Sécuriser votre navigateur Internet Explorer

malekal.com/securisez-votre-navigateur-internet-explorer-2/

malekalmorte 12/11/2010

Internet Explorer est un composant intégré à l'environnement Windows, l'explorateur de fichiers utilisent des composants d'Internet Explorer, Outlook Express et Windows Media Player aussi. Changer des paramètres affectent aussi ces programmes. Faites donc attention aux modifications que vous faites.

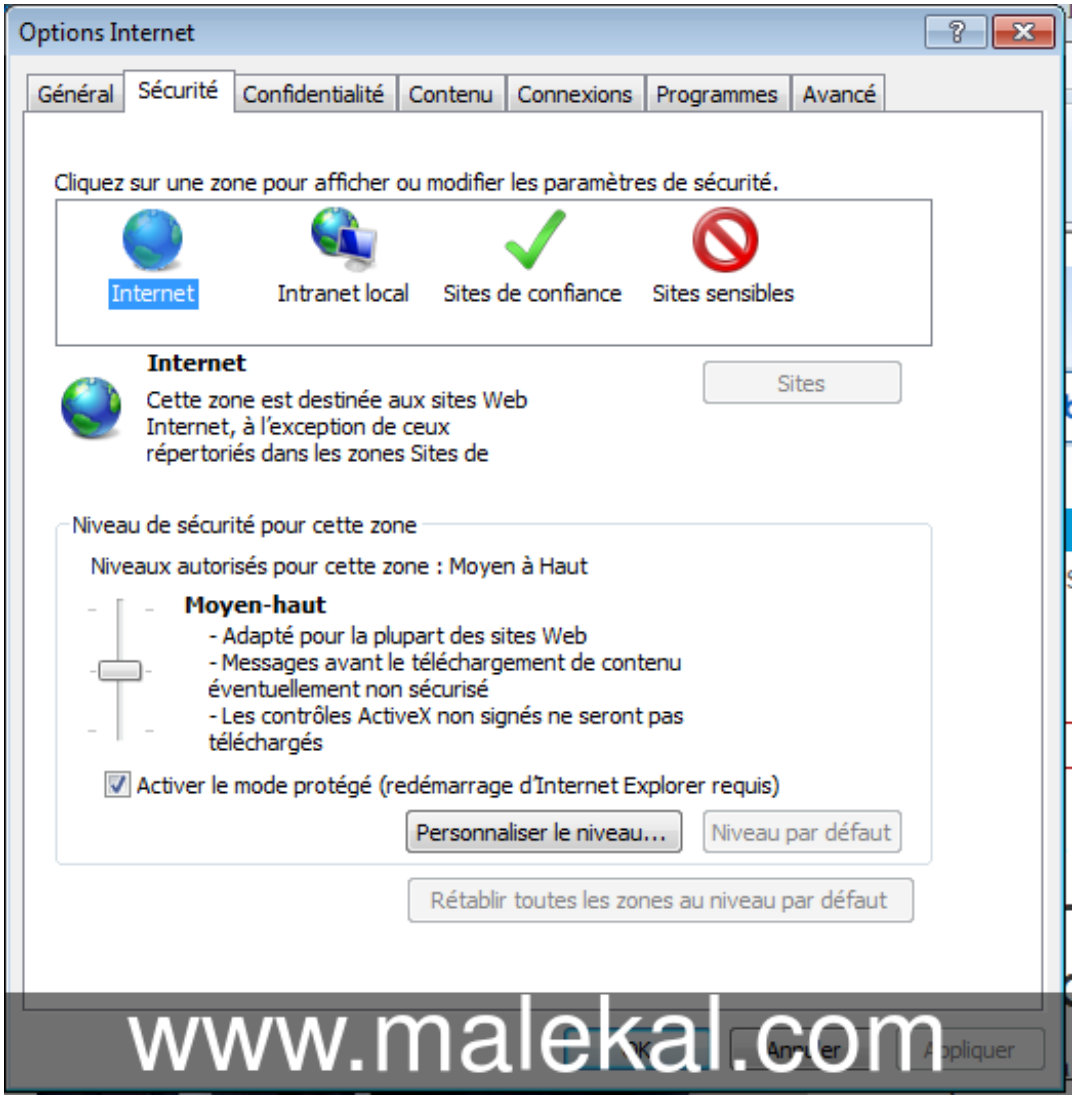
Régulièrement, des failles de sécurités pour Internet Explorer sont publiées, ne pas installer les correctifs rendent les programmes utilisant des composants d'Internet Explorer vulnérables.

Voici un article qui va vous aider à configurer Internet Explorer pour le rendre plus sécurisé.

Table des matières [masquer]

Utiliser des Zones de Sécurité

Les zones de sécurités sont la première défense dans Internet Explorer. Il existe 4 zones :



- **Intranet local** – Tous les sites qui font partis du réseau local. En général, on donne un haut niveau de confiance.
- **Sites de confiances** – Ce sont les sites auquels vous avez donnés confiance. Par défaut, la liste est vide, c'est à vous d'en ajouter.
- **Sites sensibles** – Ce sont les sites auquels vous n'avez pas confiance. Par défaut, la liste est vide.**Internet** – Le reste

Il existe une cinquième zone celle de votre ordinateur (My Computer), elle est par défaut non configurable. Les contrôles ActiveX qui sont installés sur votre ordinateur par Windows fonctionnent dans cette zone. Les sites qui référencent des fichiers de votre ordinateur fonctionnent aussi dans cette zone, les fichiers que vous sauvez d'internet continue de fonctionner dans la zone de sécurité attachée à ce site.

Concrètement : Si vous téléchargez un programme comme Adobe Acrobat, vous téléchargez son programme d'installation. Lorsque vous executez ce fichier, celui-ci tournera dans la Zone internet (sauf si vous avez mis Adobe dans la zone restreinte ou zone de confiance). Une fois le programme installé, lorsque vous allez démarrer Acrobat, celui-ci fonctionnera dans la zone My Computer. Si Adobe installe un fichier qui est ouvert par Internet Explorer, par exemple ReadMe.html, celui-ci fonctionnera aussi dans la zone My Computer.

Dans Windows XP SP2, cette zone est maintenant une zone de haute sécurité. N'importe quelle entité qui utilise un Active Scripting ou qui charge des contrôles ActiveX est interdit sauf si l'utilisateur l'a explicitement permis en cliquant sur la barre d'information. Comme cela peut interférer avec des applications WEB fonctionnant dans un réseau local, les developpeurs peuvent ajouter une « Mark of the Web » pour faire fonctionner les fichiers dans la zone intranet local au lieu de la zone My Computer ». Pour plus d'informations, consultez http://msdn.microsoft.com.

Pour assigner une zone à un site, ouvez les options internet dans les menu d'Internet Explorer ou dans le panneau de configuration.

Par exemple, sur le site malekal.com, les pubs provenant de sites extérieures :

On ajoute le site en zone sensible :

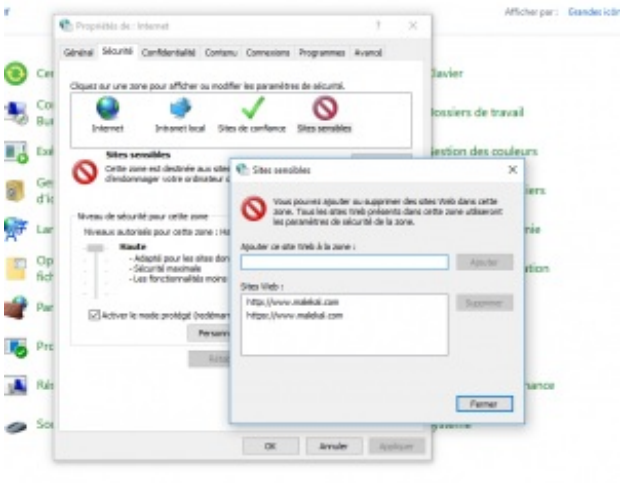
Les éléments extérieures ne sont plus chargés :

Ainsi, si un Javascript tente d'appeler un site externe, ce dernier ne sera pas chargé.

Attention Microsoft Edge ne respecte pas les zones internet

La zone intranet local inclus :

- Tous les sites qui ne sont pas assignés à une autre zone.
- Tous les sites qui outrepassent le proxy dans le cas d'un réseau qui utilisent un proxy
- Tous les fichiers ouverts par un UNC (ex: \192.168.1.2) ou ouvert par le réseau



Pour supprimer une ou plusieurs de ces catégories de l'intranet local, sélectionnez Intranet local dans l'onglet « sécurité » des « options internet », cliquez ensuite sur « Sites… ». Décochez la catégorie qui vous intéresse et cliquez sur OK

Ajouter ou supprimer un site d'une zone

Sélectionnez la zone qui vous intéresse et cliquez sur « Sites… ». Tapez ou copier coller l'adresse du site dans le champs « Ajouter un site dans à cette zone » et cliquez sur le bouton « Ajouter ». Le site apparaît alors dans la liste « Site Web ».
Pour supprimer un site, sélectionnez le dans la liste et cliquez sur le bouton « Supprimer »

Notes:

- Internet Explorer gère le protocole http. Entrez www.google est équivalent à http://www.google.com
- « Requiert un serveur sécurisé (https) pour toute la zone » oblige la zone à utiliser des sites sécurisés par le protocole SSL. Cette option est activée dans la zone de confiance. Vous pouvez mixer les sites SSL et non SSL en décochant l'option lorsque vous vous connectez à un site.
- Saisir un site avec une page, ajoute le site en entier dans la zone. Par exemple, saisir http://www.bbc.co.uk/doctorwho/characters/index.shtml ajoutera http://www.bbc.co.uk à la liste.
- Si vous saisissez une adresse IP directement n'est pas équivalent à saisir l'adresse du site. www.google.com est différent de 216.239.63.104.
- Pour déplacer un site d'une zone à une autre, vous devez supprimer le site de la zone et l'ajouter dans la nouvelle zone.

Conseil: Surveillez votre zone de confiance régulièrement. Les programmes peuvent ajouter des sites dans la zone de confiance et donnera des pouvoirs à ce site que vous ne voulez pas.

Créer votre propre zone de sécurité

Il se peut que les zones par défaut ne correspondent pas à vos besoin, vous pouvez alors créer votre propre zone. Internet Explorer ne permet pas de le faire, mais vous pouvez le faire facilement par la base de registre. Si vous n'avez aucune expérience de la base de registre : Tutoriel sur la base de registre Windows

La clef des zones est : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones.
Les sous-clefs sont :

0) MyComputer
1) Intranet local
2) Sites de confiances
3) Internet
4) Sites sensibles

Le plus simple pour ajouter une nouvelle zone est d'exporter une des sous-clefs à partir de regedit, la changer et enfin la réimporter.

1. Si vous êtes sous Windows XP, utilisez la restauration du système pour créer un nouveau point de restauration.
2. Ouvrez l'éditeur du registre et rendez-vous à la clef HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zone\2. Le mieux est de cloner la zone 2 (Trusted sites) et la zone 4 (Restricted Sites). Les autres zones peuvent avoir des propriétés qui ne vous intéressent pas.
3. Cliquez sur Fichier, Exporter, saisissez un nom de fichier .reg puis fermez l'éditeur du registre.
4. Localisez le fichier que vous avez enregistré puis faites un clic droit sur la souris dessus. Choisissez « Editer » pour l'ouvrir dans un éditeur de texte (par défaut le Bloc-Note).Vous devriez avoir quelque chose approchant à ceci :

```
REGEDIT4 [HKEY_CURRENT_USER\Software\Microsoft\Windows\Current\Version\Internet
Settings\Zones\4]
« 1400 »=dword:00000003
@= » »
« DisplayName »= »Restricted sites »
« Description »= »This zone contains Web sites that can possibly damage you computer or data. »
« Icon »= »inetcpl.cpl#00004481 »
« CurrentLevel »=dword:00000000
« MinLevel »=dword:00012000
« RecommendedLevel »=dword:00012000
« Flags »=dword:00000003
« 1001 »=dword:00000003
« 1004 »=dword:00000003
« 1200 »=dword:00000003
« 1201 »=dword:00000003
« 1402 »=dword:00000003
« 1405 »=dword:00000000
« 1406 »=dword:00000003
« 1407 »=dword:00000003
« 1601 »=dword:00000001
« 1604 »=dword:00000001
« 1605 »=dword:00000000
« 1606 »=dword:00000003
« 1607 »=dword:00000003
« 1800 »=dword:00000003
« 1802 »=dword:00000003
« 1803 »=dword:00000003
« 1804 »=dword:00000003
« 1805 »=dword:00000001
« 1A00″=dword:00010000
« 1A02″=dword:00000003
« 1A03″=dword:00000003
« 1C00″=dword:00000000
« 1E05″=dword:00010000
« {AEBA21FA-782A-4A90-978D-B72164C80120} »=hex:1a,37,61,59,23,52,35,0c,7a,5f,20,
17,2f,1e,1a,19,0e,2b,01,73,13,37,13,12,14,1a,15,39
« 1A10″=dword:00000003
« {A8A88C49-5EB2-4990-A1A2-0876022C854F} »=hex:1a,37,61,59,23,52,35,0c,7a,5f,20,
17,2f,1e,1a,19,0e,2b,01,73,13,37,13,12,14,1a,15,39
« 1608 »=dword:00000003
« 1609 »=dword:00000001
« 1A04″=dword:00000003
« 1A05″=dword:00000003
« 1A06″=dword:00000003
« 1206 »=dword:00000003
« 2001 »=dword:00000003
« 2004 »=dword:00000003
```

5. Editez commençant par [HKEY_CURRENT_USER et changer 4 à 5 à la fin de la ligne. Vous pouvez utiliser n’importe quel numéro.

6. Editez « DisplayName » (nom de la zone) et « Description » comme vous le souhaitez.
7. Changez « Icon » pour ce que vous voulez. C'est l'icône qui apparaîtra dans les options internet.
8. Editez « MinLevel » et « RecommendedLevel ». MinLevel est le niveau de sécurité le plus bas que vous pouvez affecter à la zone sans qu'un message apparaîsse. RecommendedLevel sont les paramètres par défauts qui seront affectés lorsque vous cliquerez sur le bouton « Level par défaut ».Les valeurs possibles sont :

   dword:00010000 Low
   dword:00010500 Medium-low
   dword:00011000 Medium
   dword:00012000 High

9. Editez les lignes Flag. Ce sont les différentes propriétés de la zone. Pour affecter une valeur de Flag, ajoutez une valeur ci-dessous et convertissez le en hexadecimal (voir plus bas).Les valeurs possibles sont :1 (0x01) Allow changes to custom settings
   2 (0x02) Allow users to add sites to the zone
   4 (0x04) Require https protocol
   8 (0x08) Include sites that pass the proxy server
   16 (0x10) Include sites not listed in other zones
   32 (0x20) Do not show this zone in the Internet Options dialog
   64 (0x40) Include the « Require Server verification (https:) for all sites listed in this zone » checkbox
   128 (0x80) Treat UNC paths as Intranet connections.

   Les notations entre parenthèses sont en hexadecimal.Exemple, pour créer une zone qui vous permet d'ajouter des sites et que vous pouvez personnaliser, vous devez créer le « Flags » dword:00000003Le plus simple pour convertir une valeur hexadecimal en décimal et d'utiliser la calculatrice Windows. Démarrer la calculatrice (Démarrer/Tous les programmes/Accessoires/Calculatrice) et activer le mode scientifique. En haut à gauche de la fenêtre, vous avez 4 boutons (Hex, Dec, Oct, Bin). En cliquant dessus, la valeur sera convertie.

10. Sauvez le fichier édité puis double-cliquez dessus pour importer la nouvelle zone dans la base de registre.

Vous pouvez ensuite ajuster la zone dans les options Internet.

Configurer les niveaux de sécurités

Il existe 4 configurations de zones par défauts :

- Intranet Local – Moyen-bas
- Site de confiances – Bas
- Site sensibles – Haut
- Internet – Moyen

Vous pouvez changer personnaliser les niveaux en faisant glisser de haut en bas le bouton « Niveau de sécurité de la zone ». Si vous ne voyez pas de bouton que vous pouvez faire glisser, c'est que le niveau a été personnalisé. Pour le faire réapparaître, cliquez sur le bouton « Niveau par défaut ».

Vous noterez que le niveau par défaut de la zone de confiance est plus haut que la zone intranet local…. donc ne mettez dans la zone de confiance que les sites dont vous avez plus confiance à ceux de votre intranet!

Pour changer les options d'une zone, cliquez sur le bouton « Personnaliser le niveaux » puis cochez les options dans la nouvelle fenêtres.

Utiliser le contrôle parental

Parce qu'internet est incontrôlable, il peut contenir des choses qui peuvent choquer. Le contrôle parental n'est pas forcement destiné aux parents qui veulent protéger leurs enfants, il peut être utilisé par n'importe qui, pour se protéger de certains contenus d'internet.

- Tutoriel sur le Contrôle Parental Windows et autres
- Sur Windows 10 : Windows 10 : le contrôle parental

ActiveX

ActiveX est une ancienne technologie, aujourd'hui abandonnée.

Supprimer un controle ActiveX

Il est tentant de supprimer un contrôle en cliquant sur supprimer depuis le dossier Downloaded Program Files\, cela ne désinstallera pas le control. Cela suprimera les fichiers .ocx/dll mais pas les modifications de la base de registre. Lorsque vous irez sur le site d'où le contrôle vient, Internet Explorer plantera, parcequ'il trouvera le contrôle dans la base de registre mais pas sur le disque! Si vous désirez supprimer un contrôle ActiveX, ouvrez ajout/suppression de programmes pour voir si vous pouvez le désinstaller.

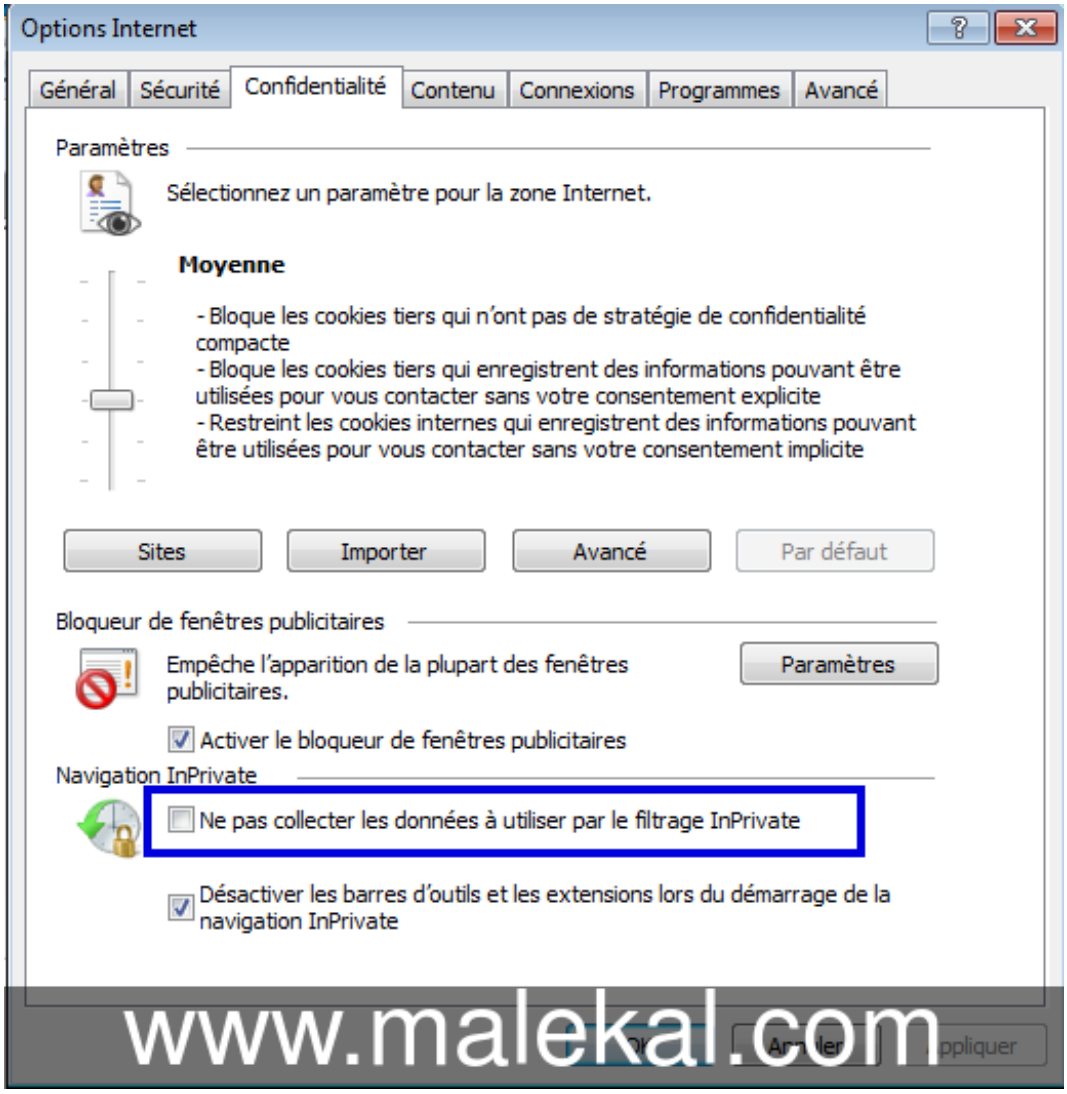
Les propriétés des contrôles ActiveX

En faisant un clic droit sur un contrôle, vous pouvez cliquer sur le bouton propriétés pour obtenir des informations. Dans l'onglet général, vous pouvez voir si c'est une applet java ou un controle activeX (Type) et où vous avez téléchargé le controle (CodeBase). Internet Explorer utilise les zones de sécurités auquel le site (CodeBase) à partir duquel le contrôle a été téléchargé. Notez que dans le cas où le CodeBase est différent du site à partir duquel vous avez télécharge le contrôle, Internet Explorer appliquera les restrictions de sécurités les plus fortes.

L'onglet version permet de savoir à quel éditeur appartient ce controle.
L'onglet Dépendances indentifie les fichiers utilisés par le composant.

Activer InPrivate

Pour empêcher le Tracking WEB, vous pouvez activer InPrivate.
L'option disponible depuis le menu Outils et Options Internet.
Onglet Confidentialité.



Plugins Adobe PDF

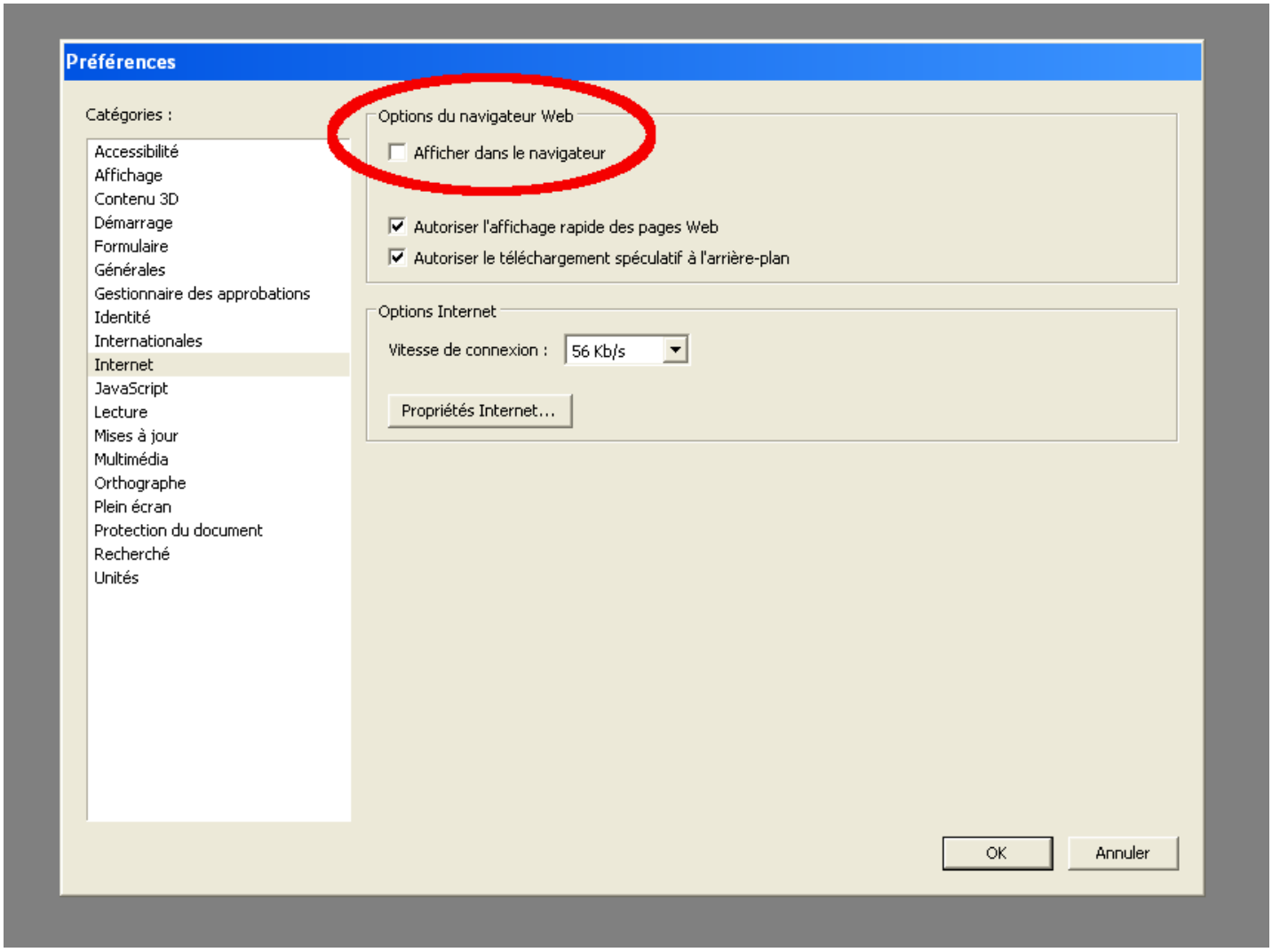
Dans un premier temps, pour comprendre le fonctionnement des plugins, vous pouvez lire la page : Plugin Flash, Java, Silverlight etc sur les navigateurs WEB

Depuis quelques mois, les auteurs de malwares tirent parti des vulnérabilités sur les plugins des navigateurs WEB pour infecter les PC.
Se reporter à la page Exploitation SWF/PDF et Java – système non à jour = danger

Pour sécuriser votre PC, vous pouvez désactiver le JavaScript dans Acrobat Reader, se reporter à la page suivante :

Vous pouvez désactiver l'ouverture automatique des PDF, pour cela :

1. Télécharger le fichier suivant : Desactiver_PDF.reg
2. Double-cliquer dessus et accepter l'inscription des données
3. Ouvrer Adobe Reader
4. Cliquer sur le menu *Edition*
5. Cliquer sur *Préférences*
6. Cliquer sur la section *Internet*
7. Décocher l'option *Affcher dans le navigateur*

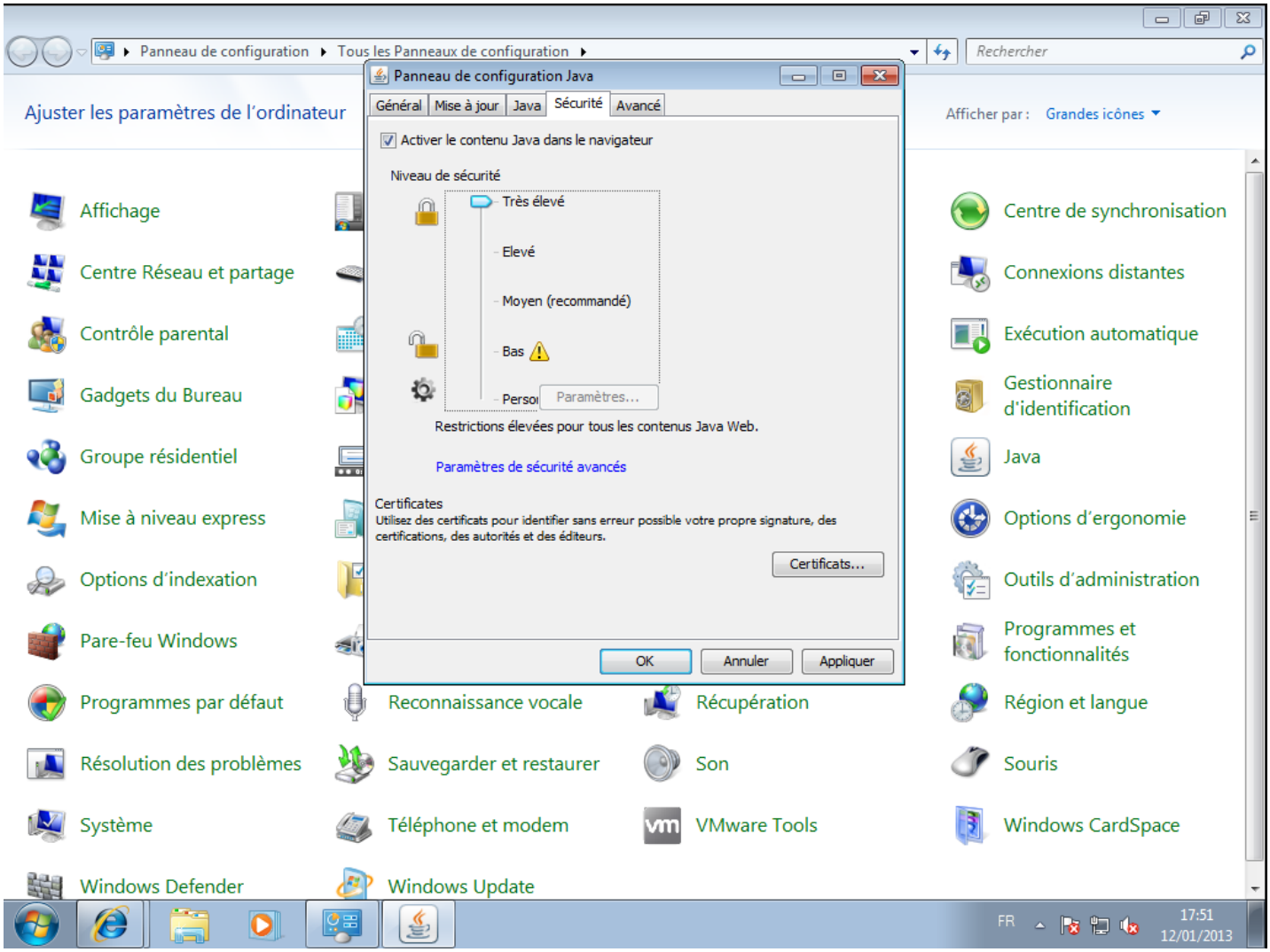


Plugin Java

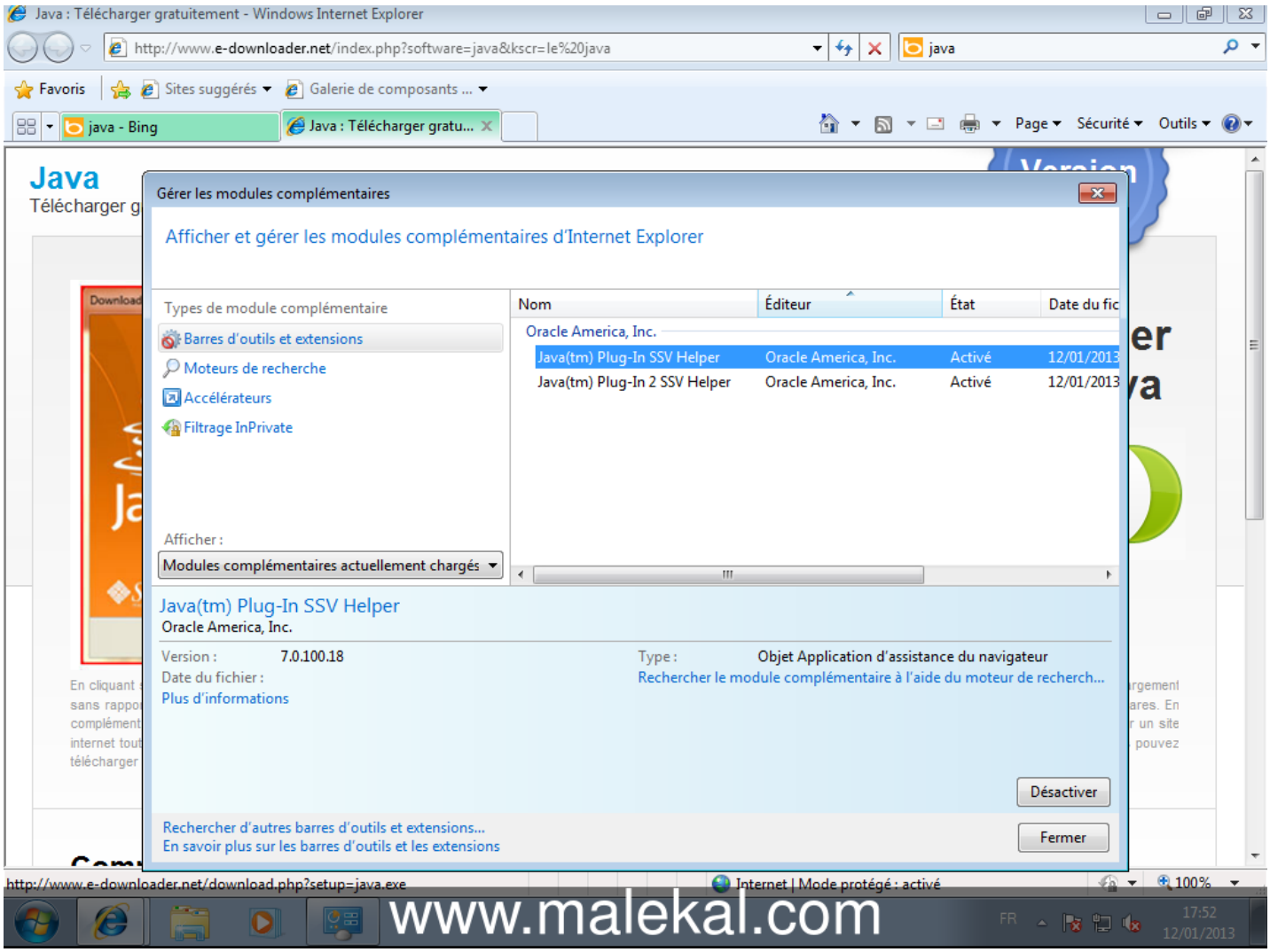
Java est aussi une extension qui est très utilisée dans les Exploits sur Site WEB.

Vous pouvez renforcer la sécurité en augmentant le niveau de sécurité de Java.
Cela se fait dans le Panneau de Configuration puis Java.
Onglet Sécurité, élevez le niveau à très élevé.

Vous pouvez aussi désactiver Java dans le navigateur WEB, si vous en avez pas besoin, en décochant l'option Activer le contenu Java dans le navigateur.



Vous pouvez carrément désactiver Java dans Internet Explorer.
Cela se fait depuis le menu Outils / Modules Complémentaires.
Dans Barres outils et extensions, sélectionnez Java puis cliquez sur Désactiver.



Les risques liés au stockage des mots de passe

Pour comprendre les risques liés au stockage des mots de passe des sites sur les navigateurs WEB.
=> Mots de passe sur les navigateurs WEB

Malwarebytes Anti-Exploit : Bloquer les Exploits WEB

Éventuellement, vous pouvez installer Malwarebytes Anti-Exploit pour bloquer les Exploits sur Site WEB.

Sécuriser son PC

Pour aller plus loin dans la sécurité de son PC, se reporter à la page : Sécuriser son ordinateur