

Comment sécuriser Firefox efficacement en quelques clics de souris ?

 <h2>Attention, danger !</h2> <hr/> <p>La modification de ces préférences avancées peut être dommageable pour la stabilité, la sécurité et les performances de cette application. Ne continuez que si vous savez ce que vous faites.</p> <p><input checked="" type="checkbox"/> Afficher cet avertissement la prochaine fois</p> <p>Je ferai attention, promis !</p>	<p>Comment sécuriser Firefox efficacement en quelques clics de souris ?</p>
---	---

Vous utilisez Firefox et vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimeront la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande `about:config`. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne `security.tls.version`. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne `geo.enabled` pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaissent pas la dernière page que vous avez pu visiter, cherchez la ligne `network.http.sendRefererHeader` et mettez la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne `browser.safebrowsing.malware.enabled`.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne `browser.safebrowsing.provider.google.lists` et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offline », en mode hors connexion. Cherchez les lignes `offline-apps.allow_by_default` et `offline-apps.quota.warn`. La première valeur est à passer en False, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach