

Sécuriser Google Chrome

 malekal.com/securer-google-chrome/

malekalmorte

14/01/2013

Voici une page qui récapitule quelques recettes à suivre pour sécuriser [Google Chrome](#).

Le but est de vous donner toutes les explications pour améliorer la sécurité de Google Chrome, se protéger des [virus](#) et comprendre comment les éviter.

Table des matières [[masquer](#)]

- [1 Activer l'Anti-Tracking](#)
- [2 Plugin et Web Exploits](#)
- [3 Gérer ses mots de passe](#)
- [4 Blocage de contenu](#)
 - [4.1 Par défaut](#)
- [5 Les extensions pour se protéger sur internet](#)
 - [5.1 NoScript et Script Safe](#)
 - [5.2 uMatrix](#)
 - [5.3 Adblock](#)
 - [5.4 uBlock](#)
- [6 Quelques extensions en vrac](#)
- [7 Plus loin dans la sécurité de son PC](#)
- [8 Liens Google Chrome](#)

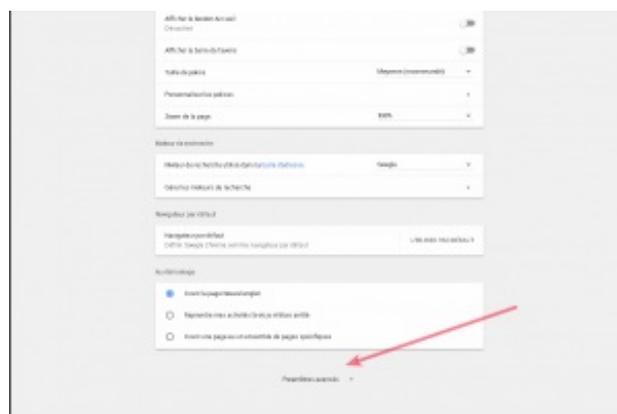


Activer l'Anti-Tracking

Pour empêcher le tracking web, vous pouvez activer l'Anti-Tracking qui permet de demander le non suivi de la part des sites internet visité, pour cela :

- Cela se fait depuis le menu Outils / Paramètres.
- En bas, cliquez sur Afficher les paramètres avancés.
- Puis dans la liste cochez Envoyer une requête « Interdire le suivi » avec votre trafic de navigation ».

L'extension Ghostery peut permettre encore d'améliorer la protection de votre vie privée :



<https://chrome.google.com/webstore/detail/ghostery/mlmiejdfkolichcfejlclcbmpeanii>

Vous pouvez empêcher les [tracking cookies](#) d'être créés à partir d'extensions, pour cela, se reporter à la page

suivante :

[Limiter les pistages par cookies \(cookies tracking\)](#)
et de manière générale sur le tracking WEB et la confidentialité sur internet : [Le Web Tracking sur internet](#)

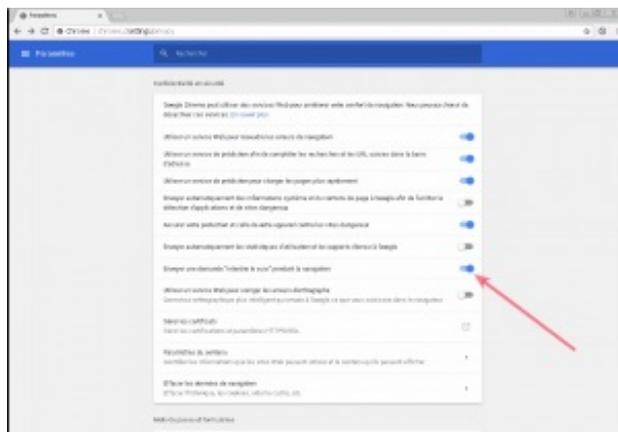
Plugin et Web Exploits

Dans un premier temps, pour comprendre le fonctionnement des plugins, ces derniers étant souvent confondus, vous pouvez lire la page : [Différences plugins et extensions sur les navigateurs WEB](#)

Des plugins non à jour possèdent des vulnérabilités qui permettent l'infection de votre PC par la simple visite d'un site via [des exploits sur site web](#).

Ci-dessous une URL [d'exploit sur site web](#) – Comme vous pouvez le constater [Google Chrome](#) affiche une alerte disant que Java a été bloqué car obsolète.

Il vous est alors proposé de mettre à jour le plugin ou de l'exécuter.



Si l'internaute choisi exécuter, Java se lance, l'exploit aussi et le [malware et virus](#) ensuite.

The screenshot shows a Windows desktop environment. On the left, a web browser window is open, displaying a page with the word "Disperse" in a large font. On the right, the Process Explorer application is open, showing a list of running processes. The processes are listed in a table with columns for Process, PID, CPU, Description, and Company Name. Several instances of "chrome.exe" are visible, with one instance highlighted in red. The taskbar at the bottom shows the Start button and several open applications, including Process Explorer, Debugging Tools, Downloads, and a browser window.

Process	PID	CPU	Description	Company Name
System Idle Process	0	59.05		
System	4			
Interrupts	n/a	0.95	Hardware Interrupts and DPCs	
smss.exe	376		Gestionnaire de session Win...	Microsoft Corporation
csrss.exe	632		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	656		Application d'ouverture de se...	Microsoft Corporation
services.exe	700	0.95	Applications Services et Con...	Microsoft Corporation
vmacthlp.exe	872		VMware Activation Helper	VMware, Inc.
svchost.exe	888		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	968		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1056		Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe	1252		Windows Security Center No...	Microsoft Corporation
svchost.exe	1176		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1272		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1612		Spooler SubSystem App	Microsoft Corporation
minvnc.exe	496		Serveur VNC pour Win32	www.ultravnc.fr
vmtoolsd.exe	532		VMware Tools Core Service	VMware, Inc.
alg.exe	1660		Application Layer Gateway S...	Microsoft Corporation
iqs.exe	2504		Java(TM) Quick Starter Servi...	Oracle Corporation
wmiapsrv.exe	316		Service de la carte de perfor...	Microsoft Corporation
svchost.exe	880		Generic Host Process for Wi...	Microsoft Corporation
lsass.exe	712		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1456		Explorateur Windows	Microsoft Corporation
VMwareTray.exe	1740		VMware Tools tray application	VMware, Inc.
vmtoolsd.exe	1768		VMware Tools Core Service	VMware, Inc.
ctfmon.exe	1784		CTF Loader	Microsoft Corporation
msmsgs.exe	1800		Windows Messenger	Microsoft Corporation
procexp.exe	456	0.95	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WinSCP.exe	432		WinSCP: SFTP, FTP and SC...	Martin Prikl
chrome.exe	1760		Google Chrome	Google Inc.
chrome.exe	3496		Google Chrome	Google Inc.
chrome.exe	2668		Google Chrome	Google Inc.
chrome.exe	3960		Google Chrome	Google Inc.
chrome.exe	3372		Google Chrome	Google Inc.
java.exe	2672		Java(TM) Platform SE binary	Oracle Corporation
regsvr32.exe	2172	38.10	Microsoft(C) Register Server	Microsoft Corporation
chrome.exe	3112		Google Chrome	Google Inc.

et surtout Maintenez ses logiciels à jour : [Logiciels pour maintenir ses programmes à jour.](#)

Gérer ses mots de passe

Il faut aussi bien savoir gérer ses mots de passe WEB très prisés des pirates pour voler des accès à vos services internet préférés.

Pour une bonne utilisation de vos mots de passe à travers votre navigateur internet, rendez-vous sur la page : [Mots de passe sur les navigateurs WEB](#)

Blocage de contenu

Par défaut

Google permet de bloquer le contenu (Javascript, Flash etc) des sites visités, à travers des listes.

Pour plus d'informations sur la gestion du contenu avec Google Chrome, suivez notre page : [Blocage de script sur Google Chrome](#)



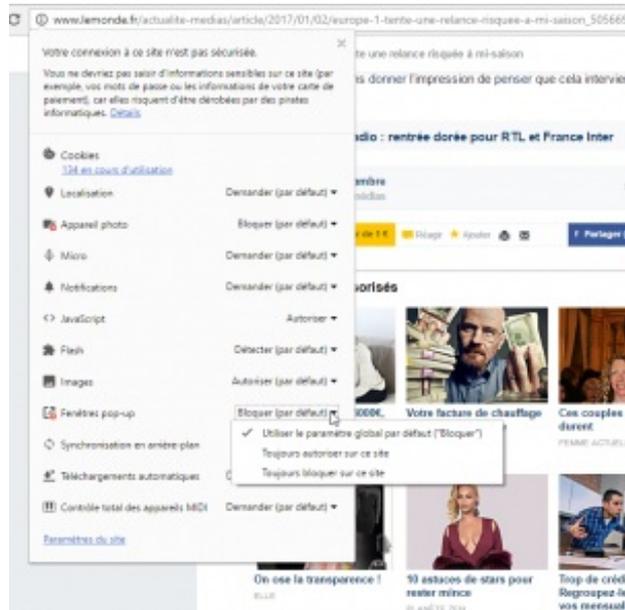
Les extensions pour se protéger sur internet

NoScript et Script Safe

NoScript ou Script Safe sont des extensions qui permettent de bloquer les scripts des sites WEB, cela permet de bloquer certaines publicités et/ou scripts malveillants.

Il est bien entendu possible d'ajouter certaines adresses en liste blanche dont les scripts seront exécutés à chaque fois.

Ci-dessous une capture de l'extension Script Safe :

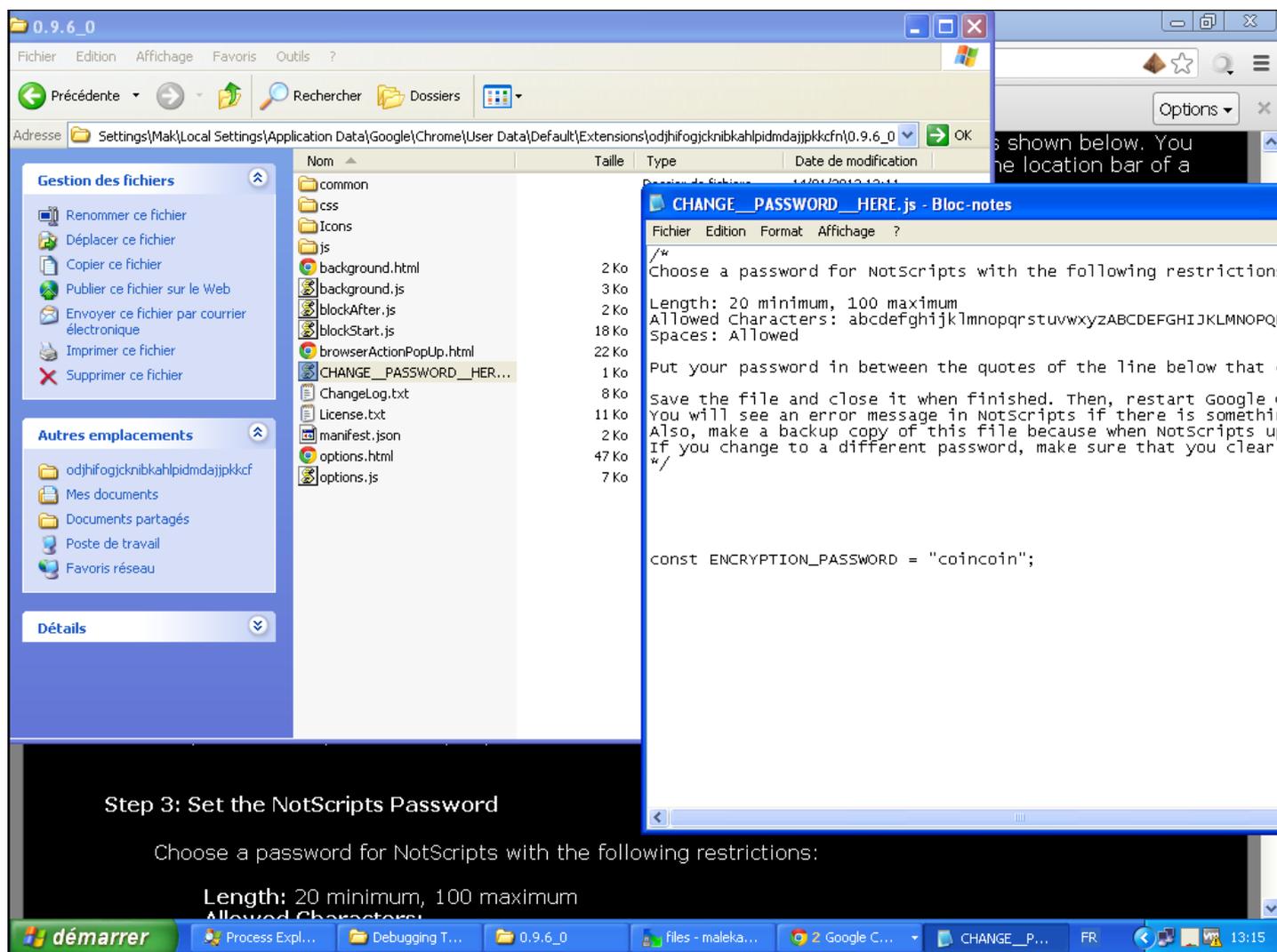


<https://chrome.google.com/webstore/detail/scriptsafe/oigbmnaadbkfbmpbfijflahbdbgdgdf> La gestion des scripts se fait à partir de l'icône rouge de blocage en haut à droite.



L'extension NoScript : <https://chrome.google.com/webstore/detail/notscript/odjhifogjcknibkahlpidmdajppkfcfn>

Après l'installation, une page s'ouvre vous expliquant que vous devez éditer le fichier CHANGE_PASSWORD_HERE.js pour ajouter un mot de passe sur la ligne const ENCRYPTION_PASSWORD = »;



puis relancez [Google Chrome](#) et l'extension est active.

Vous pouvez gérer l'activation des scripts et liste blanche avec l'icone pyramide à droite des adresses des sites consultés.



uMatrix

uMatrix est une autre extension très efficace et paramétrable pour bloquer le contenu des pages WEB, publicités et autres.

Cette extension est plus complexe et plutôt destinée à des utilisateurs avancés qui aiment bien tout contrôler.

[Lire le tutoriel uMatrix](#)

Adblock

[Adblock](#) est une extension qui permet de bloquer les publicités :



<https://chrome.google.com/webstore/detail/adblock/gighmmpiobkifepjocnamgkbbigidom?hl=>

A lire : [le tutoriel Adblock](#)

ATTENTION :

Certains sites abusent des publicités, dont leurs pages peuvent en être inondées (cela ralentit la navigation etc). Mais notez que les publicités sont parfois le seul revenus des sites WEB. Filtrer toutes les publicités peuvent, par exemple, pénaliser ces sites, c'est notamment le cas de malekal.com

Si vous pensez que certains sites n'abusent pas et méritent leurs revenus, n'hésitez pas à les ajouter dans la liste blanche pour ne pas les pénaliser.

uBlock

uBlock permet de bloquer les publicités et des services de pistages utilisateurs à travers des listes fournis. uBlock peut aussi bloquer des sites malicieux.

Pour plus d'informations lire : [Tutoriel uBlock](#)

Quelques extensions en vrac

- [View Thru](#) : permet de visualiser le contenu des liens courts sans cliquer dessus!
- [Secure Profile](#) : permet de sécuriser son profil Chrome et notamment vos mots de passe, plus d'informations sur cet aspect : [Mots de passe sur les navigateurs WEB](#)

Plus loin dans la sécurité de son PC

Contre les [exploits sur site web](#), Maintenez ses logiciels à jour : [Logiciels pour maintenir ses programmes à jour](#).

Éventuellement, vous pouvez installer [Malwarebytes Anti-Exploit](#) pour bloquer les [Exploits sur Site WEB](#).

Pour aller plus loin, Sécuriser son ordinateur : [Sécuriser Windows gratuitement](#)

Liens Google Chrome

Et si vous souhaitez booster votre [Google Chrome](#), rendez-vous sur la page [Optimiser Google Chrome et Firefox](#)

Pour plus d'informations sur le fonctionnement de Chrome, se reporter à son tutoriel : [Tutoriel Google Chrome : comment utiliser Google Chrome](#)

