

16

Bonnes pratiques pour le déploiement sécurisé du navigateur Google Chrome



BONNES PRATIQUES POUR LE DÉPLOIEMENT SÉCURISÉ DU NAVIGATEUR GOOGLE CHROME

Aujourd'hui, Google Chrome est devenu l'un des navigateurs les plus utilisés par les internautes. Ce navigateur possède plusieurs fonctionnalités telles qu'un système de « bac à sable », des possibilités de déploiement et de configuration centralisés, et son système de mise à jour automatique réactif. Nous présentons dans ce qui suit quelques recommandations pour un déploiement sécurisé de ce navigateur web.

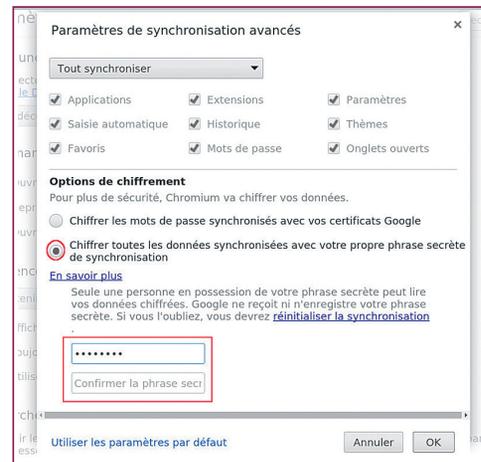
1. Protéger ses mots de passe enregistrés

Si vous laissez Chrome enregistrer vos mots de passe, toute personne qui utilise votre PC peut facilement y accéder à travers le panneau réglages. Il est donc recommandé de ne permettre qu'aux personnes de confiance d'utiliser votre compte utilisateur. Vous pouvez créer un nouveau compte standard (non administratif) pour les autres utilisateurs ou les laissez utiliser le compte Invité. Vous pouvez aussi utiliser des extensions comme ChromePW, Browser Lock, ou un profil chrom sécurisé par mot de passe. Une autre option consiste à stocker vos données sensibles en utilisant un gestionnaire de mot de passe tiers.

2. Sécuriser vos données synchronisées

Si vous avez activé la synchronisation, Chrome conserve vos renseignements (préférences, mots de passe, etc) en utilisant vos identifiants de compte Google. La synchronisation devient cependant une vulnérabilité si votre compte Google venait à être piraté. Vous pouvez ajouter un niveau de protection en définissant un mot de passe de synchronisation, qui sera toujours requis pour accéder à vos données. Pensez aussi à renforcer la sécurité de votre compte Google en utilisant la validation en deux étapes par exemple.

Figure 1 :
Mot de passe de synchronisation



3. Safe browsing

Safe browsing est une fonctionnalité de sécurité qui vise à protéger l'internaute contre les sites de phishing et les téléchargements malveillants. Il fonctionne en envoyant les adresses de sites Web visités (sous forme de hash) à Google. Dans le cas d'une page dangereuse, l'utilisateur sera averti par message. La navigation sécurisée peut être entièrement désactivée si le compromis entre la vie privée (envoi de données de navigation à google) et la sécurité (liens et pages dangereuses) n'est pas acceptable.

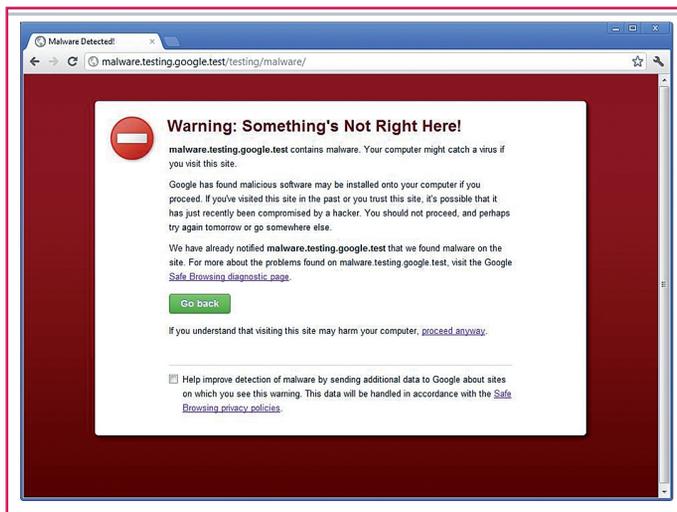


Figure 2 : Fonctionnalité Safe browsing

4. Sécurité des plugins/extensions

L'utilisateur peut installer des plugins et des extensions de la boutique en ligne Chrome.

Les plugins Chrome peuvent être développés en utilisant une des deux interfaces de programmation :

- NPAPI qui permet l'exécution des plugins avec le niveau de privilège de l'utilisateur. Une vulnérabilité affectant un plugin permet alors de compromettre la session ou le système.
- PPAPI: dont l'objectif est de rendre les plugins portables et sécurisés, et permet leur exécution en mode « bac à sable » en séparant les processus du navigateur et du moteur de rendu. L'exploitation de vulnérabilités du plugin reste alors confinée au processus.

Il est recommandé de n'autoriser que les plugins développés via PPAPI à l'inverse de NPAPI qui resté, malheureusement, l'outil le plus utilisé pour le développement de plugins. De même, il est recommandé de n'autoriser aucune extension sauf celles qui se justifient par un réel besoin métier comme par exemple les extensions de développement Web.

5. Installer des extensions pour plus de sécurité

Diverses extensions permettent d'ajouter encore plus de fonctions de sécurité. Par exemple, Adblock permet de supprimer les publicités qui peuvent conduire à des logiciels malveillants ou à des sites de Phishing.

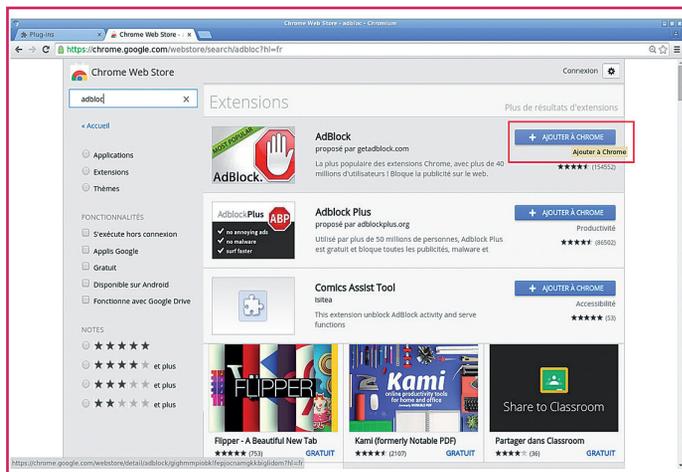


Figure 2 : Ajout des extensions dans Google Chrome

6. Chrome, active directory et politique de sécurité

Dans ses dernières versions, Active Directory de Microsoft permet de définir des règles de sécurité dans les GPO (Group Policy Object), permettant ainsi une configuration centralisée du navigateur.

En entreprise, il est recommandé d'utiliser cette fonctionnalité pour inclure des règles de configuration importantes pour la sécurité de la navigation.

7. Installer un logiciel antivirus à jour

Il est indispensable d'installer des programmes de sécurité tel qu'un antivirus et de faire en sorte qu'il soit régulièrement mis à jour afin de se protéger contre les nouvelles menaces. Certains de ces programmes permettent d'empêcher le téléchargement des logiciels dangereux sur votre ordinateur pendant la navigation sur Internet. De plus, ils permettent d'identifier les sites Web suspects au niveau des résultats de recherche vous informant du risque que présentent ces sites avant d'y accéder.

Google chrome