Firefox: Protection de la vie privée "about: config"

Il s'agit d'une collection de confidentialité **concernant: les** réglages de **configuration** . Nous vous montrerons comment améliorer la confidentialité de votre navigateur Firefox.

Préparation:

1. Entrez "about: config" dans la barre d'adresse de Firefox et appuyez sur Entrée.
2. Appuyez sur le bouton "Je ferai attention, je le promets!"
3. Suivez les instructions ci-dessous ...

Commencer:

1. Privacy.firstparty.isolate = true
    - En raison de l'effort de Tor Uplift , cette préférence isole toutes les sources d'identifiant du navigateur (par exemple, les cookies) dans le domaine de la première partie, dans le but d'empêcher le suivi sur différents domaines.
2. Privacy.resistFingerprinting = true
    - Résultat de l'effort de Tor Uplift , cette préférence rend Firefox plus résistant aux empreintes digitales du navigateur.
3. Privacy.trackingprotection.enabled = true
    - C'est la nouvelle protection de suivi intégrée de Mozilla. Il utilise la liste des filtres Disconnect.me, qui est redondante si vous utilisez déjà des filtres uBlock Origin 3rd party, donc vous devez le définir comme faux si vous utilisez les fonctionnalités complémentaires.
4. Browser.cache.offline.enable = false
    - Désactive le cache hors ligne.
5. Browser.safebrowsing.malware.enabled = false
    - Désactivez les contrôles de logiciels malveillants de Google Safe Browsing. Risque de sécurité, mais amélioration de la vie privée.
6. Browser.safebrowsing.phishing.enabled = false
    - Désactiver la navigation sécurisée Google et la protection contre les phishing. Risque de sécurité, mais amélioration de la vie privée.
7. Browser.send_pings = false
    - L'attribut serait utile pour permettre aux sites Web de suivre les clics des visiteurs.
8. Browser.sessionstore.max_tabs_undo = 0
    - Même avec Firefox configuré pour ne pas se souvenir de l'histoire, vos onglets fermés sont stockés temporairement dans Menu -> Historique -> Onglets récemment fermés.
9. Browser.urlbar.speculativeConnect.enabled = false
    - Désactiver la préchargement des URL d'autocomplète. Firefox précharge les URL qui se complètent automatiquement lorsqu'un utilisateur tape dans la barre d'adresse, ce qui est une préoccupation si des URL suggèrent que l'utilisateur ne souhaite pas se connecter. Source
10. Dom.battery.enabled = false
    - Les propriétaires de sites Web peuvent suivre l'état de la batterie de votre appareil. Source
11. Dom.event.clipboardevents.enabled = false

- Désactivez que les sites Web peuvent obtenir des notifications si vous copiez, collez ou coupez quelque chose à partir d'une page Web, et leur permet de savoir quelle partie de la page a été sélectionnée.

12. Geo.enabled = false
    - Désactive la géolocalisation.
13. Media.navigator.enabled = false
    - Les sites Web peuvent suivre l'état du microphone et de l'appareil photo de votre appareil.
14. Network.cookie.cookieBehavior = 1
    - Désactiver les cookies
    - 0 = Accepter tous les cookies par défaut
    - 1 = accepter uniquement du site d'origine (bloquer les cookies tiers)
    - 2 = Bloquer tous les cookies par défaut
15. Network.cookie.lifetimePolicy = 2
    - Les cookies sont supprimés à la fin de la session
    - 0 = Accepter les cookies normalement
    - 1 = Demande pour chaque cookie
    - 2 = Accepter pour la session actuelle seulement
    - 3 = accepter pour N jours
16. Webgl.disabled = true
    - WebGL est un risque de sécurité potentiel. Source

Information connexe

- Ffprofile.com - Vous aide à créer un profil Firefox avec les paramètres par défaut souhaités .
- Mozillazine.org - Préférences liées à la sécurité et à la vie privée.
- User.js Firefox endurant les choses : il s'agit d'un fichier de configuration user.js pour Mozilla Firefox qui est censé durcir les paramètres de Firefox et le rendre plus sécurisé.
- Paramètres de confidentialité - Un complément Firefox pour modifier facilement les paramètres de confidentialité intégrés avec un panneau de barre d'outils.