Lista para la protección de datos

o

Manual de resistencia al capitalismo de vigilancia

Valentin Delacour

2016 - 2020

Índice

1. Introducción

Este documento tiene como objetivo principal proponer herramientas y alternativas para proteger los datos y la privacidad de la predación de empresas privadas bajo el sistema actual de capitalismo de vigilancia. Ahora bien, seguir las siguientes recomendaciones permite también mejorar, en ciertas medidas, la protección contra otras entes tales como servicios de Estados o piratas, por ejemplo.

Esta lista se destina a todas las personas conscientes o tomando consciencia de la importancia de la protección de datos en nuestra sociedad, independientemente de sus conocimientos del tema. No se destina a las personas necesitando un anonimato total de parte de su función a riesgos tales como opositores políticos o algunos periodistas, aún si algunas opciones propuestas podrían convenirles. Efectivamente, la privacidad no necesariamente es igual al anonimato.

El formato de lista fue escogido con el afán de hacer su consulta lo más eficiente posible. Este enfoque impide detallar verdaderas explicaciones. Así que les invito a buscar las que les sean necesarias por sí mismos o en los recursos adicionales mencionados en el punto 6 del documento. Teniendo el propósito de proponer las opciones más reputadas y prácticas sin estar demasiado cargada, la lista no tiene por vocación ser exhaustiva y permanece subjetiva a pesar de buscar tener la mayor objetividad posible.

Esta lista propone una primera priorización (orden de aparición y presencia o no de paréntesis) subjetiva basada en el reporte privacidad/usabilidad con el fin de ayudarles a escoger entre las diferentes opciones citadas. Una segunda priorización (colores) se basa unicamente en la privacidad estimada : verde (verdadero respeto de la privacidad), azul (respeto de la privacidad bajo condiciones o presencia de un elemento problemático), rojo (no garantiza el respeto de la privacidad pero sigue siendo preferible a las opciones de los GAFAM) e incoloro (falta de elementos para formar una estimación, o una priorización no es pertinente para la entrada en cuestión). La presencia de un asterisco indica que la opción mencionada sigue en fase de desarrollo.

Espero que este documento les servirá para mejorar la protección de sus datos personales y de los de sus cercanos. Aunque siendo el fruto de varios años de búsquedas y experimentos, este trabajo permanece obviamente perfectible. Cualquier sugerencia o comentario es entonces más que bienvenido a mi correo personal : valentin.delacour@protonmail.com. Varios meses después de la presente versión del documento, se debe asumir que varias informaciones dadas serán obsoletas. El documento siendo actualizado frecuentemente, están invitados a solicitar la ultima versión.

2. Reglas de oro

- Evitar usar servicios y programas de los GAFAM (Google, Amazon, Facebook, Apple y Microsoft) SIEMPRE que sea posible. Lo más recomendable es eliminar sus eventuales cuentas.

- Siempre revisar todos los ajustes de lo que se utiliza y optimizarlos para limitar al máximo la recolección de datos personales.

- Solo instalar los programas/aplicaciones necesarios pues son accesos potenciales a sus datos personales.

- Usar programas libres/open source (sus códigos son públicos y así mismo verificables) en vez de los propietarios/closed source siempre que es posible.

- Favorecer las opciones libres populares a las desconocidas (serán más revisadas/confiables).

- Si una empresa propone sus servicios gratuitamente, en general, el producto que vende es usted (sus datos personales). Por causa del modelo impuesto por el capitalismo de vigilancia, pagar ya ni les protege de también ser el producto.

- Actualizar sus programas/sistemas operativos frecuentemente para beneficiar de los últimos correctivos de fallas de seguridad explotables y pensar en reemplazar los que ya no parecen ser actualizados.

- No usar antivirus terceros, son verdaderas aspiradoras de datos personales. Su aporte es desdeñable con tal de que se mantengan buenas costumbres numéricas. La prudencia y una buena configuración son los mejores antivirus.

- Privilegiar Web Apps o atajos desde el navegador para acceder a servicios en vez de aplicaciones a instalar para limitar el acceso y las posibilidades de recolección de datos personales.

- Utilizar correos temporales para crear cuentas para sitios/servicios poco importantes.

- Siempre desactivar el Wi-Fi, Bluetooth y geolocalización de su smartphone cuando no están usados y no conectarse a Wi-Fi públicos sin el uso de un VPN.

- No usar objetos conectados (su propósito es recolectar la mayor cantidad posible de datos personales) o no conectarlos a internet cuando son imprescindibles.

3. Computadora

3.1 Sistemas operativos

Windows es actualmente el peor sistema operativo en términos de privacidad y de seguridad. Los únicos SO fáciles de uso y protegiendo realmente los datos son las distribuciones libres (por lo tanto gratuitas) de Linux. Existe una multitud de ellas cuyas características varían considerablemente. Aquí una pequeña selección de las ofreciendo la mejor experiencia para el usuario (siempre respetando la privacidad) o garantizando la mayor protección de datos.
Cabe recordar que cada una de ellas propone una o varias interfaces (entornos de escritorio) diferentes en términos de experiencia, de consumo de recursos y de apariencia. Existe una documentación abundante en linea para escoger cual distribución y entorno de escritorio convendrán mejor a las capacidades de su computadora y a sus preferencias así como para saber como instalarla fácilmente en su computadora.

Desktop :
Linux Mint : ideal para principiantes
MX Linux (cf. 7.1) : conviene a los principiantes
(Solus) : conviene a los principiantes
((Parrot Home)) : seguridad y privacidad mejoradas (usuarios confirmados)
((Qubes OS)) : seguridad extrema (usuarios avanzados)
((Whonix)) : anonimato por Tor y seguridad extrema (usuarios avanzados)

USB live (RAM) :
MX Linux : conviene a los principiantes
Tails : anonimato por Tor (usuarios confirmados)
(Parrot Home) : seguridad y privacidad mejoradas (usuarios confirmados)

Raspberry Pi :
Plasma BigScreen* : centro multimedia para TV (comando de voz con Mycroft AI)
Raspberry Pi OS : sistema operativo clásico
LibreELEC : centro multimedia para TV
Batocera : emulador de consolas, retrogaming
(RetroPie) : emulador de consolas, retrogaming

3.2 Servicios y programas

Navegador : Firefox(cf. 3.3), Tor Browser, (LibreWolf*), ((Iridium Browser, Brave)).
Buscador : Qwant, (DuckDuckGo, searx.me), ((Startpage(proxy Google))).
Ofimática : LibreOffice, (CryptPad, Onlyoffice).
Correo : Protonmail, Tutanota, Posteo.
Plataforma vídeo : Invidious(proxy Youtube), PeerTube, FreeTube(cliente Youtube).
Mensajería instantánea : Signal, Telegram, Element, (Session*).
Videollamadas/videoconferencia(cf. 3.4) : Jitsi Meet, BigBlueButton, Jami, Element.
Red social : Mastodon, Friendica, Diaspora, PixelFed, Nitter(proxy Twitter), Bibliogram(proxy Instagram).
Traductor : DeepL, (Bergamot Project*).
Mapas : OpenStreetMap, Maps.me, Qwant Maps*.
Compartición de archivos : upload.disroot.org, swisstransfer.com, OnionShare.
Colaboración : CryptPad
Administrador de contraseñas : Bitwarden, KeePassXC.
VPN : IVPN, Mullvad, (ProtonVPN), ((Firefox VPN*)).
Cloud : Disroot(Nextcloud), Cozy Cloud, Nextcloud, Kdrive(Infomaniak).
Correo temporal : temp-mail.org, guerrillamail.com, maildrop.cc.
Limpieza y optimización de sistema : Stacer, BleachBit.
Edición de imágenes y dibujo : Gimp/Drawing, Krita, Darktable/RawTherapee.
Edición gráfica vectorial : Inkscape
Maquetación de páginas : Scribus
Edición audio : Audacity
Edición video : OpenShot, Kdenlive, (Avidemux, Pitivi, Cinelerra).
Supresión de metadatos : ExifCleaner
Herramienta de cifrado : VeraCrypt, Cryptomator.
Análisis de trafico de red : Wireshark

3.3 Firefox

Para que Firefox realmente proteja la privacidad, es necesario configurarlo de manera adecuada (ajustes, extensiones y about:config). Todas las configuraciones necesarias están desarrolladas en el punto 7.4 del documento. Estos ajustes también valen, en una cierta medida, para la versión móvil. Puesto que las configuraciones dadas son relativamente restrictivas, es recomendado tener un navegador secundario configurado de manera menos restrictiva para acceder a los sitios problemáticos (Firefox ESR u otro navegador recomendado en la lista son ideales para cumplir este papel). Usar otro perfil del mismo Firefox igualmente es una posibilidad recomendada.

Extensiones :
Lista completa : uBlock Origin, uMatrix, Decentraleyes, HTTPS Everywhere, Chameleon, CanvasBlocker, Cookie AutoDelete, ClearURLs, Invidition, (Privacy Badger).

Lista ligera : uBlock Origin, Decentraleyes, HTTPS Everywhere, Cookie AutoDelete.

Configuraciones de la extensiones detalladas en el punto 7.4

3.4 Instancias de videoconferencia

El interés de recomendar varias instancias diferentes para Jitsi Meet es de poder cambiar si una de ellas esta sobrecargada o funciona mal. Es recomendado probarlas siguiendo el orden establecido.

Jitsi Meet :
Framasoft : https://framatalk.org/accueil/es/
Snopyta : https://talk.snopyta.org/
FDN : https://talk.fdn.fr/
/e/ : https://visio.ecloud.global/
Infomaniak : https://meet.infomaniak.com/
Jitsi : https://jitsi.org/jitsi-meet/

BigBlueButton :
FDN : https://bbb.fdn.fr/b

4. Smartphone

4.1 Sistemas operativos

Android modificado para la privacidad :
/e/OS : Lineage OS degooglizado pero con microG y servicios integrados (cuenta /e/)
CalyxOS : Android degooglizado y seguro con microG para una mejor compatibilidad
GrapheneOS : el Android más privado, degooglizado y seguro disponible
(Volla OS*) : Android sin Google apps
(Lineage OS) : Android sin Google apps pero no totalmente degooglizado

Linux :
UBports
Postmarket OS*
Manjaro*
PureOS*
(Sailfish OS Jolla)

Las opciones basadas en Linux, en su estado de desarrollo actual, todavía no son recomendables para usuarios promedios (a excepción de Sailfish OS).

4.2 Hardware

Fairphone 3 : /e/OS (solo disponible en el sitio del proyecto /e/)
Volla Phone* (salida noviembre 2020) : Volla OS, UBports, Sailfish OS y otros
(Librem 5*) : PureOS y otros OS basados en Linux
(PinePhone) : UBports y otros OS basados en Linux

Otros modelos con /e/OS preinstalado están disponibles en el sitio del proyecto /e/ : https://esolutions.shop/

Si no desean instalar o comprar un smartphone con un sistema operativo respetuoso (grave error), recuerden que se debe evitar absolutamente todas las marcas chinas así como Samsung y que iOS (Apple), a pesar de limitar sus usuarios, explota menos los datos personales que Android por defecto y ofrece más protecciones.

4.3 Aplicaciones

Las aplicaciones propuestas para Android y derivados deben ser buscadas primero en la tienda de aplicaciones libres F-Droid (garantía que no tengan rastreadores terceros) y si no están, luego en Aurora Store.

Android y derivados :
Tienda de aplicaciones : F-Droid(cf. 7.2), Aurora Store(proxy Play Store), (Apk mirror).
Navegador : Fennec(Firefox)(cf. 7.4), Bromite(cf. 7.2), Tor Browser, (Privacy Browser).
Mensajería instantánea : Signal(cf. 7.2), Telegram, Element, (Session*, Briar).
Videollamadas/videoconferencia : Jitsi Meet, Signal, Element, Jami, Telegram.
Cliente Youtube : Newpipe, (Skytube).
Teclado : AnySoftKeyboard, OpenBoard.
Mapas/navegación GPS : Maps(OpenStreetMap), OsmAnd, Magic Earth.
Bloqueador de publicidad/rastreadores : Blokada(cf. 7.3), (Nebulo).
Web Apps : WebApps
Redirector de contenido Youtube, Twitter, Instagram y Google Map : UntrackMe
Autentificación a dos factores : Aegis, andOTP.
Cliente Mastodon, Friendica, Peertube y PixelFed : Fedilab
Cliente respetuoso Facebook/Twitter/Instagram : Frost/Twidere/InstaGrabber.
Agenda : Simple Calendar, Etar.
Notas : Joplin, Nextcloud Notes, (Simple Notes, Standard Notes).
Galería : Simple Gallery
PDF : PDF Viewer Plus, (MuPDF Viewer).
Contactos : Open Contacts, Simple Contacts.
Cámara : Open Camera, (Simple Camera).
Supresión de metadatos : ImagePipe, Scrambled Exif.
Revelador de rastreadores terceros : ClassyShark3xodus, Exodus privacy.
Simulador de localización : Private location
(Reemplazo de Google Services : MicroG GmsCore)
(Gestor de privacidad : XprivacyLua, App Manager.)
(Aislador red de aplicaciones : NetGuard)

IOS :
Navegador : Firefox(cf. 7.4), Onion Browser, (Brave).
Mensajería instantánea : Signal, Telegram, Element, (Session*).
Videollamadas/videoconferencia : Jitsi Meet, Signal, Element, Jami, Telegram.
Bloqueador publicidad/rastreadores : Blokada(cf. 7.3), (DNSCloak), ((Better Blocker)).

5. DNS

5.1 Transcontinental

Con protección :
NixNet (DoH, DoT)
(Adguard) (DoH, DoT, DNSCrypt)
((NextDNS)) (DoH, DoT, DNSCrypt)

Sin filtros :
DNSWatch (no cifrado)
UncensoredDNS (DoT)

NixNet :
DoH : https://adblock.any.dns.nixnet.xyz/dns-query
IPv4 : 198.251.90.89, 198.251.90.114

DNS.Watch :
IPv4 : 84.200.69.80, 84.200.70.40
IPv6 : 2001:1608:10:25::1c04:b12f, 2001:1608:10:25::9249:d69b

5.2 Europa

Con protección :
BlahDNS (DoH, DoT, DNSCrypt)
LibreDNS (DoH, DoT)

Sin filtros :
Snopyta (DoH, DoT)
PowerDNS (DoH)
FDN (no cifrado)

BlahDNS DoH : https://doh-de.blahdns.com/dns-query
LibreDNS DoH : https://doh.libredns.gr/ads

6. Recursos adicionales (fuentes)

Los recursos adicionales también actúan, en una cierta medida, como fuentes para el presente documento.

General

Excelente libro para comprender el capitalismo de vigilancia y sus amenazas :
La era del capitalismo de vigilancia, Shoshana Zuboff

Tutoriales fáciles para la privacidad :
https://spreadprivacy.com/tag/device-privacy-tips/

Excelentes cadenas acerca de la privacidad (con tutoriales) :
https://www.youtube.com/channel/UCjr2bPAyPV7t35MvcgT3W8Q
https://www.youtube.com/channel/UCs6KfncB4OV6Vug4o_bzijg

Asociaciones para la defensa de la privacidad (informaciones) :
https://www.laquadrature.net/es/
https://www.eff.org/deeplinks

Asociaciones proponiendo excelentes servicios respetuosos de la privacidad :
https://disroot.org/es/
https://framasoft.org/en/
https://snopyta.org/
https://www.drycat.fr/en

Buenas costumbres de protección de datos :
https://www.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide

Excelente sitio listando servicios y programas respetuosos :
https://www.privacytools.io/

Operadores recomendables :
https://www.eff.org/pages/quien-defiende-tus-datos

Grupos y canales Telegram

Privacidad, protección de datos y más :
t.me/privacid
t.me/techloregroup
t.me/techloreofficial
t.me/NoGoolag

Linux y libre :
t.me/grupo_telegram_proyectotictac
t.me/LinuxMintEs
t.me/mxantixes

Sistemas operativos

MX Linux :
https://mxlinux.org/

Linux Mint :
https://linuxmint.com/

/e/ OS (Android respetuoso de la privacidad):
https://e.foundation/

Firefox

Configuración Firefox :
https://www.youtube.com/watch?v=tQhWdsFMc24

Configuración Firefox básica :
https://12bytes.org/articles/tech/firefox/the-firefox-privacy-guide-for-dummies

Configuración Firefox avanzada :
https://12bytes.org/articles/tech/firefox/firefoxgecko-configuration-guide-for-privacy-and-performance-buffs

7. Configuraciones

7.1 MX Linux

Plugin Flash :
Entrar el comando siguiente en la terminal para eliminar el plugin Flash propietario : sudo apt purge --remove adobe-flashplugin flashplugin-installer pepperflashplugin-nonfree

Solo si el plugin Flash es necesario para su navegación internet, entrar el comando siguiente para instalar una versión libre : sudo apt install browser-plugin-freshplayer-pepperflash

Configuración Wi-Fi :
Clic derecho en el icono Wi-Fi, modificar las conexiones, seleccionar el Wi-Fi activo, bajo Wi-Fi seleccionar Dirección MAC clonada : Aleatoria.
Bajo ajustes IPv6, seleccionar Extensiones de confidencialidad IPv6 : Activado (dirección temporal preferida).

7.2 F-Droid

Para poder encontrar y descargar algunas aplicaciones desde F-Droid, es necesario agregar sus repositorios. Para esto, ir a los ajustes de F-Droid, luego bajo "repositorios", activar el repositorio "Guardian Project" y por fin presionar el "+" y entrar las direcciones mencionadas deseadas.

Bromite : https://fdroid.bromite.org/fdroid/repo

Langis (versión modificada de Signal a utilizar si las notificaciones no llegan con la versión clásica de Signal) :
https://gitlab.com/TheCapsLock/fdroid-patched-apps/raw/master/fdroid/repo

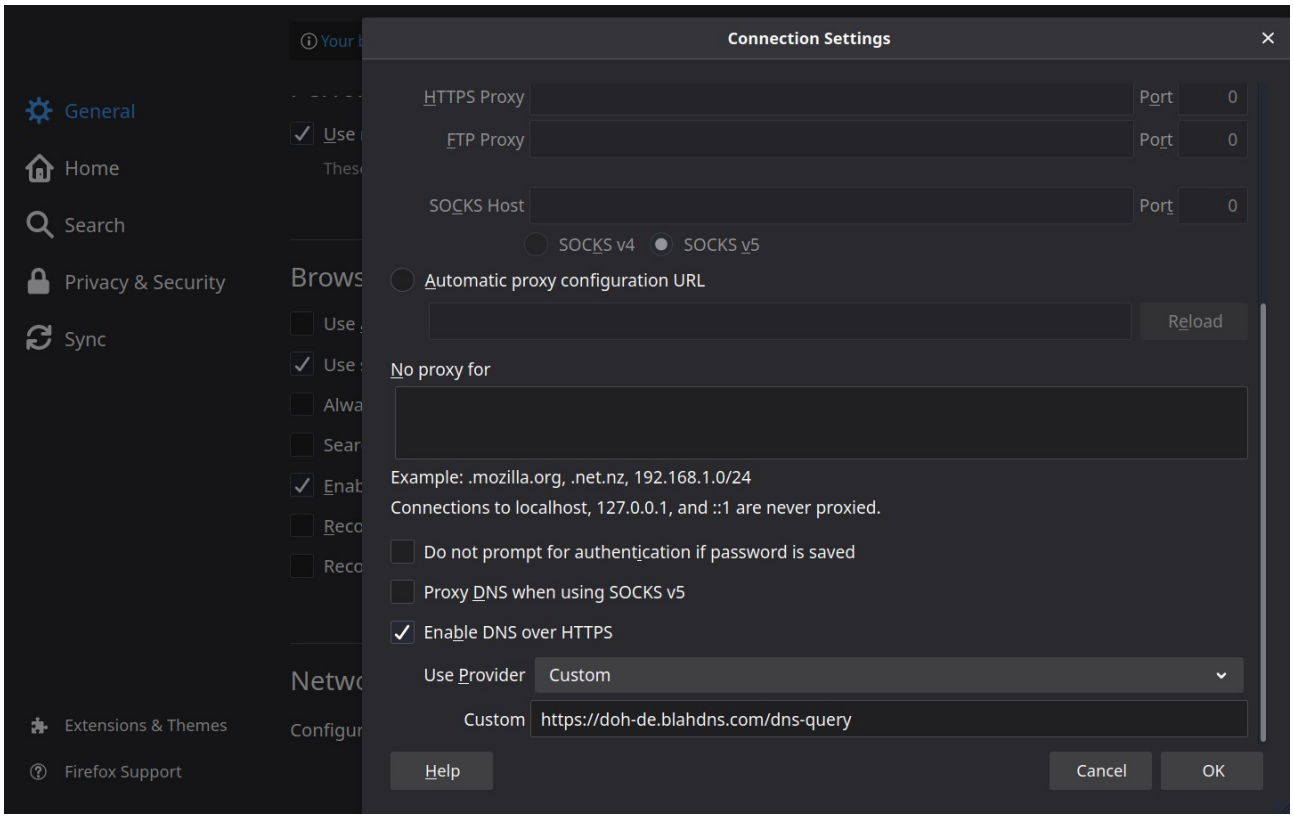
7.3 Blokada

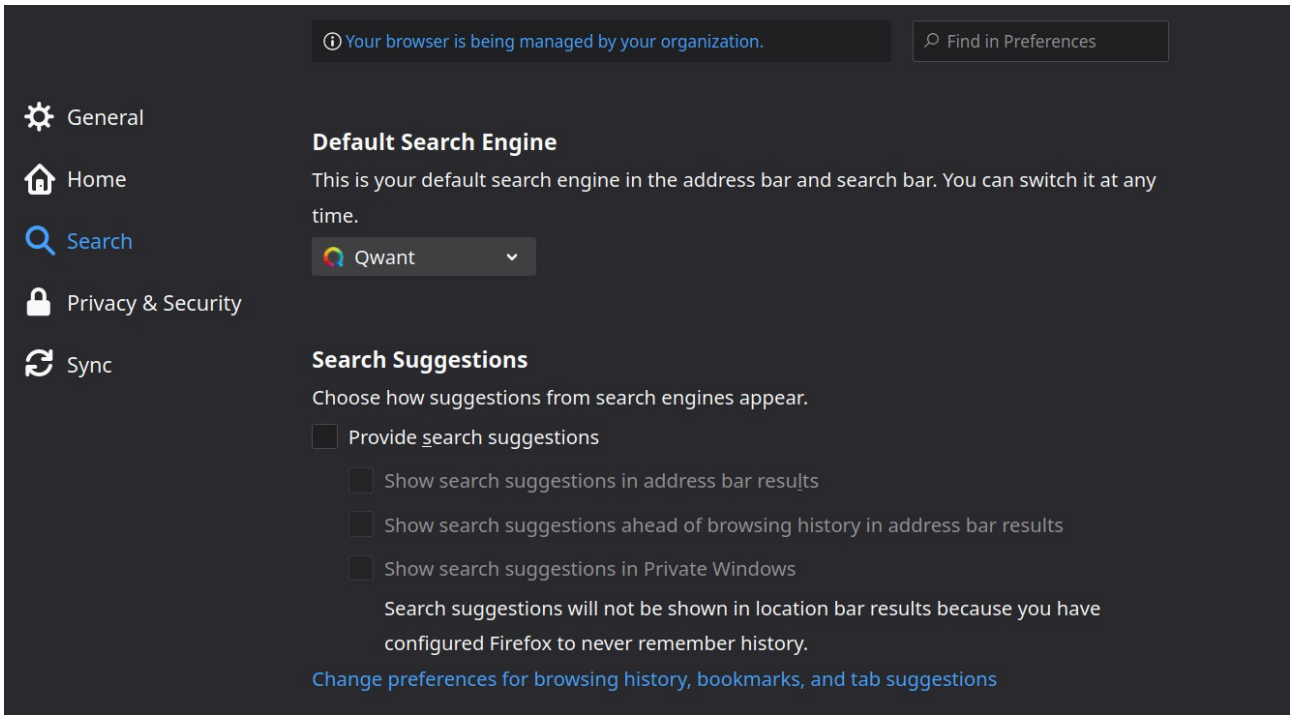
Blocklists :
- Energized : Basic (o Blu si memoria RAM inferior a 4gb)
- DuckDuckGo Tracker Radar
- (Goodbye Ads : Samsung o Xiaomi (solo sirven para los modelos de esas marcas))

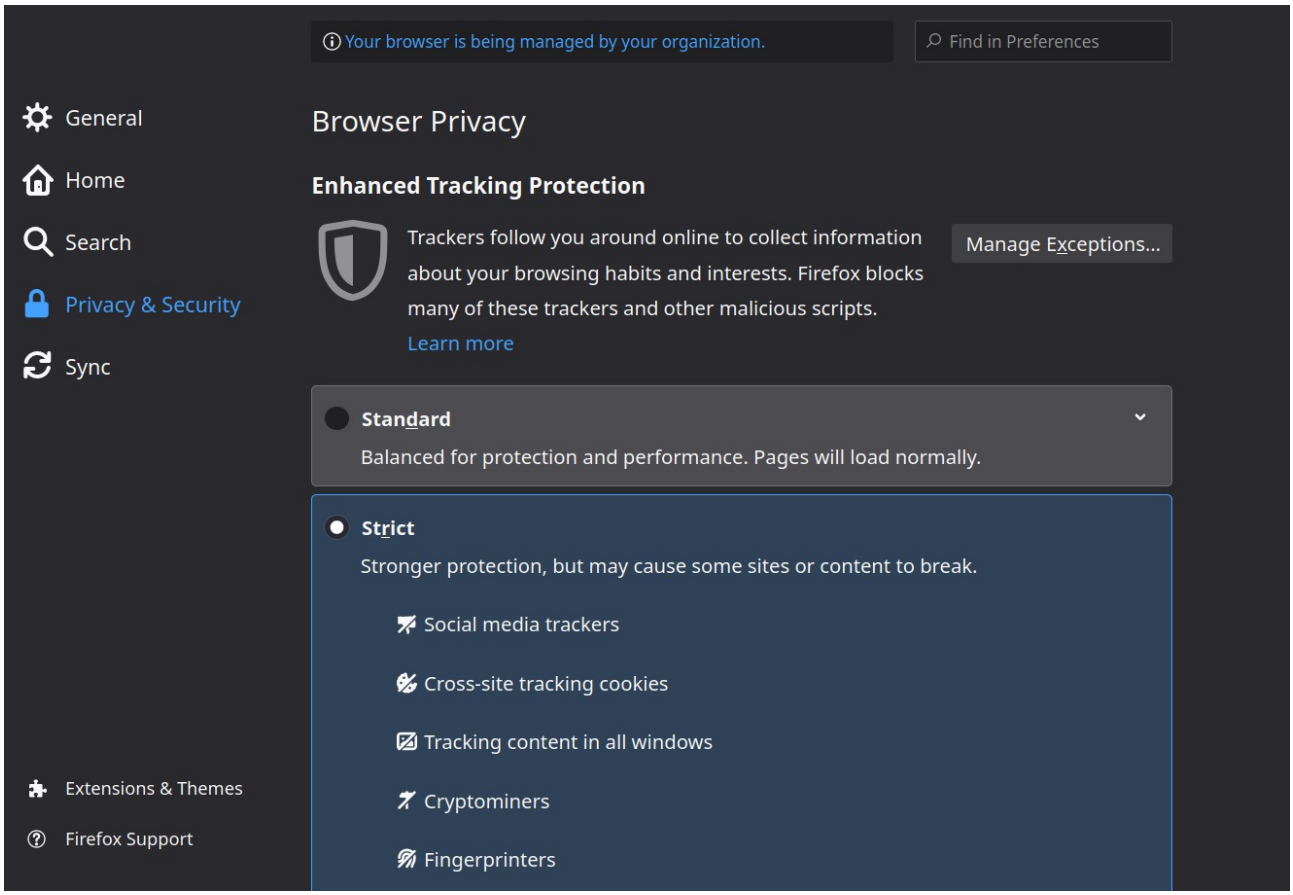
Encryption : DNS : Blah DNS, (DNS.Watch, Uncensored DNS, FDN(Europa)).

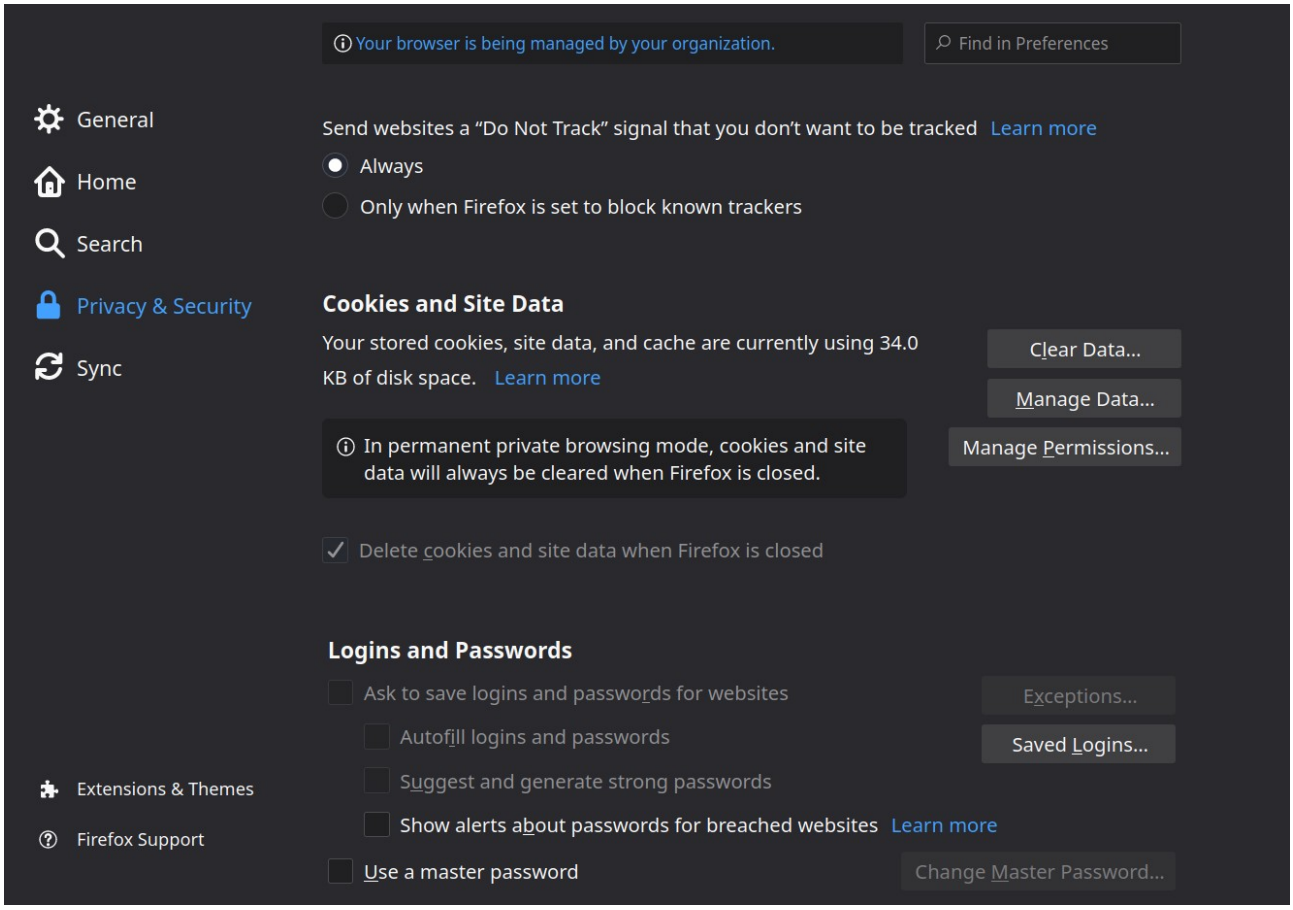
7.4 Firefox

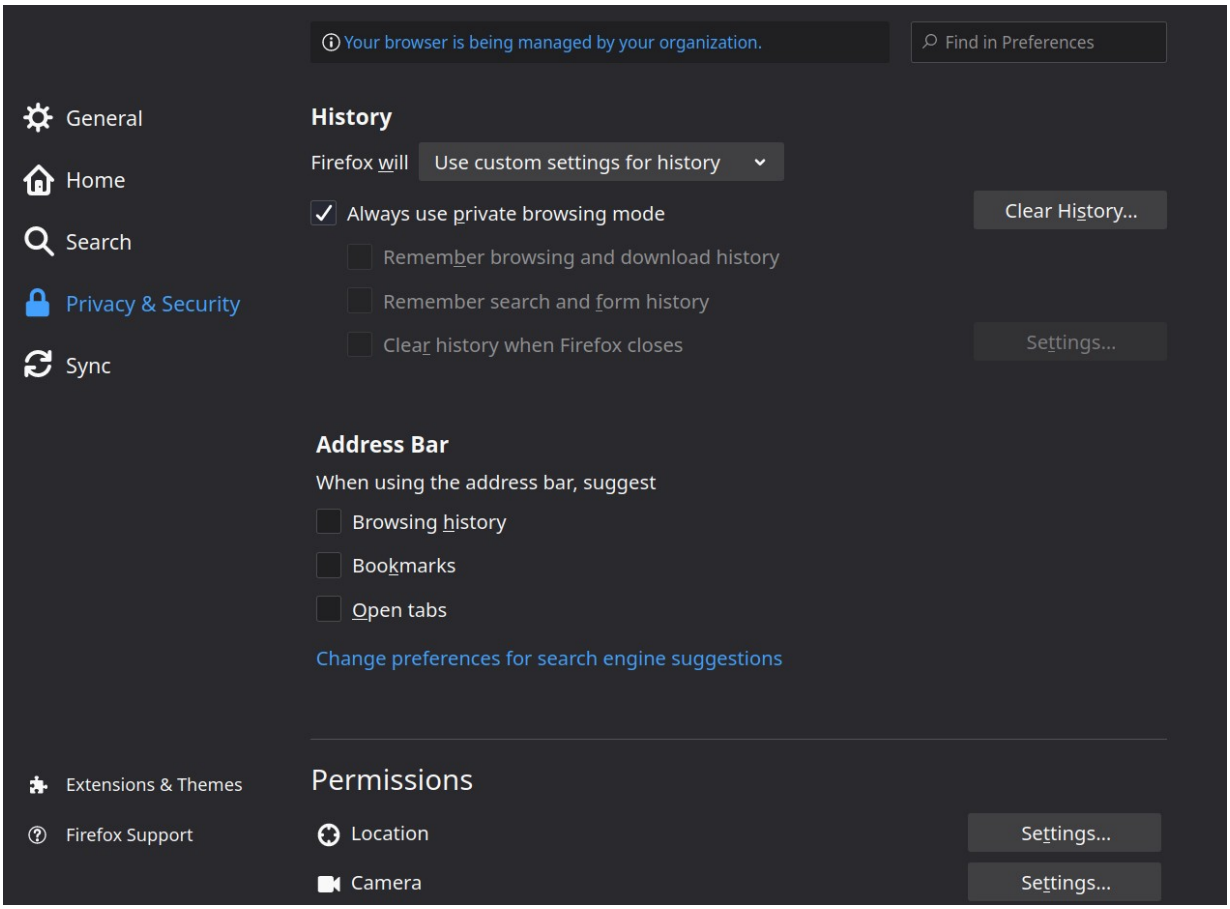
Configuración general

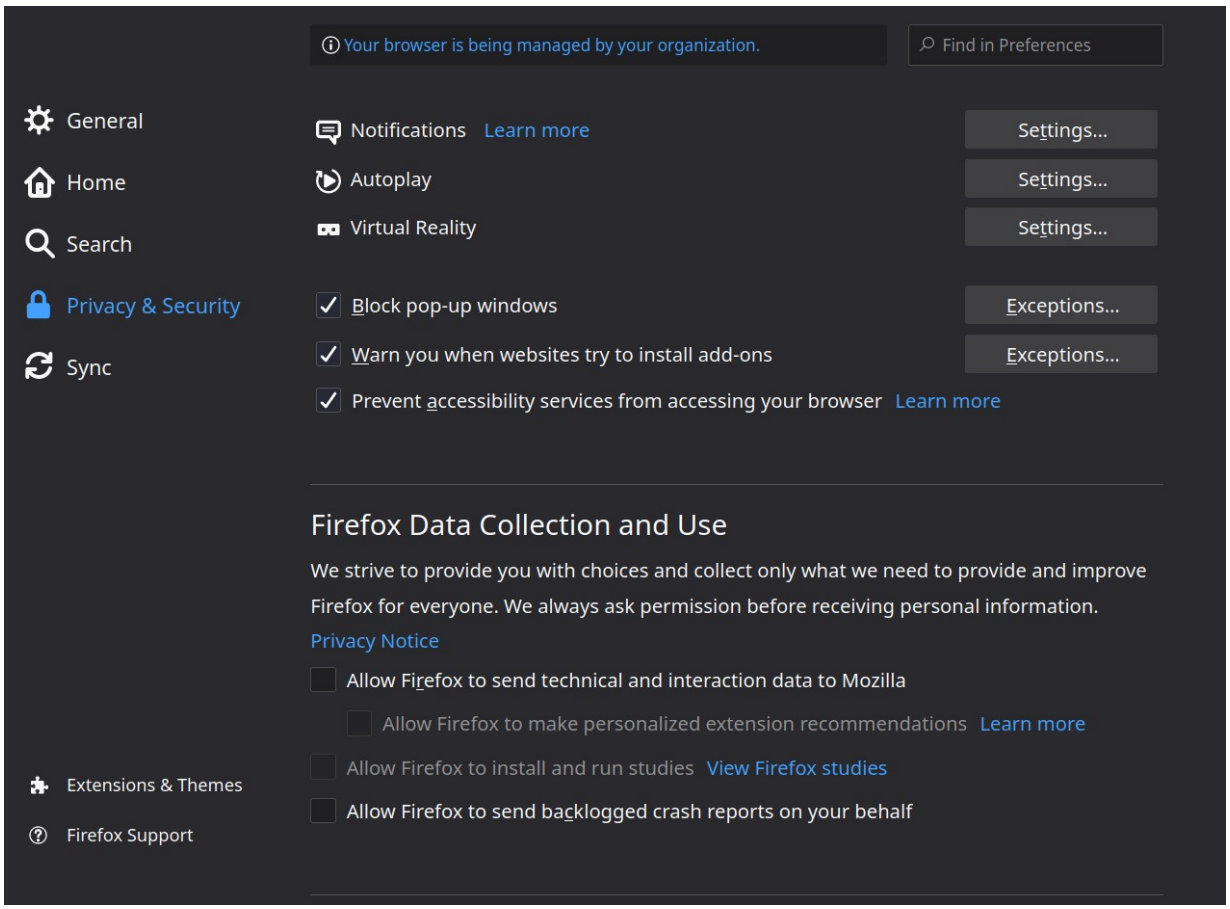


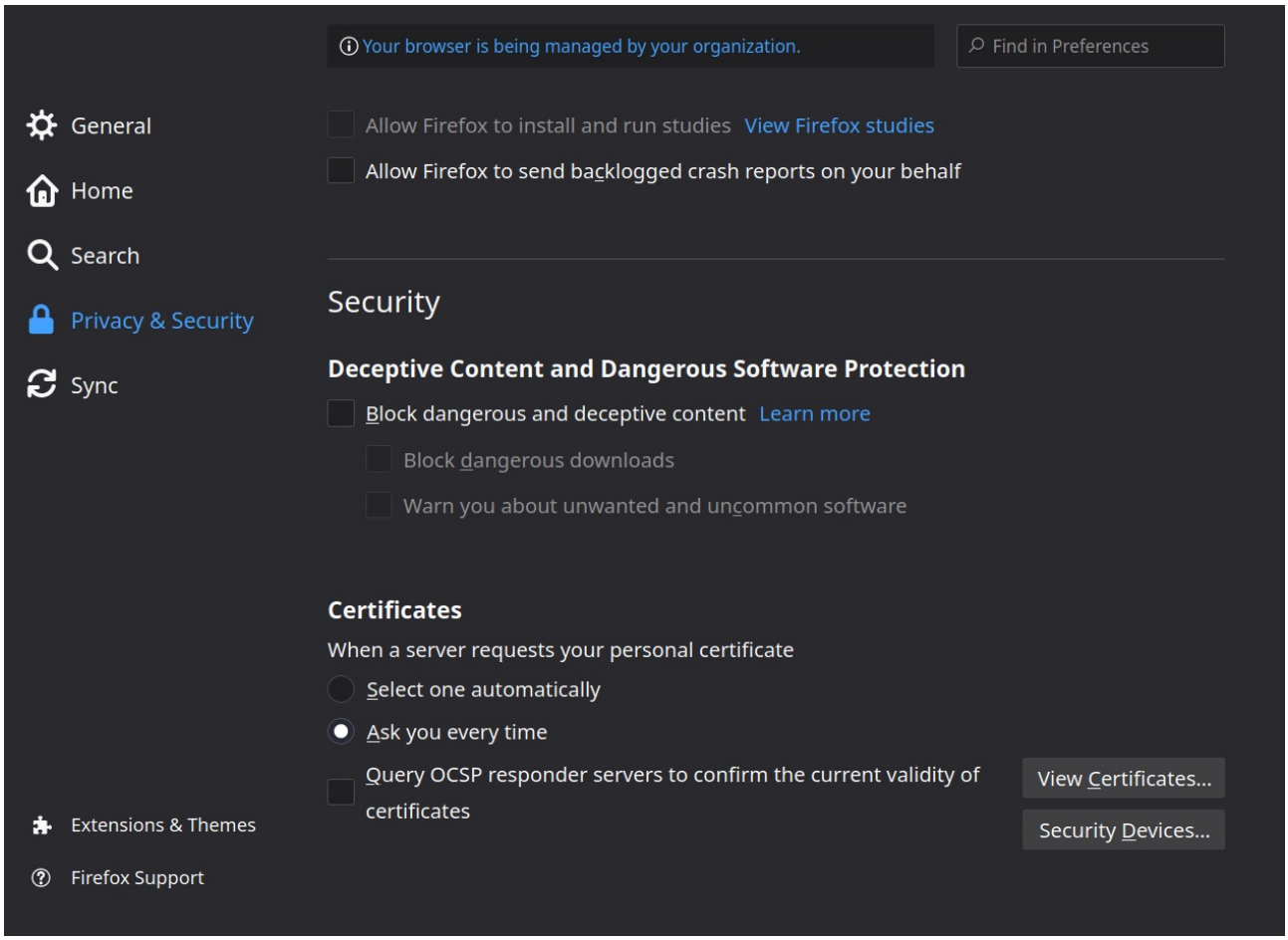



Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Browser Privacy
Enhanced Tracking Protection
Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.
Learn more
Manage Exceptions...
Standard
Balanced for protection and performance. Pages will load normally.
Strict
Stronger protection, but may cause some sites or content to break.
Social media trackers
Cross-site tracking cookies
Tracking content in all windows
Cryptominers
Fingerprinters


Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Send websites a "Do Not Track" signal that you don't want to be tracked Learn more
Always
Only when Firefox is set to block known trackers
Cookies and Site Data
Your stored cookies, site data, and cache are currently using 34.0 KB of disk space. Learn more
Clear Data...
Manage Data...
Manage Permissions...
In permanent private browsing mode, cookies and site data will always be cleared when Firefox is closed.
Delete cookies and site data when Firefox is closed
Logins and Passwords
Ask to save logins and passwords for websites
Exceptions...
Autofill logins and passwords
Saved Logins...
Suggest and generate strong passwords
Show alerts about passwords for breached websites Learn more
Use a master password
Change Master Password...


Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
History
Firefox will
Use custom settings for history
Always use private browsing mode
Clear History...
Remember browsing and download history
Remember search and form history
Clear history when Firefox closes
Settings...
Address Bar
When using the address bar, suggest
Browsing history
Bookmarks
Open tabs
Change preferences for search engine suggestions
Extensions & Themes
Firefox Support
Permissions
Location
Settings...
Camera
Settings...


Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
Notifications
Learn more
Settings...
Autoplay
Settings...
Virtual Reality
Settings...
Block pop-up windows
Exceptions...
Warn you when websites try to install add-ons
Exceptions...
Prevent accessibility services from accessing your browser
Learn more
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
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
Extensions & Themes
Firefox Support



Configuración de las extensiones

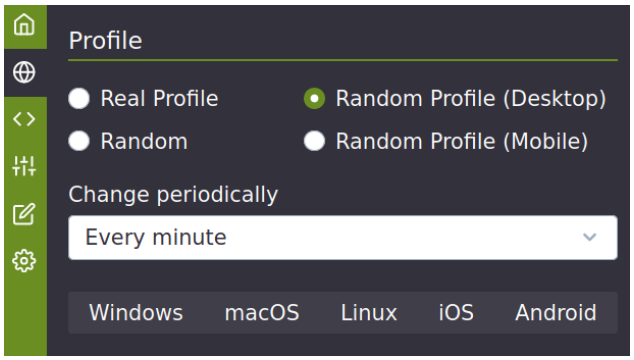
Es importante autorizar esas extensiones a funcionar en navegación privada y activar sus actualizaciones automáticas.

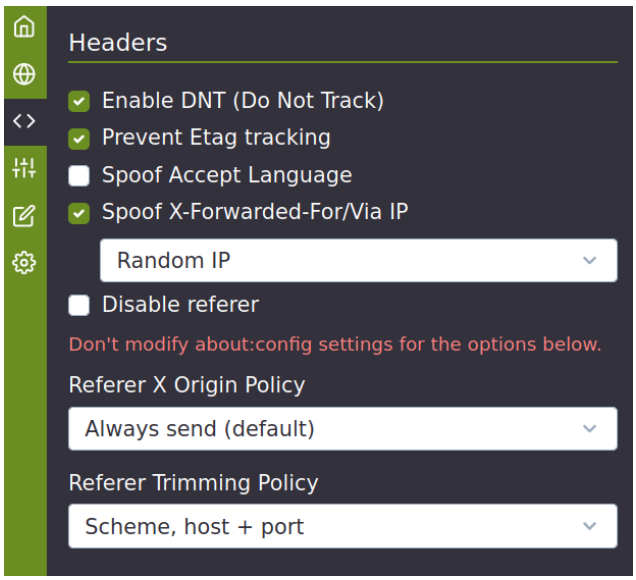
Decentraleyes, HTTPS Everywhere y Invidition :
Ninguna configuración necesaria

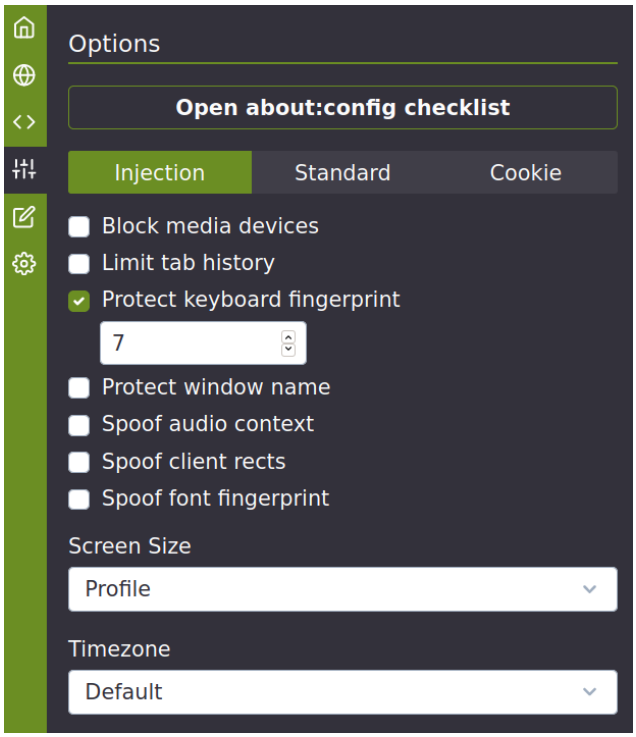
uBlock :
- Settings : activar todo bajo “Privacy”
- Filter Lists : activar TODAS las listas, excepto bajo “Regions” (idiomas usados)
- (Agregar las listas de filterlists.com : Energized : Ultimate Protection, Xtreme + IP + Social extension)

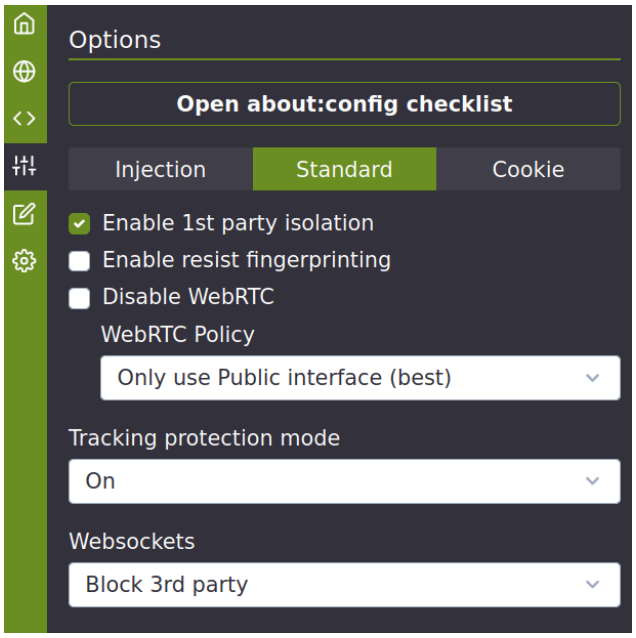
uMatrix :
Tutorial video : https://www.youtube.com/watch?v=TVozpo3zUBk

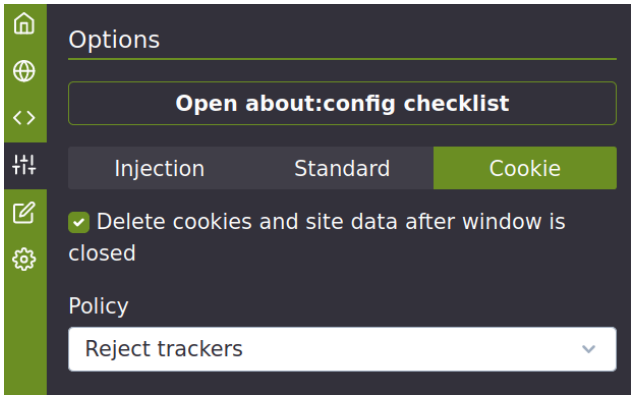
Chameleon :


Profile
Real Profile
Random Profile (Desktop)
Random
Random Profile (Mobile)
Change periodically
Every minute
Windows
macOS
Linux
iOS
Android


Headers
Enable DNT (Do Not Track)
Prevent Etag tracking
Spoof Accept Language
Spoof X-Forwarded-For/Via IP
Random IP
Disable referer
Don't modify about:config settings for the options below.
Referer X Origin Policy
Always send (default)
Referer Trimming Policy
Scheme, host + port


Options
Open about:config checklist
Injection
Standard
Cookie
Block media devices
Limit tab history
Protect keyboard fingerprint
7
Protect window name
Spoof audio context
Spoof client rects
Spoof font fingerprint
Screen Size
Profile
Timezone
Default


Options
Open about:config checklist
Injection
Standard
Cookie
Enable 1st party isolation
Enable resist fingerprinting
Disable WebRTC
WebRTC Policy
Only use Public interface (best)
Tracking protection mode
On
Websockets
Block 3rd party


Options
Open about:config checklist
Injection
Standard
Cookie
Delete cookies and site data after window is closed
Policy
Reject trackers

CanvasBlocker :
- General : marcar "Expert mode"
- Presets > open > Stealth mode
- Random number generator : non persistent
- APIs : marcar "Protect Window api" + aceptar excepción captcha
- Misc : desmarcar "Block data URL pages"

ClearURLs :
request types:
beacon,csp_report,font,image,imageset,main_frame,media,object,object_subrequest,other,ping,script,speculative,stylesheet,sub_frame,web_manifest,websocket,xbl,xml_dtd,xmlhttprequest,xslt

Cookie AutoDelete :
- Automatic Cleaning Options : activar todo
- Extension Options : desactivar “Show notification after cookie cleanup”

(Privacy Badger) :
(- General settings : marcar "learn in private/incognito windows")

Configuraciones about:config

Acceder a estos ajustes entrando about:config en la barra de direcciones de Firefox. Esas diversas configuraciones mejoran la privacidad, la seguridad y el rendimiento. Los elementos entre paréntesis no suelen ser deseables en todos los casos.

accessibility.blockautorefresh = true

((accessibility.force_disabled = 1))

beacon.enabled = false

browser.cache.offline.capacity = 0

browser.cache.offline.enable = false

browser.display.use_document_fonts = 0

browser.send_pings.max_per_link = 0

browser.sessionhistory.max_entries = 15
Numero máximo de paginas disponibles con "precedente", aligera Firefox
browser.sessionhistory.max_total_viewers = 4
Numero máximo de paginas cargadas con "precedente", aligera Firefox

browser.sessionstore.interval = 50000

browser.sessionstore.privacy_level = 2

(browser.startup.homepage_override.buildID = borrar)

browser.urlbar.autofill.enabled = false
(browser.urlbar.maxRichResults = 0)
browser.urlbar.speculativeConnect.enabled = false

browser.urlbar.trimURLs = false

browser.xul.error_pages.expert_bad_cert = true

captivedetect.canonicalURL = borrar

device.sensors = false para todos los elementos

dom.allow_cut_copy = false

dom.battery.enabled = false

dom.enable_performance = false
dom.enable_resource_timing = false

dom.event.clipboardevents.enabled = false
dom.event.contextmenu.enabled = false

dom.push = false para todos los elementos + borrar las direcciones e identificadores

dom.serviceWorkers.enabled= false

dom.vr.oculus.enabled = false

dom.webaudio.enabled = false

gamepad = false para todos los elementos

geo = borrar todas las direcciones
geo.enabled = false

(gfx.font_rendering.graphite.enabled = false)

google = false para todos los elementos + borrar las direcciones

javascript.options.baselinejit = false
javascript.options.ion = false

javascript.options.native_regexp = false

layers.acceleration.force-enabled = true

layout.css.visited_links_enabled = false

mathml.disabled = true

((media.gmp-widevinecdm.enabled = false))
((Desactiva DRM, sí videos DRM no necesarias))

media.navigator.enabled = false

media.video_stats.enabled = false

network.captive-portal-service.enabled = false

network.dnsCacheEntries = 4000
network.dnsCacheExpiration = 43200
network.dnsCacheExpirationGracePeriod = 43200

network.IDN_show_punycode = true

network.http.referer.XOriginPolicy = 0
network.http.referer.XOriginTrimmingPolicy = 2
network.http.referer.spoofSource = true
network.http.referer.trimmingPolicy = 2

network.http.speculative-parallel-limit = 0

network.manage-offline-status = false

normandy = false para todos los elementos + borrar las direcciones e identificadores

pocket = false para todos los elementos + borrar las direcciones e identificadores

privacy.clearOnShutdown.offlineApps = true

privacy.spoof_english = 2

privacy.trackingprotection.socialtracking.enabled = true

report (reporter/reporting) = false para todos los elementos + borrar las direcciones

safebrowsing = false para todos los elementos + borrar direcciones e identificadores

security.cert_pinning.enforcement_level = 2

security.mixed_content.upgrade_display_content = true

security.OCSP.enabled = 0

security.ssl.enable_false_start = false
security.ssl.enable_ocsp_must_staple = false
security.ssl.enable_ocsp_stapling = false
security.ssl.require_safe_negotiation = true
security.ssl3.rsa_des_ede3_sha = false

security.tls.enable_0rtt_data = false

security.tls.version.min = 3

telemetry = false para todos los elementos + borrar las direcciones e identificadores

ui.use_standins_for_native_colors = true

webgl.disabled = true

webgl.enable-debug-renderer-info = false

webgl.enable-webgl2 = false

Solo si no se usa la extensión Chameleon :

(privacy.resistFingerprinting = true)

(Mejor poner "false" y falsificar el fingerprint con Chameleon)

Estos deberían ser configurados directamente con Chameleon sí esta instalado :

media.peerconnection.ice.default_address_only = true

media.peerconnection.ice.no_host = true

((media.peerconnection.enabled = false))

privacy.firstparty.isolate = true