that extra layer of security.

VMWare - Throwing this configuration into a setup Windows Virtual Machine is also a great way to

top it off.

Conclusion

Hope you utilized this informational to your needs, if you have any questions or suggestions send me a private message or reply below. ?

If you'd like a bit more in-depth information check [here](#).

vaxton - October 13, 2018, 6:06 am

so many interesting information, this should be pinned!

MR. MORNINGSSTAR - October 13, 2018, 6:14 am

This is a nice list of information.

Thanks for posting!

DirtyDiesel - October 13, 2018, 7:18 am

Thank you for this! ?

Saber Tooth Ram Tiger - October 13, 2018, 8:01 pm

This was actually more informative than I thought it was going to be.

Thank you for sharing this.

zoh - October 13, 2018, 8:22 pm

Can we use do this on Chrome?

SecureOp - October 14, 2018, 6:44 am

Thank you for the replies.

(Oct 13, 2018 08:22 PM)Koolhunk Wrote: [\[CITE\]](#) Can we use do this on Chrome?

Yes, technically you can but a lot would suggest not to. Reason being you'll be modifying and browser made to accustom these features.

V.V.V.V.V - October 14, 2018, 1:28 pm

Some really great info in here!

Many things that I actually didn't know of at all. Thank you for sharing this and good job writing it all up.

Thanks.

SecureOp - October 14, 2018, 2:03 pm

(Oct 14, 2018 01:28 PM)V.V.V.V.V Wrote: [\[CITE\]](#) Some really great info in here!

Many things that I actually didn't know of at all. Thank you for sharing this and good job writing it all up.

Thanks.

Thanks, glad you got something out of it.

DirtyDiesel - October 14, 2018, 7:21 pm

Epic guide, Thanks for putting it together so nicely. Noticed a slight increase in browser speed and

page loading, almost like a fresh install.

amateur - October 15, 2018, 9:49 pm

thanks for this knowledgeable information man

SniperKiller - October 16, 2018, 10:18 am

Lovely information! Lovely information!

SecureOp - October 19, 2018, 3:04 pm

(Oct 16, 2018 10:18 AM)SniperKiller Wrote: [\[CITE\]](#) Lovely information! Lovely information!
Lol, lovely lovely yes..

DirtyDiesel - October 19, 2018, 3:29 pm

(Oct 19, 2018 03:04 PM)Zajbu Wrote: [\[CITE\]](#) Lol, lovely lovely yes..
Spam post, seems like alot of those around here.

SecureOp - October 29, 2018, 5:15 am

Let's give education a bump.

JacktheRipperRN - November 3, 2018, 5:52 am

This is a great piece of information :)

Thanks for sharing :D

Minisaints - November 4, 2018, 3:58 pm

Ever thought to include Brave?

SecureOp - November 4, 2018, 4:41 pm

(Nov 4, 2018 04:58 PM)Minisaints Wrote: [\[CITE\]](#) Ever thought to include Brave?
I've been meaning to give it a try as heard it's name here and there. It's also implemented with BAT tech which is intriguing.

Hetepheres - January 8, 2019, 2:00 pm

Well, all I can say is thank you. This is a very detailed thread about how to protect your browser, and to be honest, before of finding this, I was using portable Google Chrome in order to get rid of the cookies. Thanks, once again!

TerenceMcKenna - January 9, 2019, 12:30 am

Really useful information. I worry that the add on "Chameleon" spoofing the IP and different browser every minute may flag my HF account. I guess time will tell.

SecureOp - June 15, 2019, 11:37 am

Worth a bump for some spark.

sarapapa - June 17, 2019, 10:58 pm

thanks man i really appreciate this you have been of great help^^

Zan - June 17, 2019, 11:22 pm

This was really helpful! Thanks for posting! This should be sticky. ?

Criminal - June 17, 2019, 11:26 pm

thank you thank you so much!

laf3r - June 19, 2019, 5:32 am

Thanks for the detailed tutorial.

Check The Name - June 23, 2019, 1:33 am

Nice thread, thank you for the share.

Magictabz - July 28, 2019, 9:49 am

i cant find network.http.sendSecureXSiteReferrer is it just me or?

SecureOp - August 2, 2020, 1:22 pm

Just came back to use this thread - maybe useful for someone else and their opsec ?

SIM-4391894 - August 2, 2020, 2:46 pm

Thanks for this thread, learned something new here :) i didn't that we need to change many options in about:config, i only used media.peer and navigation.

mindshift5 - September 25, 2020, 11:11 pm

Oh man. Thanks a lot ...I really appreciate the info

Stray - September 30, 2020, 9:42 pm

Does this still work?? Sounds interesting.

Fluox - October 1, 2020, 2:17 am

This is a pretty useful guide; thanks for the information. :)

pipito - October 1, 2020, 11:24 am

Excellent information, I agree that you should pin this thread on the forum. Everything is very well explained, I like to find useful contributions like this. Thank you very much for sharing friend.