Eviter une attaque virale : les bons réflexes pour sécuriser votre ordinateur

Date de dernière mise à jour : 29/04/2014 à 19:17

En posant la question suivante : "qui n'a jamais eu de virus sur son ordinateur ?" je suis presque certain d'obtenir très peu de mains levées. Et pour cause, les virus sont de plus en plus malicieux, et l'usage de l'informatique beaucoup plus grand qu'auparavant.

L'**infection virale** peut avoir des conséquences dévastatrices pour votre ordinateur voire votre entreprise :

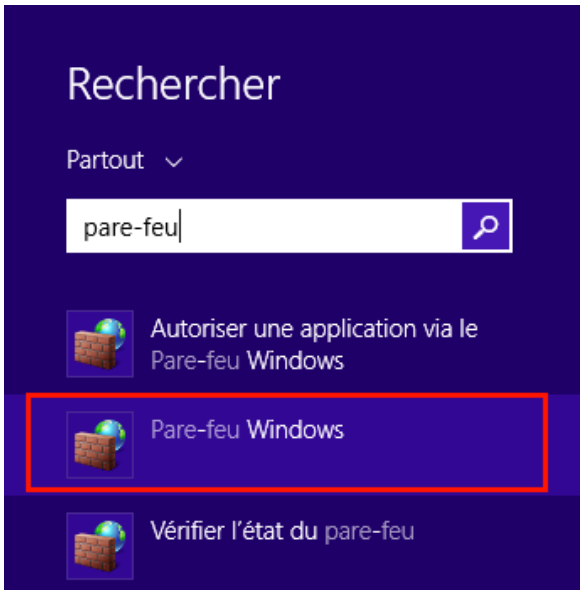
Mauvais fonctionnement de la connexion réseau
Mauvais fonctionnement de l'ordinateur- (blocages, etc.)
Perte de données

Pour éviter de se faire contaminer, certaines règles simples s'imposent.

Cette page à pour but de vous faire éviter le piratage ou la contamination de votre PC par des règles simples :

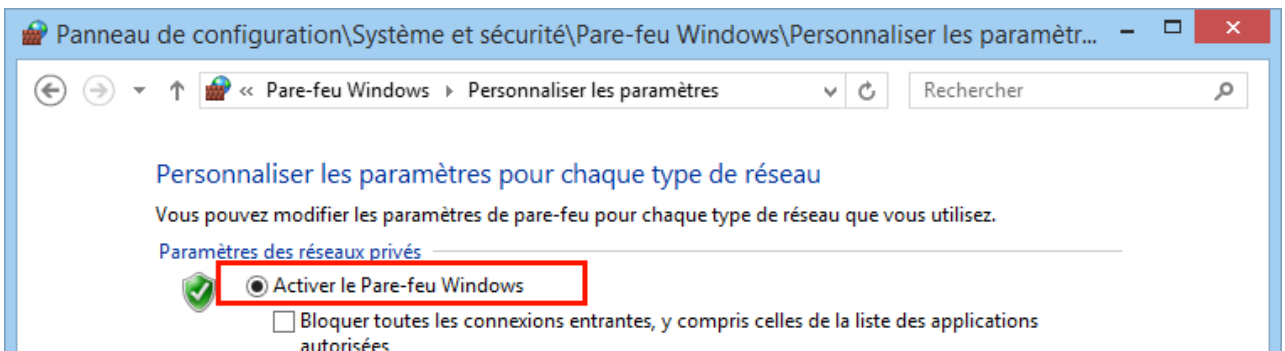
Installez un pare-feu
Windows XP (SP2 et SP3), Windows 7 et Windows 8 intègrent nativement un pare-feu (firewall). Prenez le soin de toujours l'activer. Pour activer le firewall, suivez la procédure suivante :

Activer le pare-feu de Windows 8



Placez-vous sur l'interface **Metro** puis tapez **pare-feu**. Cliquez ensuite sur **Pare-feu Windows**. Cliquez ensuite à gauche sur **Activer ou désactiver le pare-feu Windows**.

Pour chacun des types de connexions disponibles, sélectionnez **Activer le pare-feu Windows**, puis validez.

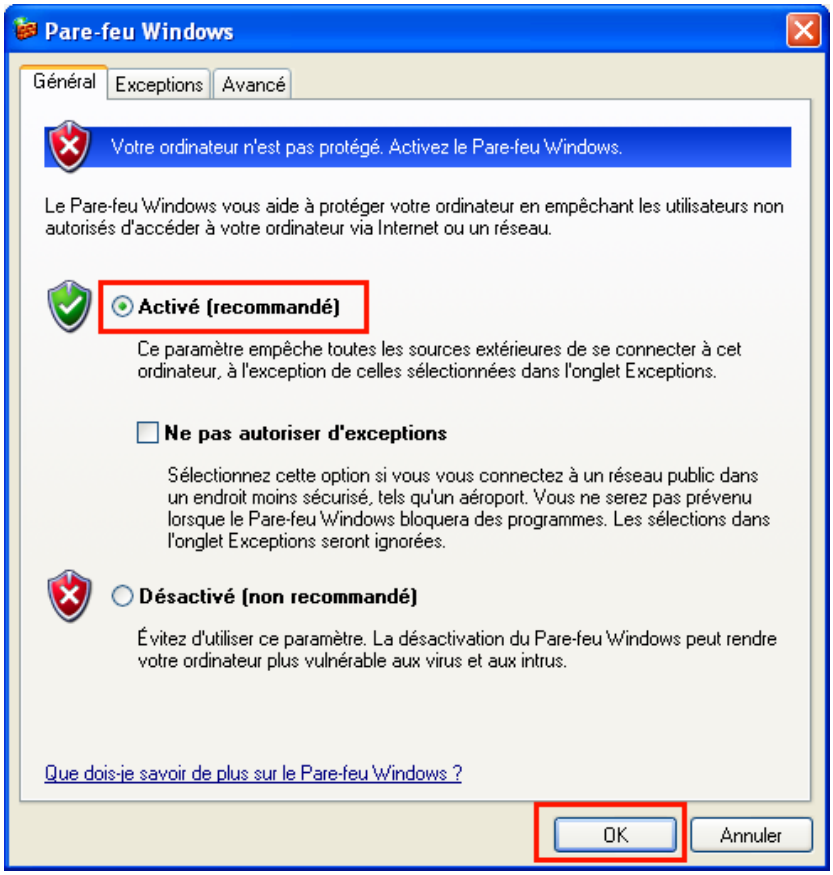


Activer le pare-feu Windows

Activer le pare-feu de Windows 7
Cliquez sur le bouton Windows, puis sur sur **Panneau de configuration => Sécurité => Pare-feu Windows**.

Cliquez sur **Activer ou désactiver le Pare-feu Windows => Activer le pare-feu Windows** et validez.

Activer le pare-feu de Windows XP
Cliquez sur **Démarrer => Panneau de configuration => Pare-feu Windows**. Sélectionnez ensuite l'option **Activé**.



Activer le pare-feu sur Windows XP

N'ouvrez pas les emails douteux (Phishing)
Si vous recevez un mail douteux, ne l'ouvrez pas, et ne cliquez pas sur les liens du message. En effet, la plupart de ces mails vous sont envoyés par des robots dans le seul but d'infecter votre machine et/ou de vous dérober vos informations personnelles (informations bancaires, état civil, etc.).

Si par mégarde vous avez cliqué sur le lien contenu dans le message, **fermez le navigateur** et faites un scan antivirus. Ne remplissez surtout pas de formulaire vous demandant votre login ou mot de passe.

Le fait de proposer un lien vers un site qui n'est pas réellement celui affiché sur le lien s'appelle du **phishing**.

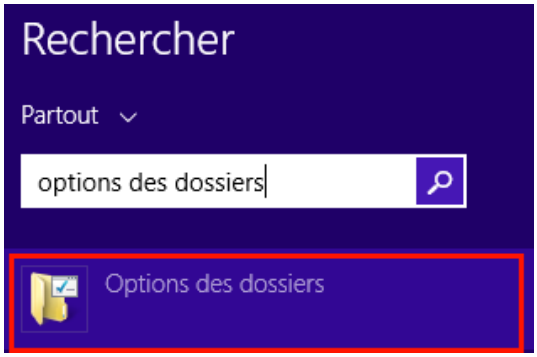
-Méfiez-vous des messages électroniques trop attractifs ou vous promettant monts et merveilles (augmenter la taille de votre pénis, être riche en un mois, etc.).
-Méfiez-vous des messages électroniques rédigés en langue étrangère.

Surveillez vos fichiers

Certains fichiers sont plus dangereux que d'autres. Les malfrats le savent bien, c'est pourquoi, pour mieux vous tromper, ils **renomment la plupart du temps les fichiers en vous faisant croire qu'ils sont inoffensifs**. Par exemple, un pirate peut inclure un fichier exécutable qu'il appellera **image.jpg.exe**. Windows masquant par défaut l'extension du fichier, vous ne verrez plus que la mention **image.jpg** et croirez à tort qu'il s'agit d'une image saine.

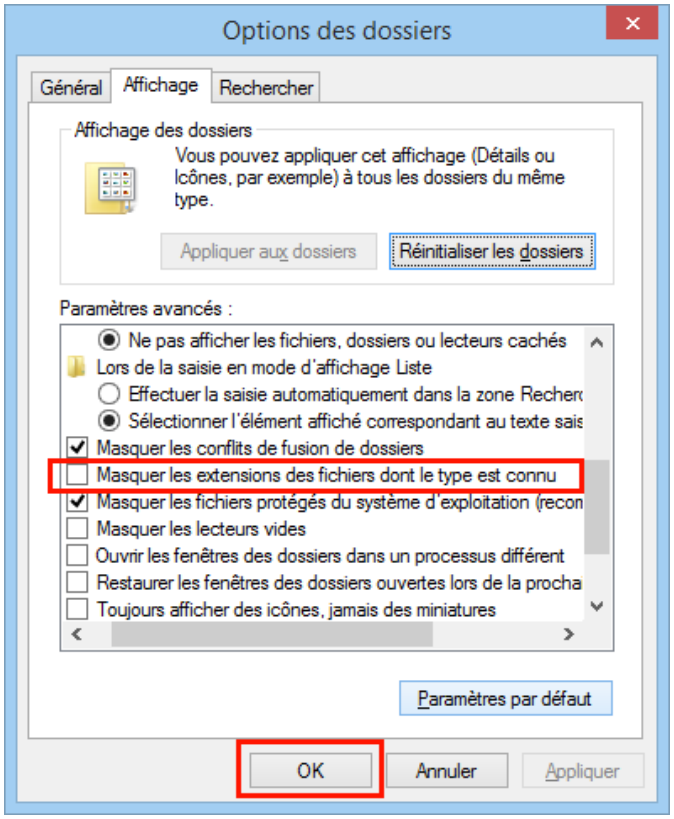
La première chose à faire sous Windows est d'**activer l'affichage complet des extensions de fichiers**.

Afficher toutes les extensions de fichiers sous Windows 8
Sur l'interface Modern UI (Metro), tapez **Options des dossiers** puis cliquez sur le menu du même nom.



Options des dossiers

Cliquez sur l'onglet **Affichage** puis décochez la case **Masquer les extensions des fichiers dont le type est connu**. Validez.



Ne plus masquer les extensions connues

Afficher toutes les extensions de fichiers sous Windows 7
Cliquez sur le bouton **Démarrer** puis sur **Panneau de configuration => Apparence et personnalisation => Options des dossiers**. Cliquez sur

l'onglet **Affichage** puis décochez la case **Masquer les extensions des fichiers dont le type est connu**. Validez.

Quelles sont les extensions dangereuses ?
Voici une petite liste des extensions dangereuses :

-.exe (fichier exécutable)
-.com (fichier exécutable)
-.bat (script Windows)
-.vbs (script Visual Basic)
-.scr (écran de veille)
-.dll (librairie)
-.cmd (fichier de commandes)
-.swf (fichier Flash, ce programme est régulièrement la cible des pirates)

Lorsque vous recevez un email douteux, n'ouvrez jamais une pièce jointe portantl'une de ces extensions.
D'autre part, soyez prudent avec les fichiers **.doc, .xls et .pps**. Ces documents sont susceptibles de contenir des **virus macro**. En revanche, les fichiers textes (*.txt), ou image (.jpg, .gif, .bmp, etc) sont inoffensifs.

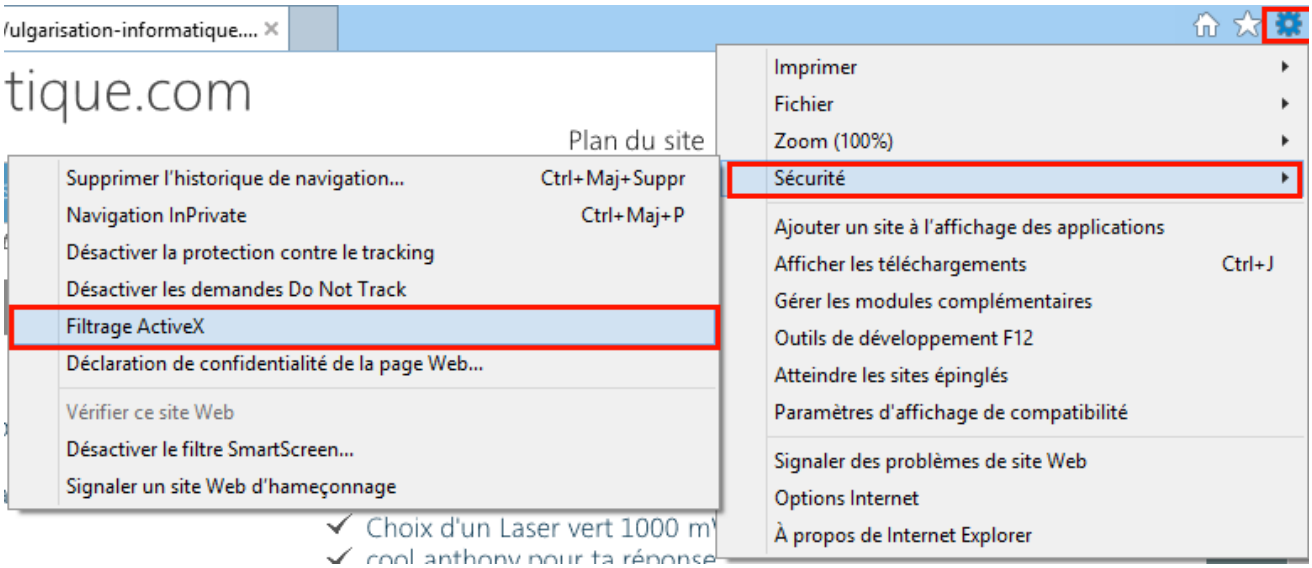
Sécurisez votre navigateur Web
Principal vecteur de propagation des virus, Internet est devenu au fil du temps accessible à tous. Faites attention où vous surfez, et sécurisez votre navigateur. Internet Explorer dispose de moult fonctionnalités méconnues vous permettant de surfer l'esprit tranquille :

Sécuriser Internet Explorer
Certains sites web se servent de **contrôles activeX**, qui sont des programmes incorporés aux pages web pour afficher des animations, etc. Certains programmeurs peuvent néanmoins y mettre un virus.

Pour éviter cela, vous pouvez demander à internet explorer de **ne pas prendre en charge les contrôles activeX**, ou de vous prévenir lorsque qu'un contrôle activeX se trouve sur la page internet que vous visitez.

Dans internet explorer, cliquez sur la roue dentée puis sur **Sécurité => Filtrage active X**. Constatez que l'option est ensuite bien cochée. Elle le restera tout le temps, jusqu'à ce que vous la décochiez.

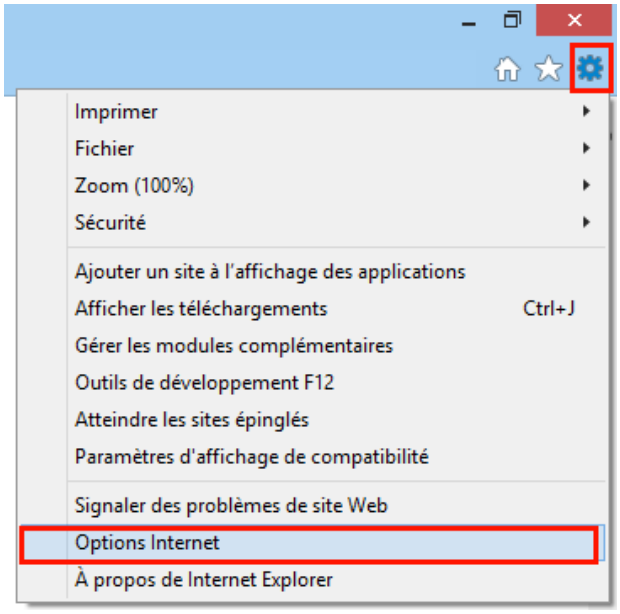
Attention au contenu Flash et Java de certains sites web qui ne sera plus visible ! vous pourrez alors décocher la case sur les sites posant problème.



Filtrage activeX

De cette manière, les contrôles activeX ne seront plus affichés.

Dans internet explorer, cliquez sur la roue dentée puis sur **Options internet** (sur les vieilles versions d'IE, cliquez sur **Outils => Options Internet**.



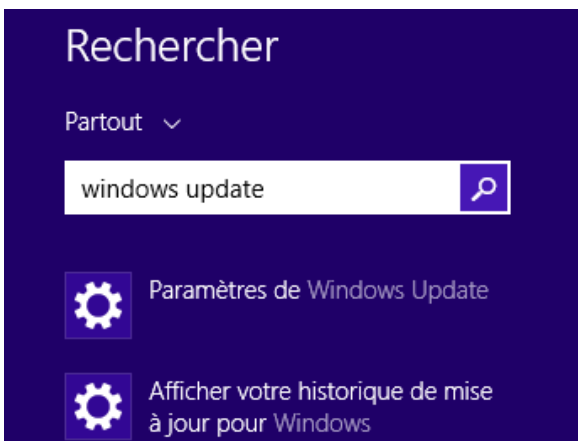
Options Internet

Cliquez sur l'onglet **Sécurité** puis sur **Personnaliser le niveau**. Dans la section **Contrôles ActiveX et plug-ins**, procédez de l'une des façons suivantes :

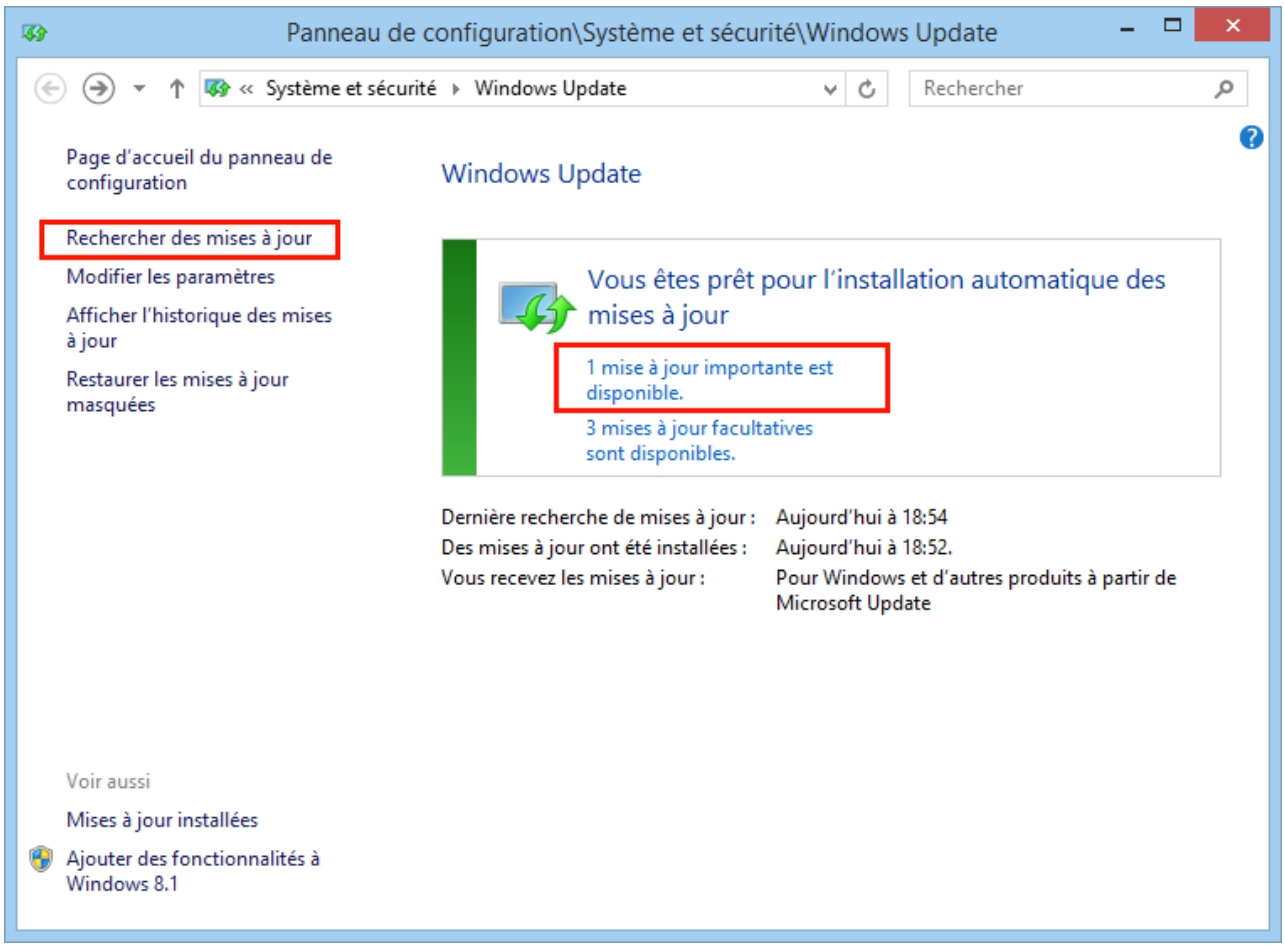
Autoriser le filtrage activeX- : sélectionnez **Activer**-.
Autoriser les contrôles activeX précédemment inutilisés à s'exécuter sans confirmation- : **Désactiver**-.
Autoriser uniquement les domaines approuvés à utiliser les contrôles activeX- : **Activer**-.
Contrôles activeX reconnus sûrs pour l'écriture de scripts- : **Activer**-.
Demander confirmation pour les contrôles activeX- : **Activer**-.
Exécuter le logiciel anti-programmes malveillants sur les contrôles activeX- : **Activer**-.
Exécuter les contrôles activeX et les plugins- : **Activer**- (si vous désactivez cette option, vous surferez en sécurité mais ne verrez plus le contenu Flash et Java de certains sites internet. À vous de choisir !)
Télécharger les contrôles activeX non signés- : **Désactiver**-.
Télécharger les contrôles activeX signés- : **Demander**-.

Mettez à jour Windows régulièrement
Installez régulièrement les patchs de sécurité de windows. Ceux-ci vous garantiront que votre système est doté des dernières protections contre les failles de sécurité et les programmes malicieux.

Mettre à jour Windows 8
Sur l'interface Metro, tapez **Windows Update** puis cliquez sur l'icône du même nom :

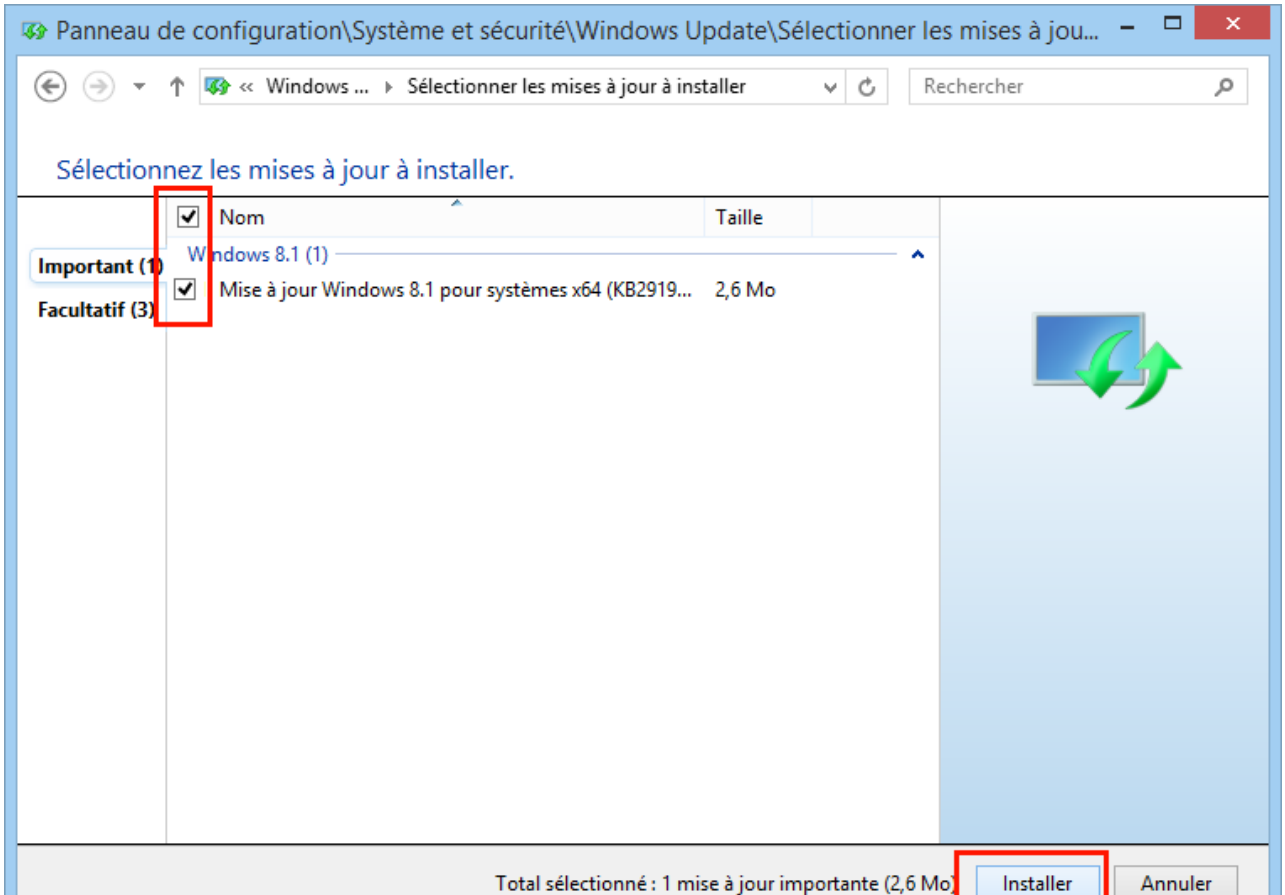


Cliquez sur **Rechercher des mises à jour** puis, si des mises à jour sont trouvées, cliquez sur le lien vous indiquant qu'elles sont disponibles :



Des mises à jour sont disponibles ...

Cochez les cases et cliquez sur **Installer** :



Choix et installation des mises à jour

Mettre à jour Windows 7

La procédure est sensiblement la même que sous Windows 8, sauf que vous devez passer par le **Panneau de configuration => Système et sécurité => Windows Update**

Mettre à jour Windows XP

Depuis le mois d'avril 2014, Windows XP n'est plus supporté par Microsoft. Les mises à jour ne sont donc plus disponibles. Je vous conseille de suivre drastiquement les conseils de cette page et d'opter pour un antivirus performant (Microsoft Security Essentials n'étant plus maintenu pour XP).

Sauvegardez vos données

Même si la sauvegarde n'empêchera pas les virus d'entrer sur votre machine, en faire régulièrement vous permettra d'être moins tracassé. Faites donc régulièrement des sauvegardes de vos données.

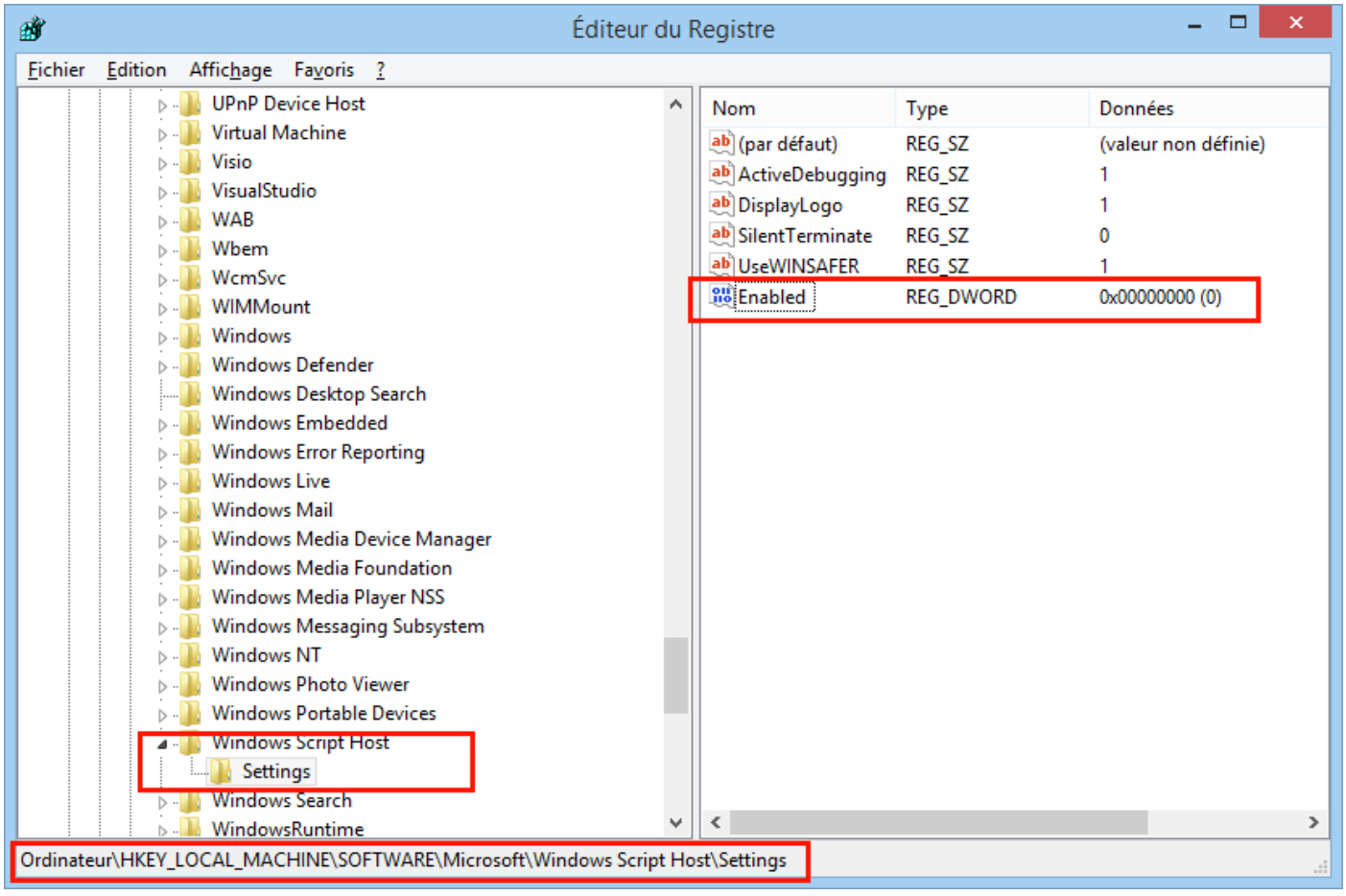
Désactivez VBScript

Visual basic script est un langage de programmation qui permet d'exécuter des macros commandes dans windows (extensions de fichiers **.vbs**. Malheureusement, certains virus se servent de cette fonction (dont on se sert rarement au quotidien).

Pour désactiver cette fonction, cliquez sur les touches
+ R et tapez **regedit**.

Avec Windows 8 et Windows 7

Rendez-vous à la clé **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings**. Recherchez la valeur nommée **Enabled**, et attribuez-lui la valeur . Si elle n'existe pas, créez une valeur DWORD (clic droit => Nouveau => Valeur Dword et nommez-la **Enabled**, puis attribuez-lui la valeur .



Désactiver l'exécution des fichiers vbs