17

Les bonnes pratiques pour le déploiement sécurisé du navigateur Firefox

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

LES BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR FIREFOX

Firefox est le navigateur web libre et gratuit édité par la fondation Mozilla et dont la première version stable date de 2004. Il a connu un succès croissant depuis sa sortie, il est aujourd'hui soutenu par une importante communauté de développeurs du monde libre.

Firefox dispose d'un mécanisme de mise à jour automatique et peut être configuré de manière centralisée. Il se prête bien à une utilisation professionnelle.

Avec Firefox, vous disposez de nombreux outils et réglages pour vous aider à vous protéger efficacement contre les sites frauduleux et les escrocs du net.

Ces bonnes pratiques visent à sensibiliser le lecteur aux enjeux de sécurité d'un navigateur Web et le guider dans la mise en œuvre d'une stratégie de sécurisation spécifique à Firefox.

1. Garder vos logiciels et votre système d'exploitation à jour

Les mises à jour logicielles contiennent des correctifs de vulnérabilité afin de protéger votre ordinateur et vos informations personnelles.

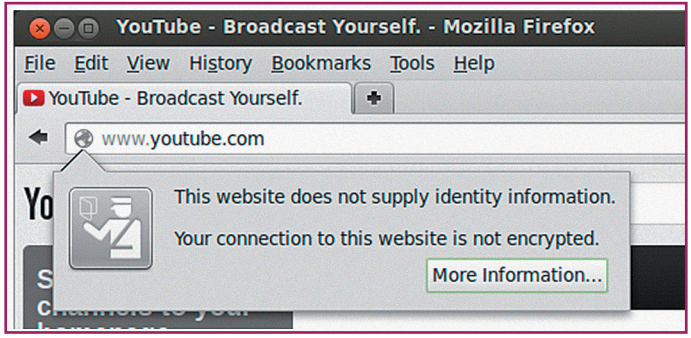
- Mettre à jour Firefox
- Cliquez sur le bouton (en haut à droite)
- Cliquez sur aide et sélectionnez le menu À propos de Firefox.
- Consultez Mettre à jour Firefox vers la dernière version pour plus de détails.[1]
- Mettre à jour vos plugins : Allez sur la page de vérification des plugins de Mozilla[2] et suivez les liens pour mettre à jour les plugins obsolètes.

1. https://support.mozila.org/kr/kb/mettre-jour-firefox-derniere-version
2. https://www.mozila.org/pluginchеck

2. Définir des permissions

Dans la fenêtre d'informations sur la page que vous êtes en train de visiter, vous avez la possibilité de définir pour le site courant le comportement à adopter pour le chargement ou non des images, l'ouverture ou non des fenêtres pop-up, l'autorisation ou non des cookies, l'installation ou non de thèmes ou d'extensions pour le navigateur.

- Cliquez sur **le bouton d'identité du site** (l'icône du site web à gauche de son adresse), puis sur le bouton **Plus d'informations**… dans l'invite.
  Par exemple, lors de la visite d'un site (www.youtube.com) définir le comportement à suivre vis-à-vis des images **(Bloquer, Autoriser, Toujours demander).**
- Dans Permissions, Décochez la case **Permission par défaut** devant **Charger des images.**

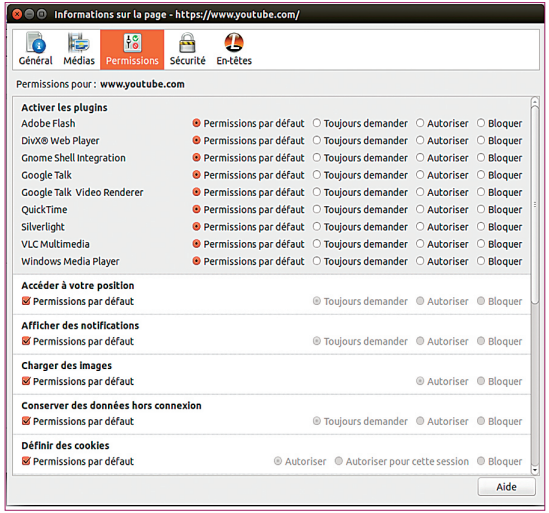


- Cliquer sur **Bloquer.**
- Ainsi les images seront bloquées pour ce site. **Fermez la fenêtre.**

3. Limiter le choix des plugins

Tout plugin ajouté à Firefox fait courir un risque de sécurité supplémentaire, d'où l'importance de les limiter au strict nécessaire.

Les plugins ou greffons, qui sont des composants compilés dédiés à offrir des fonctionnalités avancées du navigateur, et répondre à des besoins spécifiques. Une vulnérabilité affectant un plugin permet en revanche de compromettre la session ou le système.



4. Ne déployer que des extensions de confiance et nécessaires

Contrairement aux plugins qui sont des programmes compilés, les extensions s'exécutent dans le processus du navigateur et sans système de permission permettant de restreindre les libertés qui leur sont accordées. Ainsi, une extension malveillante peut accéder à des informations sensibles concernant la navigation de l'utilisateur puis les envoyer à un serveur illégitime sur Internet. Ou encore introduire de nouveaux comportements indésirables suite à une mise à jour. En parallèle, de nombreuses extensions présentent des vulnérabilités qui peuvent être exploitées (par le contenu des pages visitées ou encore, par courriels spécifiquement forgés et consultés par webmail).
Ces extensions vulnérables peuvent également servir à exploiter, par rebond, les vulnérabilités d'éventuels plugins activés et ainsi obtenir un accès complet au système.

5. Désactiver l'utilisation de SSL

Désactiver l'utilisation de SSL et n'autoriser que les protocoles TLS v1.1 et supérieurs (la v1.0 étant vulnérable). Il est également possible de restreindre les suites cryptographiques utilisable en désactivant celles reposant sur des algorithmes obsolètes comme RC4.

6. Garantir la confidentialité

- Désactiver les divers rapports disponibles de plantage, de performance, etc. pour limiter les données envoyées à Mozilla.
- Activer les fonctionnalités de protection de la confidentialité (anti pistage, navigation privée, suppression des données privées, etc.) lorsque le navigateur n'est pas dédié à une navigation Intranet.
- Interdire les fonctions de géolocalisation.
- Dès lors que la confidentialité des recherches est jugée primordiale, il conviendra d'imposer un moteur de recherche de confiance et de désactiver les fonctionnalités de recherche instantanée ou de suggestion de recherche.

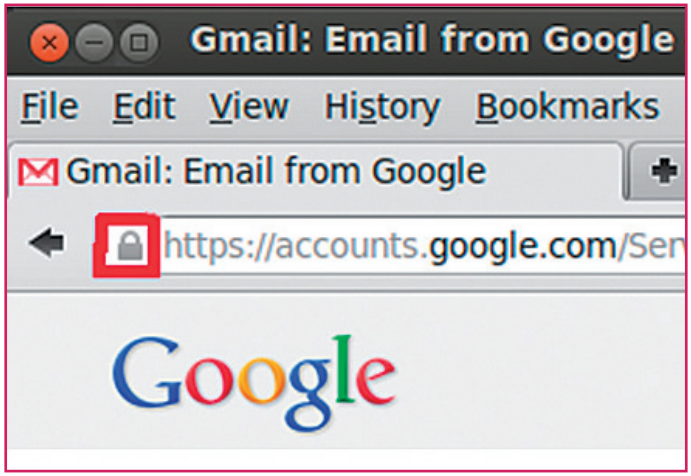
7. Page d'accueil

Il est préférable que le navigateur n'enregistre pas les sessions de navigation. Lors du démarrage du navigateur (après un arrêt normal ou brusque), il est en effet conseillé de ne pas restaurer la session précédente de l'utilisateur mais d'afficher une (des) page(s) connue(s) et de confiance.

8. Stratégie de double navigateur

Dédier un Il est recommandé d'utilise deux navigateurs. Le premier sera dédié à la navigation sur Internet avec une configuration durcie, sa surface d'attaque est réduite au

maximum. Le deuxième sera réservé à l'accès aux serveurs internes, configuré pour permettre uniquement l'accès et l'usage de l'ensemble des sites et applications légères de l'Intranet.



9. Vérifier vos paramètres de Firefox

Firefox a de nombreuses façons de vous aider à rester protégé sur le Web.

- Savoir si ma connexion vers un site web est sécurisée ?

Avec le bouton d'identité de site intégré à Firefox qui permet de donner des informations supplémentaires sur le site visité, savoir s'il est chiffré, si sa sécurité a été vérifiée et par qui, à qui appartient le site web. Cela peut vous aider à identifier les sites malveillants qui tenteraient d'obtenir des informations personnelles. Lors d'une visite à un site, vérifier toujours l'état du bouton d'identité du site qui peut prendre une de ces 5 formes.

- Désactiver les cookies tiers dans Firefox pour éviter de pister vos visites sur les sites web : Le réglage des cookies tiers est disponible dans le panneau « Vie privée » de la fenêtre « Préférences », cliquer sur **Ne rien indiquer aux sites concernant mes préférences de pistage** et aussi Positionnez **Accepter les cookies tiers à jamais.**
- Utiliser un mot de passe principal pour protéger les identifiants et mots de passe enregistrés :
- Cliquez sur le bouton menu et sélectionnez Préférences
- Cliquez sur le panneau **Sécurité.**
- Cochez Utiliser un mot de passe principal. La fenêtre « Modifier le mot de passe principal » apparaît.
- Saisissez votre mot de passe principal.