

## Renforcez les défenses de Windows

---

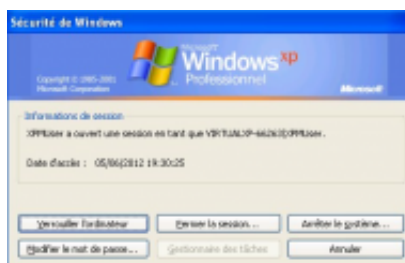
**Sécurisez votre système d'exploitation contre les codes malicieux provenant du réseau et protégez-vous des erreurs de manipulation.**

### **Partagez un dossier sans le rendre visible sur le réseau**

Pour partager un dossier sur le réseau sans pour autant qu'il soit visible de tous, faites un clic droit dessus et allez au menu **Propriétés**. À l'onglet **Partage**, cliquez sur **Partage avancé**. Cochez l'option **Partager ce dossier**. Entrez un nom qui se terminera obligatoirement par le signe « \$ ». Par exemple : *photos\$*. Cliquez sur **OK**. Pour accéder à ce dossier, les utilisateurs du réseau devront saisir son adresse, avec le nom de votre ordinateur suivi de celui de l'élément partagé. Si votre ordinateur se nomme max : \\max\photos\$.

◆ Vista et 7 (niveau 3)

### **Interdisez l'accès au Gestionnaire des tâches**



agrandir la photo

Le Gestionnaire de tâches est un outil à ne pas laisser entre toutes les mains. Pour en bloquer l'accès dans l'éditeur de registre, naviguez jusqu'à **HKEY\_CURRENT\_USER, Software, Microsoft, Windows, CurrentVersion, Policies**. Allez au menu

**Edition, Nouveau** pour créer une **Clé** nommée **System**. Faites un clic droit dans le panneau droit et créez une **Valeur DWORD 32 bits** nommée **DisableTaskMgr** avec une valeur de **1**.

Désormais, les liens vers le Gestionnaire des tâches seront grisés. Pour rétablir l'accès supprimez la clé ou changez sa valeur par **0**.

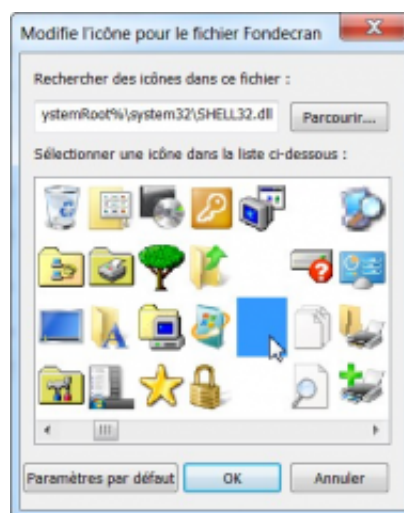
◆ *XP, Vista et 7 (niveau 3)*

## Masquez votre ordinateur dans le réseau

Vous souhaitez que votre ordinateur bénéficie de tous les avantages du réseau tout en restant invisible ? C'est possible. Sur la machine à « cacher », lancez Regedit. Ouvrez les clés **HKEY\_LOCAL\_MACHINE, SYSTEM, CurrentControlSet, Services, LanmanServer, Parameters**. Dans la fenêtre de droite, créez une valeur **DWORD 32 bits** nommée **Hidden** avec en valeur **1**. Redémarrez Windows. L'ordinateur n'est plus visible sur le réseau. Pour y accéder, les autres utilisateurs doivent, dans la zone **Adresse** de la fenêtre **Réseau** ou **Favoris réseau**, taper leur nom précédé de deux barres antislash.

◆ *Vista et 7 (niveau 3)*

## Créez un dossier invisible sur le bureau



agrandir la photo

Créez un dossier et nommez-le avec un espace insécable en maintenant la touche **Alt** et en tapant **0160** sur le pavé numérique. Faites un clic droit sur le dossier et **Propriétés**. Activez l'onglet **Personnaliser** et cliquez sur **Changer d'icône**. Parcourez la liste d'icônes jusqu'à sélectionner une image vide (un blanc dans la liste). Validez par **OK**. Votre dossier sera invisible même si l'option **Afficher les dossiers cachés est activée**. Pour retrouver son emplacement faites **Ctrl + A** sur le bureau.

◆ *XP, Vista et 7 (niveau 1)*

## Affichez l'heure du dernier démarrage

```
C:\Users\SCR>net statistics workstation
Statistiques de station de \\S07-119

Statistiques depuis 06/06/2012 10:55:21

Octets reçus                398324
Blocs SMB reçus             1401
Octets envoyés              381798
Blocs SMB envoyés           1379
Lectures                    118
Écritures                   0
Refus de lectures brutes    0
Refus d'écritures brutes    0
```

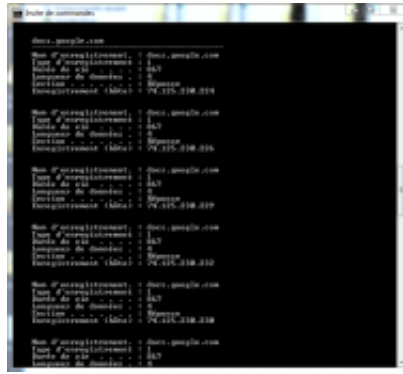


agrandir la photo

Vous souhaitez savoir depuis combien de temps votre fils se sert du PC ? Pressez **Win + R** et saisissez **Cmd**, puis pressez **Entrée**. Tapez **net statistics workstation** et **Entrée**. La ligne **Statistiques depuis** indique la date et l'heure du dernier démarrage de l'ordinateur.

*XP, Vista et 7 (niveau 1)*

## Effacez vos traces de navigation



```
ipconfig /displaydns
Name: www.google.com
Type: A
Address: 64.233.160.101
TTL: 300
Name: www.yahoo.com
Type: A
Address: 98.139.103.100
TTL: 300
Name: www.msn.com
Type: A
Address: 64.233.160.101
TTL: 300
Name: www.google.com
Type: A
Address: 64.233.160.101
TTL: 300
Name: www.yahoo.com
Type: A
Address: 98.139.103.100
TTL: 300
Name: www.msn.com
Type: A
Address: 64.233.160.101
TTL: 300
Name: www.google.com
Type: A
Address: 64.233.160.101
TTL: 300
Name: www.yahoo.com
Type: A
Address: 98.139.103.100
TTL: 300
Name: www.msn.com
Type: A
Address: 64.233.160.101
TTL: 300
```



agrandir la photo

Même si vous prenez soin de vider régulièrement l'historique de votre navigateur, des traces de vos pérégrinations sur le Web subsistent. Pour vous en rendre compte, pressez **Win + R** et tapez **cmd** puis **Entrée**. Dans l'invite de commande, saisissez **ipconfig /displaydns**. Une liste des domaines visités s'affiche. Pour la purger, tapez la commande **ipconfig/flushdns** et pressez **Entrée**.

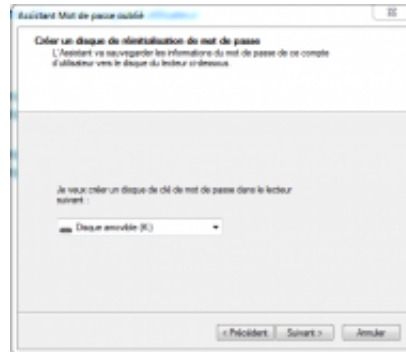
◆ *XP, Vista et 7 (niveau 1)*

## Protégez le Registre

On trouve sur le Web de nombreux fichiers portant l'extension **.reg** qui permettent d'un clic de modifier la base de registre. Si votre ordinateur est utilisé par plusieurs personnes et que vous souhaitez empêcher que ce type de fichier soit exécuté trop facilement, ouvrez le Registre à la clé **HKEY\_CLASSES\_ROOT, regfile, shell**. À droite, double-cliquez sur la clé **(Par défaut)** et saisissez *edit* dans le champ **Données de la valeur**. Validez par **OK**. Désormais, un double-clic sur un fichier **.reg**, l'ouvre dans le **Bloc-Notes**. Pour ajouter les informations qu'il contient au Registre, il faut faire un clic droit dessus et choisir la **Fusionner**.

◆ *XP, Vista et 7 (niveau 3)*

**N'ayez plus peur de perdre votre mot de passe !**



agrandir la photo

Vous avez choisi un mot de passe complexe pour protéger votre session utilisateur, c'est bien, mais pour ne pas risquer d'être bloqué en cas d'oubli, pensez à créer l'utilitaire qui permettra sa réinitialisation. Munissez-vous d'une clé USB et allez dans **Panneau de configuration, Comptes d'utilisateurs** au menu **Créer un disque de réinitialisation**.

◆ *Vista et 7 (niveau 1)*

## **Bloquez les périphériques de stockage USB**

Quand vous branchez un disque ou une clé USB à votre micro, il est immédiatement utilisable. Pour interdire aux utilisateurs de copier sur leurs clés des fichiers de votre disque ou de déposer les leurs, peut-être vérolés, désactivez la détection des périphériques USB dans le Registre. Trouvez la clé **HKEY\_LOCAL\_MACHINE, SYSTEM, CurrentControlSet, Services, USBSTOR**. Dans le volet de droite, double-cliquez sur **Start**. Dans le champ **Données de la valeur**, remplacez **3** par **4** et cliquez sur **OK**. Fermez le Registre et redémarrez le PC. Les périphériques USB sont désormais ignorés. Pour réactiver la détection, il suffit de rétablir la valeur d'origine.

◆ *XP, Vista et 7 (niveau 3)*

## **Activez la diffusion multimédia**



agrandir la photo

Si vous avez plusieurs ordinateurs en réseau ou une console de jeu compatible UPnP, vous pouvez transformer votre PC en serveur multimédia. Lancez Windows Media Player (11 ou 12) et allez au menu **Diffuser en continu**, puis **Activer la diffusion multimédia en continu**. Nommez votre bibliothèque et validez, si besoin, l'accès des différentes machines détectées sur le réseau, puis cliquez sur **OK**. Les fichiers de vos bibliothèques WMP sont maintenant accessibles sur votre réseau local.

◆ Vista et 7 (niveau 2)

## Réglez vos comptes



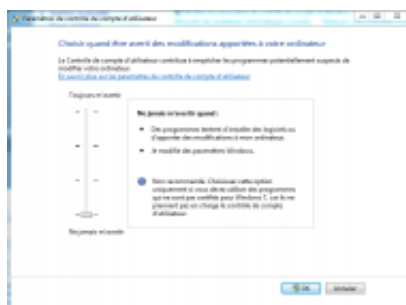
agrandir la photo

Le meilleur moyen d'éviter de mettre la pagaille sur votre ordinateur, s'il est partagé avec plusieurs membres du foyer, c'est de créer plusieurs comptes, pressez **Win + R** et tapez **control userpasswords** pour accéder à la gestion des comptes. Gardez le compte **Administrateur** pour vous et créez des comptes **Standard** pour les personnes qui n'ont pas à toucher aux paramètres système. Le compte **Invité** pourra être utile si vous souhaitez permettre à des amis de passage d'utiliser votre ordi

sans qu'ils aient accès à vos données.

◆ XP, Vista et 7 (niveau 1)

## Désactivez l'UAC

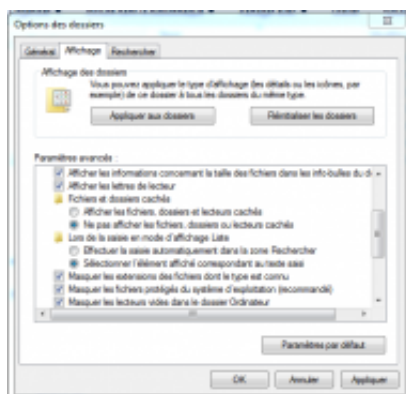


agrandir la photo

Instauré avec Vista, le contrôle de comptes utilisateurs avertit à chaque manipulation pouvant présenter un risque pour l'ordi. Si vous vous sentez à l'aise et que vous êtes seul à utiliser votre PC, vous pouvez désactiver cette option ou baisser son niveau. Avec Windows 7, dans le **Panneau de configuration** au menu **Système et sécurité** sous **Centre de maintenance**, cliquez sur **Modifier les paramètres du contrôle de compte**. Avec Vista **Panneau de configuration**, **Centre de Sécurité** et à gauche **Modifier la manière dont le centre de sécurité m'avertit**.

◆ Vista et 7 (niveau 2)

## Affichez les extensions de fichiers

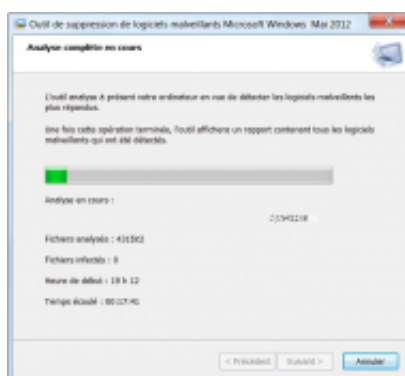


agrandir la photo

Par défaut, les extensions de fichiers sont masquées dans Windows. Pour des raisons de sécurité, il est plus prudent de les faire réapparaître, vous éviterez ainsi de cliquer par mégarde sur des fichiers malveillants camouflés. Par exemple, sans extension, un fichier baptisé **musique.mp3.exe** apparaît en inoffensif **musique.mp3**. Pour activer l'affichage des extensions, pressez **Win + R** et tapez **Control folders**, à l'onglet affichage, décochez **Masquer les extensions**, puis cliquez sur **Appliquer**.

◆ *XP, Vista et 7 (niveau 2)*

## Recherchez les logiciels malveillants



agrandir la photo

Windows intègre d'origine un outil pour détecter et supprimer les logiciels malveillants, pour le lancer pressez **Win + R** et tapez **mrt**, puis faites **Entrée**. Si vous n'avez jamais utilisé cet outil, ou pas depuis longtemps, dans la fenêtre qui s'affiche, vous devriez avoir lien permettant de télécharger la dernière version en date.

◆ *XP, Vista et 7 (niveau 1)*

## Convertissez une partition FAT en NTFS sans perdre les données

Plus sécurisé que le Fat 32, le système de fichiers NTFS a aussi d'autres avantages, comme la gestion des partitions de plus de 2 To ou la prise en charge des fichiers de plus de 4 Go. Si vous



disposez encore de volumes au format **FAT** ou **FAT 32**, vous pouvez facilement les convertir en NTFS en tapant la commande **convert X: /fs:ntfs** (remplacez X par la lettre du volume à convertir) dans l'Invite de commande (tapez **cmd** dans le menu **Démarrer**, puis **Entrée**). Contrairement à un formatage, cette commande n'efface pas les données présentes sur le disque.

◆ *Vista et 7 (niveau 2)*

## **Empêchez l'écriture sur les clés USB**

Vous voulez pouvoir consulter le contenu de périphériques de stockage USB, mais vous ne voulez pas qu'on copie des données dessus depuis votre ordinateur. Allez dans le registre à **HKEY\_LOCAL\_MACHINE, SYSTEM, CurrentControlSet, Control** et créez une nouvelle clé (menu **Edition**) nommée **StorageDevicePolicies**. Dans la fenêtre de droite, créez une valeur **DWORD 32 bits** nommée **WriteProtect** avec une valeur de **1** et redémarrez l'ordi. Pour lever la limitation, supprimez la clé ou changez sa valeur pour **0**.

*XP, Vista et 7 (niveau 3)*

## **Contrôlez l'usage du PC**

Vous trouvez le profil d'utilisateur **Standard** un peu laxiste, vous pouvez utiliser le module de contrôle parental dans l'interface de gestion des comptes utilisateurs (pressez **Win + R** et tapez **control userpasswords**) pour définir les applications autorisées ou encore les périodes horaires durant lesquelles l'utilisateur du compte aura le droit de se connecter à sa session.

◆ *Vista et 7 (niveau 1)*

## **Et aussi...**

**Surveillez les processus** (*XP, Vista et 7 / niveau 3*)

Téléchargez l'utilitaire **Process Monitor** ([t.01net.com/tc36541](http://t.01net.com/tc36541)), décompressez l'archive et cliquez sur **Procmon.exe**. Le programme s'exécute sans installation. Il liste tous les processus en temps réel, permettant ainsi de repérer d'éventuelles activités suspectes.

### **Effacez toutes traces de vos fichiers** *(XP, Vista et 7 / niveau 2)*

Lorsque vous supprimez un fichier, il n'est pas vraiment effacé du disque et peut être récupéré par certains logiciels. Pour être sûr que vos données soient détruites, tapez **cmd** dans **Démarrer** pour lancer l'Invite de commande et saisissez **cipher /w:x:\** (x étant la lettre du volume à nettoyer). Le programme va écrire sur les espaces vides pour écraser les données, cela peut durer longtemps sur un disque volumineux.

### **Créez un volume bootable pour analyser votre PC** *(XP, Vista et 7 / niveau 1)*

Windows Defender Offline, disponible gratuitement sur notre site, permet de créer un support CD/DVD ou clé USB sur lequel vous pourrez démarrer et qui analysera votre système à la recherche de codes malicieux, chevaux de Troie, rootkits et autres douceurs.

### **Redémarrez en mode sans échec** *(XP, Vista et 7 / niveau 1)*

Le mode sans échec charge une version minimale de Windows qui peut être utile pour réaliser certaines tâches de nettoyage, désinstaller des programmes ou supprimer des fichiers récalcitrants en mode normal, car utilisés par des processus peu faciles à identifier. Pour accéder à ce mode, il suffit de presser la touche **F8** (ou **F5**) au début de la séquence de démarrage du PC.

### **Désactivez la saisie du mot de passe** *(Vista et 7 / niveau 1)*

Un mot de passe sécurise votre session, mais si vous êtes le seul à utiliser votre PC vous n'avez peut-être pas envie de le saisir à chaque démarrage. Pour que Windows ouvre la session sans

vous le demander à chaque fois, pressez **Win + R**, tapez **netplwiz** et décochez **Les utilisateurs doivent toujours entrer un nom (...)**. Validez par **Appliquer**.