Identification
des virus et des risques

Au fil des ans, les virus ont évolué et ont multiplié leurs tactiques. Le virus classique s'installe sur un ordinateur et se reduplique pour se propager sur d'autres machines. Pour cela, il se greffe sur un programme et modifie son fonctionnement. Les plus inoffensifs affichent un message (le virus du narcissique), d'autres réalisent une action plus grave. Ces derniers se déclinent en plusieurs variantes : les vers qui ne s'attachent à aucune application précise, mais ralentissent les réseaux, les chevaux de Troie qui se cachent dans un programme bénin et les logiciels malveillants *(malware)*. Le malware, aux visées bien plus délétères que le virus de base, pénalise le fonctionnement d'un ordinateur. La machine n'est jamais totalement bloquée, mais elle est plus lente, plus gauche. Les publiciels *(adware)*, eux, submergent votre écran de publicités indésirables.

Et, enfin, les pires sont les logiciels espions *(spyware)*. Ceux-là sont partout, pour peu que l'on ait, et c'est normal, une vision très stricte du respect de la vie privée. Car des sociétés ayant pignon sur rue se lancent dans l'espionnage de nos habitudes. Microsoft a été ainsi poursuivi en justice aux États-Unis, dans le district de Washington, pour avoir utilisé son programme d'anticopie Windows Genuine Advantage afin de collecter des données confidentielles. Le comble !

Les spyware imposent la surveillance de toutes les activités réseau sortant de l'ordinateur, contrôle peu efficace sur les coupe-feu classiques, qui sont plus habitués à verrouiller les activités entrantes. Là, les pros de la sécurité ne se contenteront pas de tout bloquer en sortie (c'est impossible), mais devront utiliser des inspecteurs de paquets pour vérifier le contenu de tout ce qui sort d'un Mac.

LES MENACES viennent d'internet

Après ce préambule inquiétant, comme l'aiment les marchands de peur et d'antivirus, rassurons les possesseurs de Mac. Si Windows croule sous tous les types de virus, le Mac reste encore épargné. Normal, le virus de base, classique, n'est plus créé à destination d'OS X, mais bien de Windows. On peut quand même noter une montée des risques sur d'autres types de menaces. La presse PC a fait grand cas de l'unique cheval de Troie destiné au monde Mac, l'année dernière. Tapage stupide, car il était inclus dans une version pirate des démonstrations d'iWork et de Photoshop CS4. Jamais votre grand-mère n'aurait su où la trouver et surtout comment la télécharger, d'autant qu'Apple la mettait à disposition gratuitement. Une fausse alarme et... une leçon : la piraterie n'aime pas les amateurs. Plus sérieuse, l'apparition récente d'iBotnet, un botnet (robot qui prend le contrôle d'un serveur pour exécuter ses tâches) spécifiquement Mac. Un peu comme si son auteur avait voulu faire une démonstration... aux débutants ? Pas du tout ! Aux pros, qui ont un serveur web lourd. Ce n'était donc pas la faille sécuritaire de monsieur Tout-le-monde. En fait, les vraies menaces ne sont pas spécifiques à un OS. Car ce sont à présent les applicatifs qui deviennent une cible. Et, bien entendu, le plus visé est le navigateur internet, qui par le biais du phishing (on vous présente un faux site web sur lequel vous entrez naïvement vos données personnelles), devient le point vulnérable de tout ordinateur. Heureusement, Safari 4 est équipé contre le phishing. L'antivirus est donc réservé aux Mac qui communiquent avec des PC, car eux sont en danger.

Les antivirus *passés au crible*

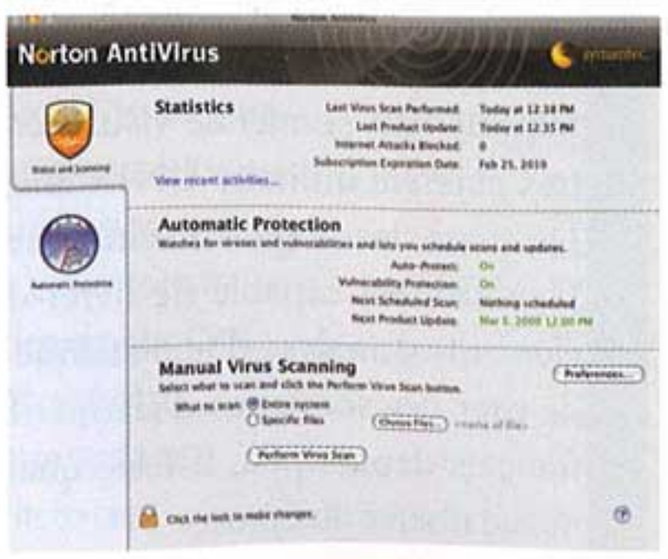
VIRUSBARRIER X5 10.5.8

Prix : **72 €.**
Éditeur : **www.intego.com/fr**

Développé par Intego, une société qui travaille principalement pour le Mac, VirusBarrier a pour objectif principal la détection et l'éradication des virus. Interface claire pour définir ses options d'analyse. La version 10.5.9 est compatible avec Snow Leopard (OS X v.10.6), ce qui est un net avantage sur Norton, toujours lent dans ses mises à jour. Certes, tout antivirus ralentit le fonctionnement naturel d'un Mac, mais, au moins, VirusBarrier est plus discret que Norton et (un peu) plus compatible avec les différents logiciels.

NORTON ANTIVIRUS 11.0.1

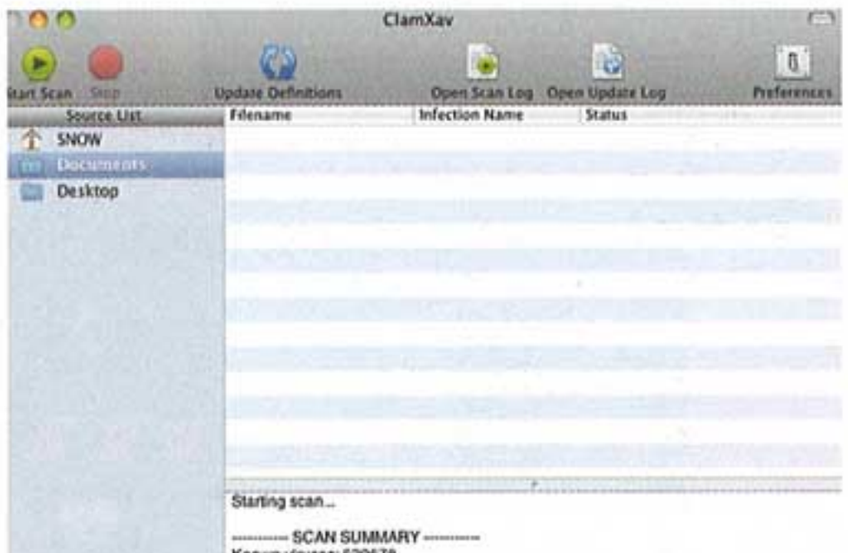
Prix : **50 €.**
Éditeur : **www.symantec.com/fr**



Un vétéran sur Mac qui a essayé d'être de moins en moins envahissant et plus respectueux du fonctionnement d'OS X. Sa base de données de descriptions de virus Windows est plus complète que celle de VirusBarrier. Mais, au moment où nous mettions sous presse, il n'était pas compatible avec Snow Leopard. Symantec vient seulement d'améliorer la compatibilité avec Leopard (10.5). Malgré tout, il est plus exigeant en puissance avec sa fonction AutoProtect.

CLAMXAV 2.0.1

Prix : **gratuit.**
Éditeur : **www.clamxav.com**



Il est gratuit, il est sérieux et il fonctionne même sous Snow Leopard. C'est d'ailleurs avec ce système que nous l'avons testé sur un Mac mini. Une interface claire, une installation simple. Hélas ! Elle impose deux étapes. L'une, véloce, du téléchargement de l'application, l'autre, plus lente, des définitions de virus. Mais il est rapide (écrit en C et non plus en Java). Il nous a semblé plus à l'aise sur les Mac-Intel (Mac mini 2009 et iMac) que sur les vieux Mac PowerPC (G4). Vu son faible coût et ses mises à jour régulières, c'est la solution la plus abordable pour filtrer les macrovirus des courriels destinés... aux PC sous Windows.

Les coupe-feu *à l'épreuve*

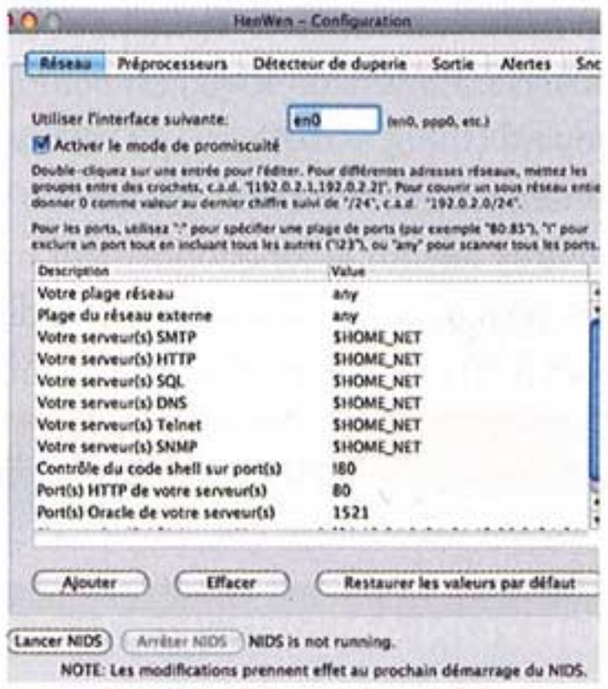
NETBARRIER X5 10.5.4

Prix : **72 €.**
Éditeur : **www.intego.com/fr**

NetBarrier est très riche en fonctions et en voyants. Il est adapté aux débutants qui enclencheront facilement des règles pour contrer les chevaux de Troie, les publiciels, les logiciels espions, et protéger les données confidentielles. Le programme est en français, il inclut même des réglages pour les politiques de sécurité. Bien plus utile qu'un antivirus sur Mac.

HENWEN 2.1.2

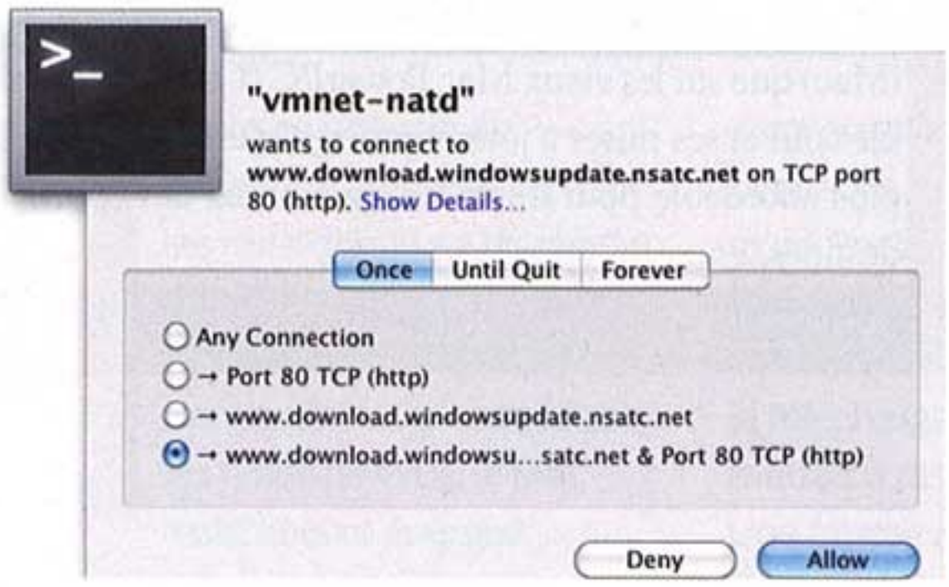
Prix : **gratuit.**
Éditeur : **seiryu.home.comcast.net/~seiryu/henwen.html**



HenWen est un gratuiciel NIDS (Système de détection d'intrusions réseau en français) qui permet de visualiser le très puissant utilitaire UNIX Snort. De tous les logiciels cités, seul HenWen est capable de livrer des éléments d'analyse d'une attaque et de tirer des sonnettes d'alarme. En français depuis peu, il reste quand même réservé aux pros.

LITTLE SNITCH 2.2.B1

Prix : **29,95 $.**
Éditeur : **www.obdev.at**

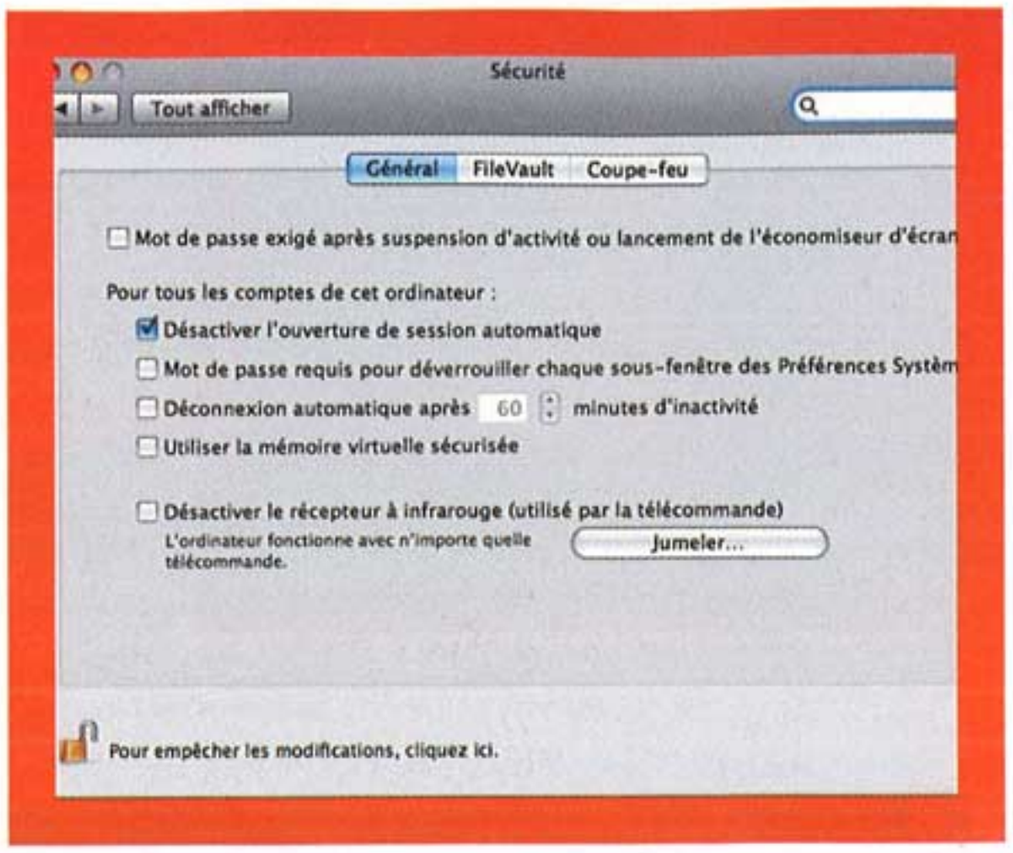


Il est spécialisé dans le filtrage des données sortant de la machine et allant vers internet. Léger, n'alourdissant jamais le fonctionnement du Mac, compatible avec Snow Leopard, Little Snitch est simple, peu cher, mais en anglais. Avec lui, vous créez votre règle de blocage au vol en choisissant autorisations et interdictions permanentes ou momentanées d'un clic de souris dans une unique fenêtre.

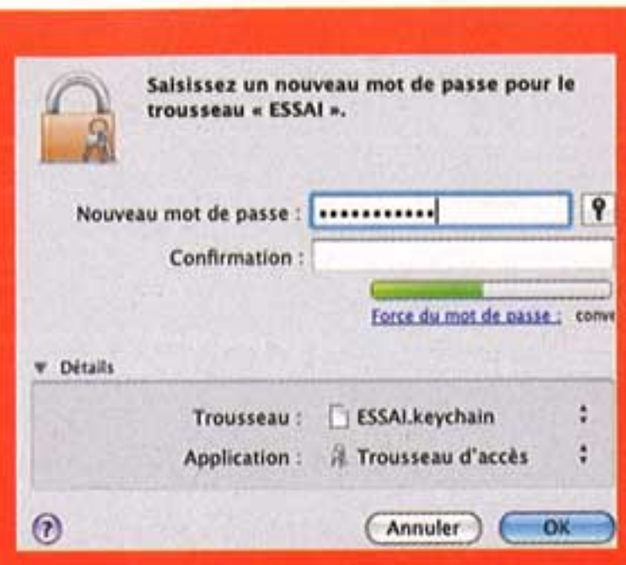
Protégez votre Mac

1 NE DÉMARREZ JAMAIS sans mot de passe

Ne démarrez pas votre Mac sans mot de passe. Certes, c'est plus pratique, mais dangereux. Sous Leopard, **allez dans les *Préférences* d'OS X**, cliquez sur l'icône *Sécurité*, puis sur l'onglet *Général*. Cochez ensuite : *Désactiver l'ouverture de session automatique.*



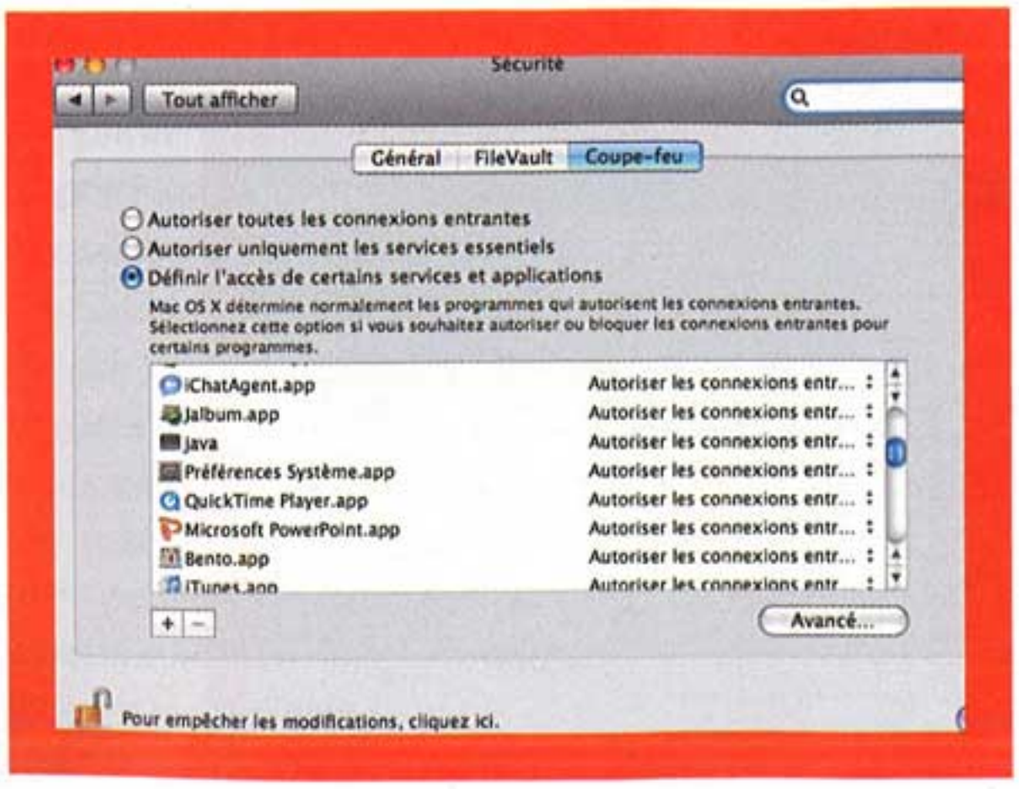
2 CRÉEZ UN MOT DE PASSE FIABLE



Pour générer un excellent mot de passe, ne prenez pas un mot du dictionnaire, ni votre date de naissance. L'idéal est un mixte de lettres (majuscules et minuscules) et de chiffres. Difficile de le retenir ? Ne l'écrivez pas sur un Post-it collé sur l'écran ! Préférez une phrase. Et pour vous aider, allez dans le dossier Applications, sous-dossier Utilitaires et **lancez Trousseau d'accès**. Sélectionnez *Nouveau trousseau* dans le menu *Fichier*. **Entrez *Essai* comme nom**, cliquez sur *Créer*. Dans la fenêtre qui s'ouvre, vous allez avoir un testeur de force de mot de passe. Le testeur indiquera "faible" et affichera un point rouge. Puis passera au jaune et au vert pour signifier que votre choix est fiable. Une fois testé, cliquez sur *Annuler*. Quittez le Trousseau.

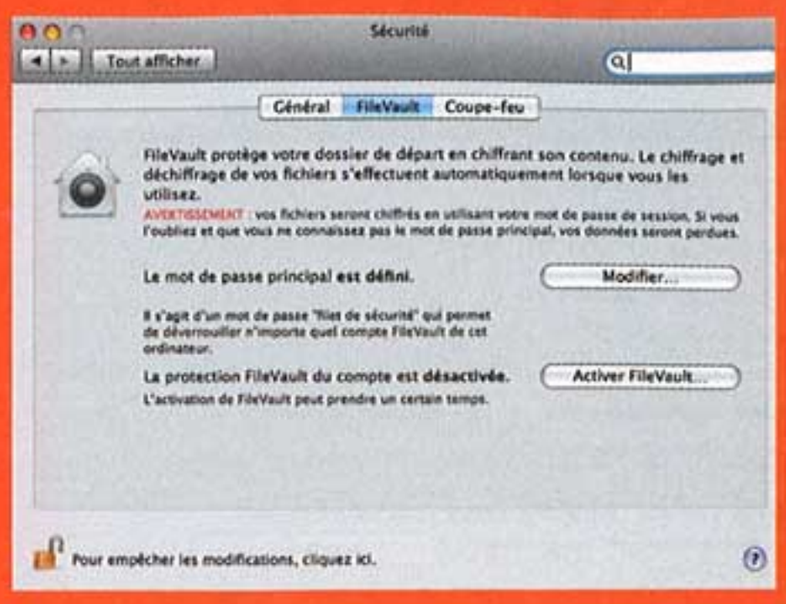
3 LANCEZ le coupe-feu

Le coupe-feu de votre Mac bloque les entrées illicites depuis internet. Dans Leopard, allez dans les ***Préférences*, cliquez sur *Sécurité*,** puis sur l'onglet *Coupe-Feu*. Cliquez sur le 3e bouton *Définir l'accès de certains services et applications*. Cliquez ensuite sur le bouton *Avancé...* et **cochez *Activer le mode furtif*** pour vous protéger contre les attaques par Flood (déluge de connexions). Toutes les fois qu'une application requiert une connexion entrante, une petite fenêtre s'affichera et vous demandera si vous l'autorisez. **Cliquez sur *Oui*,** et son nom entrera dans la liste des applications fiables.



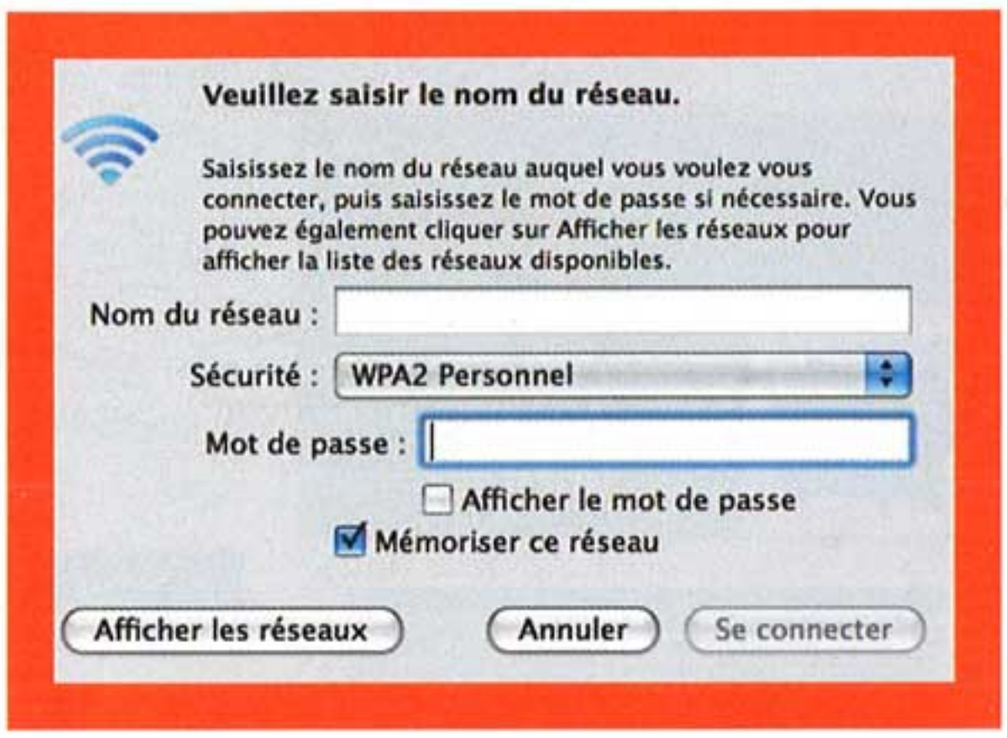
4 ALLEZ PLUS LOIN : FILEVAULT ?

Dans la fenêtre *Sécurité* figure l'arme ultime sous l'onglet *FileVault*. Avec elle, vous pourriez chiffrer totalement votre dossier de départ. Parfait pour les paranos, mais cette supersécurité est parfois incompatible avec certaines applications. On ne peut la recommander qu'aux gourous (après sauvegarde). Mais vous pouvez cocher, sous l'onglet *Général*, *Utiliser la mémoire virtuelle sécurisée*. Précaution moins radicale que FileVault, mais assez efficace.



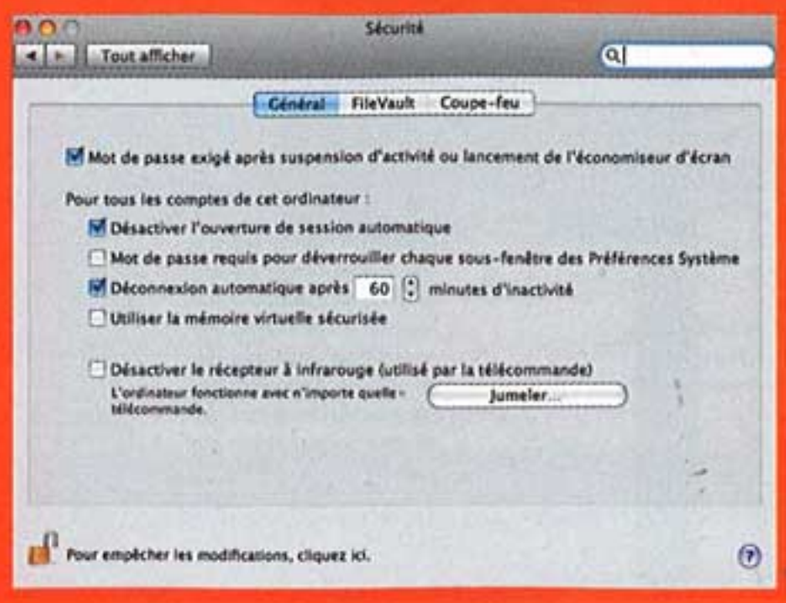
5 SÉCURISEZ le wi-fi

Toutes ces précautions sont suffisantes pour une liaison câblée. Si vous êtes en wi-fi, il faut être encore plus prudent. Vos bornes wi-fi ne doivent pas diffuser leur nom. Dans l'interface d'administration de votre box ADSL, désactivez l'option de diffusion du nom de réseau SSID. Il faudra vous souvenir de ce nom et ne pas laisser le nom standard, connu de tous. Ensuite, optez pour l'encryptage de la communication la plus moderne. Interdiction d'utiliser le WEP (il se craque en quelques minutes) ou même le WAP (plus aussi sûr). Il faut le WPA 2. Même dans ce cas, certaines box vous proposeront encore le vieil encodage en TKIP, hérité du WEP et donc à proscrire. Prenez l'AES 256. Et si tout cela est trop complexe, passez en CPL et servez-vous du réseau électrique de votre habitation pour vous connecter.



6 VERROUILLEZ L'ÉCRAN ET LE TROUSSEAU

Au bureau, prenez l'habitude de sécuriser automatiquement l'accès à votre ordinateur lorsque vous ne l'utilisez pas. Allez dans les *Préférences* d'OS X, cliquez sur *Sécurité*, onglet *Général*, et cochez *Mot de passe exigé après suspension d'activité*. Leopard introduit l'option de désactiver le récepteur de télécommande infrarouge (cochez-la). Pour encore plus de sécurité, cochez *Déconnexion automatique après XX minutes d'inactivité*. Choisissez la durée de votre choix. Enfin, allez dans Applications, sous-dossier Utilitaires, lancez Trousseau d'accès, sélectionnez l'article *Modifier les réglages du trousseau session* dans le menu *Édition*. Dans la fenêtre qui s'ouvre, cochez les deux cases *Verrouiller*.

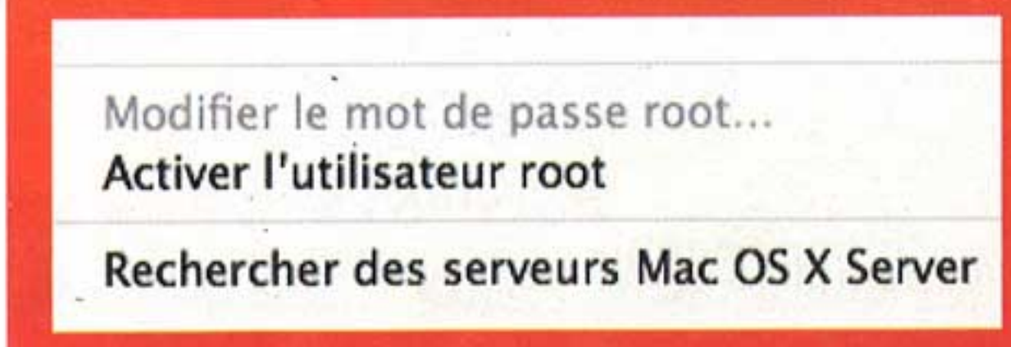


7 DÉSACTIVEZ les partages d'invités

Pour ne pas laisser s'introduire de mauvais plaisants, vérifiez dans les *Préférences* d'OS X, icône *Partage*, qu'aucune case de service n'est cochée. Précaution supplémentaire, pour tous les partages, même non actifs, cochez la case *Uniquement ces utilisateurs* (même s'il n'y en a pas) pour bien signifier que vous ne cochez pas *Tous les utilisateurs* (grave risque dans ce cas).

8 UTILISATEUR ROOT NON ACTIVÉ

Sous Tiger (OS X v.10.4), l'utilitaire Gestionnaire NetInfo permettait d'activer l'utilisateur root, opération la plus antisécuritaire qui soit. Par chance, cet utilitaire a disparu sous Leopard et Snow Leopard et, par défaut, l'utilisateur root est toujours désactivé sur ces systèmes. Signalons qu'il y a, bien dissimulée, une manière de voir si ce compte est désactivé, option destinée aux administrateurs. Apple ne recommande pas la diffusion de cette information. Désolé pour les pirates qui nous liraient.



9 N'OUBLIEZ PAS Safari

Ne négligez pas la sécurité de votre navigateur web. Passez impérativement à Safari 4 (ou Firefox 3.52). Safari 4 intègre un outil d'antiphishing qui détecte les sites frauduleux. Attention ! L'antiphishing fonctionne avec des listes de sites qui doivent être mises à jour. Pour voir si c'est le cas, allez dans les *Préférences* de Safari, onglet *Sécurité*, cochez la case *Avertir de l'accès à un site Web frauduleux*. Si un triangle jaune affiche *Service de navigation sécurisée indisponible*, votre liste n'est plus à jour. Laissez Safari ouvert sans vous connecter à un site, il se mettra à jour au bout de quelques minutes. Profitez-en pour cocher le bouton *Provenant seulement des sites que je visite* dans la section *Accepter les cookies*, et décochez la case *Activer Java* dans la section *Contenu web*.