Getting past that ever annoying ‘turn your ad block off to use this site’ crap and MORE!!

Nothing is 100% secure Nothing is 100% private. But you can mitigate the risk

.

Hello, You have came across this document due to my rants on Reddit or Twitter. This text will help you take control of your interneting experience completely and unashamedly. The first part addresses ad blocking fixes, and the second privacy fixes.

If you do not want to take about 30 minutes to take control of the internet and stop it from invading your privacy, then either get lost, or bookmark this site for later, because this document is filled with **A LOT** of information, facts, and evidences, to support my claims/views!! Experienced uBlock Origin users can skip Adblocking 101 and go straight to page 2! **Ad Block Wall** problems are also addressed on page 2. **Do know this a dynamic document and is always changing/being tweaked, so be sure to check back**. Currently I am changing a lot of things in the Script-Blocking and Crypto-Mining section with up to date news/info. And at the end, I list ‘my setup’ that totally kicks ass adblocking and privacy wise.

ALSO….Be aware of websites starting to hijack users to farm crypto coin without them knowing/giving permission. They are popping up on sites left and right, and filter lists can’t keep up with them. More on this in Crypto-Mining section. **https://thepiratebay.org/ is/was mining using your CPU again. BLOCK ALL SCRIPTS ON THE SITE**

ADBLOCKING 101

You want to be using uBlock Origin, not AdBlock, Not AdBlock Plus, Not AdBlock Pro, not plain old uBlock. Here is why.   uBlock Origin does more than block ads, it also blocks scripts all through a simple easy mouse-click interface. When used with Privacy Badger it is the BEST way to keep you private and safe from trackers and ads! It also works faster using far less system resources **AND** you don’t have to mess with manual filter syntax crap in the ‘my filters’ tab like with AB or ABP. You can do it all via POINT and CLICK with your mouse.

https://i.imgur.com/VHTFqVp.png https://i.imgur.com/I57ZnM4.png   THESE ARE THE FILTER LISTS I USE BE SURE YOU ARE USING THESE

You have mentioned your ad blocker no longer blocks ads on ‘insert site here’
Welcome to the world of Dynamic Ad Blocking. This means you can no longer, just sit back, and relax and expect the computer to do the work’
Here is my tips to block ads on ‘insert site here’ *NOTE* To block ads on Twitch, you need Twitch5
Scan your computer for Adware!! https://www.malwarebytes.com/adwcleaner/
Set your uBlock Origin to these settings This will fix 95% of your problems
https://github.com/gorhill/uBlock/wiki/Blocking-mode:-medium-mode
Make your filters the same as mine https://i.imgur.com/N7iV8CB.png
This will fix 95% of your problems
NOW, you also want to read https://github.com/gorhill/uBlock/wiki/Dynamic-filtering:-quick-guide and learn what dynamic blocking entails.
Here is my suggestion. You will see the importance of doing this in just a bit.
In addition to the filter list settings in medium mode, block all 3rd party scripts and frames GLOBALLY. If you run into a site not working, you can change the settings LOCALLY for that site, that will override the global settings, and you can SAVE the settings for that particular site.

Why do all this, you ask?

- Web pages will load significantly faster
- Your privacy exposure will be significantly reduced.
- **You no longer depend mostly on 3rd-party filter lists to dictate what is blocked or not.**
  - The static filter lists are still used to mop up whatever network requests is not blocked in this mode -- so double protection.
- High likelihood of web pages being broken: you have to be ready and willing to fix them when this happen.
  - Keep in mind though that as you build your ruleset for the sites you usually visit, you will spend less and less time fixing web pages.

ADBLOCK WALLS

Getting around ad block walls:
There are two solutions.
https://jspenguin2017.github.io/uBlockProtector/
This is designed exclusively for Chrome and uBlock Origin
and
https://adblockprotector2.github.io/AdBlockProtector2/
Which is designed for Firefox Quantum and everything else

Adblocker2 is brand new and in development, as to the release of FireFox Quantum
So pay attention to that page ***but DO be aware, of this….***

"ABR2 is an experiment, just like AAK-Cont and unlike uBR, I will not be using it myself, and I'll be honest with you, I probably won't care too much if it is slow or it break. Sure I want it to be shiny and fast, but that's easier said than done, pretty much everything else in my life will have higher priority than fixing ABR2. If there is a bug that affect only one website for one browser that's not Chrome, be ready to wait months before it gets resolved."

No help/ideas is offered for AdBlock or AdBlock Plus, so if you 'insist' on using them, you are making a bad choice.

.

Now is when you tell me Chrome tracks you, and all that other wonderful stuff

Actually every website practically uses Google-Analytics. Which allows Google to track your IP, time spent on the site, your physical location, and they store it and match it to other sites you visit. The same thing happens when you use other browsers too!. More on this in the PRIVACY section. So perhaps Firefox is more private than Chrome, until you visit a web page.

This point and beyond, if you use Disconnect, or Ghostery, get rid of them. They are useless as they use filter 'lists' and offer no real time protection compared to **DYNAMIC** ad and script blocking!

SCRIPT BLOCKING / CRYPTO-MINING

"Since September 19, the second most frequently blocked website for our customers has been http://coinhive.com " - @Malwarebytes

https://blog.adguard.com/en/crypto-mining-fever/
https://www.bleepingcomputer.com/news/security/the-internet-is-ripe-with-in-browser-miners-and-its-getting-worse-each-day/

If you are not yet scared from these two articles, you either did not read them, or should not be using a computer. Blocking 3rd party scripts **globally** and allowing them **locally** on a PER SITE basis is a **MUST** now. If you are unable or unwilling to globally block scripts as a preventative measure, then you are just wasting your, and my time reading this. Mainstream websites are now being hacked and 'loaded' with mining code. You **ABSOLUTELY** must know and recognize 'bad' websites that are trying to load script onto your browser!

https://twitter.com/bad_packets **READ THIS EVERY DAY!!!** You will be knowledgeable in no time!

So by now you have uBlock Origin in medium mode, and you know how to globally block 1st and 3rd party scripts.
http://prntscr.com/gnhxdt is what your uBo menu should look like roughly with GLOBAL settings on the left side, and LOCAL settings on the right. Yes you will need to 'play with the settings' on some sites to get it to work. But the settings are saved. But if you're wondering how to 'block every damned thing possible' except for the bare minimum to make a website run, you need **uMatrix**, This comes later.

https://www.bleepingcomputer.com/news/security/coinhive-is-rapidly-becoming-a-favorite-tool-among-malware-devs/
https://www.bleepingcomputer.com/news/security/showtime-websites-used-to-mine-monero-unclear-if-hack-or-an-experiment/
http://www.theregister.co.uk/2017/10/13/politifact_mining_cryptocurrency/
BLOCK ALL SCRIPTS GLOBALLY AND ALLOW ON A AS NEEDED BASIS
The new thing will be not to bring websites down, but to keep them up, filled with bad code!

https://twitter.com/bad_packets BOOKMARK THIS GUY!! He seems to be up to the minute on hacked websites.
Follow this hashtag. #cryptojacking
Test your antivirus.
Disable ad blocking, Enable all scripts
https://www.2giga.link/
https://ppoi.org/
If your anti-virus goes off. Consider yourself sorta safe and you can breath a bitl. If not…
You have choices. **GET AVAST!!** It seems to catch most of them, but it is not 100%. Check out

a> get a few anti coin mining extension. They are not 100% I tested a few for Chrome, and out of five sites tested, they all missed at least two. I have two running now AntiMinerand MinerBlock. NoCoin sucks royally

b> another tool to help you see what's going on- NOT AS GOOD AS the F12 button!!
https://chrome.google.com/webstore/detail/quick-source-viewer/cfmcghennfbpmhemnnfjhkdmnbidpanb

I don't know the equivalent for FireFox. This quickly shows you what 1st party scripts are used on any questionable site. It should take you a minute or two at most to see a script called 'coin' or 'mine' or 'hive' that will tip you off! It takes practice.Explore those 2 sites above with all scripts blocked. Load the quick source viewer extension… Learn. Grow. Email me if you have questions!!!

USE THIS SITE

https://censys.io/domain?q=coinhive.min.js
https://censys.io/domain?q=authedmine.min.js
https://censys.io/domain?q=miner.min.js

IF you are starting to put 2 and 2 together, congratulations. If not. I am telling you how to find sites that use 'such and such' miner. Based on its min.js name!!

Many sites quickly remove the mining when they 'get caught' Most sites tend to be less popular streaming sites. But there will always be attempts at hacking big name websites and sneaking stuff in.

PRIVACY & STILL MAINTAINING FUNCTIONALITY!

Short sweet and to the point. Works for all browsers

1) You need to get a VPN. No way around it. You have to be able to change IP's. See next section.
2) Install Privacy Badger! And actually monitor it, and change settings on those websites you are wary of
3) https://panopticlick.eff.org/ Run this test, you will need to disable your ad blocker. Click show full results for fingerprinting. Look at the '**one in *x*browsers have this value'** This is how websites track you and are able to keep tracking you over time! Notice the Canvas Hash, and User Agent high numbers and Fonts, and WebGL?
4) https://browserprint.info/ Run this test too. Notice at the bottom AUDIO fingerprinting. Read this. https://thehackernews.com/2016/05/audio-fingerprint.html and https://www.bestvpn.com/privacy-news/audio-battery-fingerprinting/
5) For User Agent. There is a switcher that can be installed for either browser. Merely look for 'user agent switcher'. Yes it can affect how websites are displayed so be careful.
6) Install a Referer Control. This prevents websites from tracking what website you just came from before.
7) Install HTTPS Everywhere
8) Script blocking **If you are using uBlock Origin READ**: https://github.com/gorhill/uBlock/wiki/Blocking-mode:-medium-mode Only use Scripts on sites that you trust, or have a need to turn it on. **AS A STANDARD** I BLOCK ALL 1ST PARTY AND 3RD PARTY SCRIPTS unless it's needed to make a site I trust run.

Blocking 1st and 3rd party scripts, but allowing inline scripts to run on sites you trust, Is a good base to start with on uBlock Origin. Run those 2 browser privacy tests again and see how the #'s have changed!. Now, do remember. You may get high numbers for User Agent if you are using a new browser version because their #'s are based on previous user tests.

If a site doesn't work, you will need to change local script settings, but you should rarely have to allow 3rd party scripts.

Nothing is 100% secure Nothing is 100% private.
You can however lower your risk while still maintaining USABILITY!!

HOW TO OBTAIN AND RETAIN FINE CONTROL OVER THE INTERNET USING uMATRIX

This is for the smaller niche of users who want ABSOLUTE control of their browser for ad blocking and privacy. It is fun,effective and you learn **A LOT** about how websites work and works for both Chrome and Firefox

You go from this
https://i.imgur.com/HuXDQip.png
To this
https://i.imgur.com/p9y2EsF.png

Notice the **control** you now have!! You go from wide spectrum 3rd party blocking to controlling exactly what gets let through, and what gets blocked out, you also see what is trying to put 'stuff' on the website you are trying to view.
http://adamantine.me/index.php/2015/11/18/umatrix-desperately-needed-guide/

My brief how to guide: Before anything, Click on the settings button on the top left, and disable all those filter hosts files.   This leaves the adblocking to uBlock Origin and uMatrix will handle the rest. Go to a website, and click the umatrix icon. Click the blue button till it goes black and then back to blue. Blue is **LOCAL** rules for that site… Black is **GLOBAL** rules.
https://i.imgur.com/0ix9vaI.png is what I suggest for first time users to use as global rules. Once set, click the button to blue. Now go to a site you frequent, perferablly one requiring a login. You first want to enable 1st party scripts. Reload the site, try to sign in. NOW   click the **PADLOCK BUTTON** to save changes for that site!!   Also in settings, block referers, and use 4-5 of the top from this list to put in as your user agent settings https://techblog.willshouse.com/2012/01/03/most-common-user-agents/
Use my settings as a guide.   https://i.imgur.com/9S9Bwez.png
Thats it!!! Now go, and **LEARN.** If you need any more help, e-mail me!

VPN's

Yes you should be using one, and no, not a free one, and no don't use the app store to find one. To keep it simple and easy as possible for the 'everyday user'

Here is a small list of vpns I recommend
ExpressVPN
IVPN
Private Internet Access
AirVPN
DO NOT USE WINDSCRIBE
DO NOT USE PureVPN
https://vpnleaks.com/ **LIST OF VPNS TO NEVER CONSIDER**

TOR

Tor is useless, pure and simple, and here is proof. JavaScript is enabled for this test on both browsers. All Tor does is make your browser settings the same as everyone elses that uses it. So your are EASILY identified as 'clone' Tor user and quite often banned from many websites as such. https://i.imgur.com/jnARBtK.png is my results using Chrome from https://panopticlick.eff.org Notice the 'high results' for Canvas and WebGL?? That is fingerprint spoofing to PREVENT websites from TRACKING me over time. Here is my results using the TOR browser with that same testing site. https://i.imgur.com/Oo78PtL.png Notice how comparable the numbers are?? And also note, that my Chrome browser uses User Agent Spoofing rotating between 4 relatively new Browsers. NOTE: ALL Browser fingerprint tests are BASED on its collective results from PREVIOUS tests. The ONLY thing that ANYONE can question about my setup is my Browser Plug in Details. But. I rotate IP's regularly. So my Chrome browser, is fully functional as I see fit, and I have made it so I can not be tracked across IP's UNLESS I use a website that I sign in to. I am happy with that. That output makes TOR useless indeed My results tell the website one thing, and one thing only. I in fact know what I am doing to maintain my privacy. All Tor is, is a slow free vpn for those that say paid VPN's are bad. I end it with this proverb: "You get what you pay for"

MY SETUP and why

Do Realize Privacy Badger has 'issues'
It doesn't like to work with other extensions thinking it's the 'only kid on the block' so It has occasional 'conflicts because it wants to be the extension to 'do something' but i have it delegated to another extension.' with my uMatrix and ScriptSafe, But i've tested stuff. It works fine.

Chrome *latest version*
VPN- TorGuard I use the OpenVPN GUI, not their crappy house built app.
uBlock Origin set to easy mode
uMatrix

I have uBlock set up to block only 'filter list' stuff. uMatrix handles EVERYTHING else including **SCRIPTS**//css/cookies/xhr/frames It is 'hardcore' but the BEST way to maintain privacy for **ADVANCED** users,. It also blocks referrers and does user agent spoof. Just turn off 'hosts file' so that way uBo alone does the filter blocking.
http://adamantine.me/index.php/2015/11/18/umatrix-desperately-needed-guide/
Is a brief primer for uMatrix

uBlock Protector
Privacy Badger

I am getting some 'errors' conflicting this with uMatrix, nothing to worry about. Privacy Badger was programmed to spoof referers for everything it 'blocks' I have asked them if there is a way to disable it. I don't think there is. There seems to be no 'problems' though Umatrix spoofs all the referrers, while Privacy Badger just blocks the one it's marked to 'ignore'

Click&Clean

HTTPS Everywhere

Scriptsafe

Now I use this to block **FINGERPRINTING** attempts. And I allow all scripts through to be handled by uMatrix. Takes some time to tinker with it in order for it to do just the fingerprinting and not clash with uBo,, BUT WELL WORTH IT!!. You may want to DISABLE the clipboard interference option. Email me if you need help. This extension does cause problems with some video heavy sites… like Twitch, but not Youtube.

Disable HTML5 Auto Play

Use this until Chrome integrates it in January

uBo-Scope Just gives you an idea of how your internetting behaviors connects to various 3rd party systems.

If you have ANY questions I have not answered, PLEASE email me!

Eddiejf321@gmail.com!

Stay safe, and remember, it is YOUR internet. YOU control it, not vice-versa!

Eddie!