chapitre
10

Sécurité Internet

Nombre d'utilisateurs pourraient s'adonner à l'informatique personnelle en toute sérénité si Internet n'existait pas. En effet, le revers de la médaille de la révolution Internet se manifeste sous la forme de pirates prêts à tout pour pénétrer dans nos ordinateurs pour y semer des virus, y implanter des outils de piratage à distance, nous infester de logiciels espions, essayer de nous soutirer notre numéro de carte de crédit et transformer notre vie en un enfer perpétuel de sessions de dépannage. De plus, leurs méfaits ont une énorme répercussion financière sur les entreprises et les utilisateurs du monde entier : le coût de la lutte contre les virus, les logiciels espions et le courrier indésirable est estimé à cent milliards de dollars par an.

Une part importante des faiblesses du système, en termes de sécurité, trouve son origine dans Windows XP, conçu à une époque où ce type d'attaques était bien moins fréquent sur Internet. À l'époque, les points d'accès laissés ouverts par Microsoft s'inscrivaient dans un but pratique (notamment pour permettre aux administrateurs système de communiquer avec votre PC depuis le réseau), une initiative dont les pirates ont malheureusement su tirer profit.

C'est pourquoi la firme de Redmond a élaboré Windows Vista avec comme priorité le renforcement de la sécurité de Windows, devant son relookage, l'élaboration de fonctionnalités musicales et vidéo à la pointe du progrès, et la refonte de toute la gestion du réseau. Bien entendu, des personnes à l'esprit mal tourné continueront à faire tout leur possible pour nous rendre la vie infernale, mais une chose est sure : leur tâche n'a pas été facilitée.

Info : Ce chapitre est consacré aux nouvelles fonctionnalités d'autodéfense de Vista, toutes sans exception. Nous l'avons intitulé Sécurité Internet parce qu'en fait, la grande majorité des désordres infectieux pouvant toucher un PC proviennent aujourd'hui d'Internet. Un PC qui ne se connecte jamais a toutes les chances d'être épargné.

Pourquoi Internet Explorer (IE) est-il la cible privilégiée des pirates ? Premièrement, c'est de loin le navigateur le plus populaire de la planète. Deuxièmement, Internet Explorer est directement ancré dans Windows, de sorte que les pirates peuvent semer la pagaille dans Windows en se servant d'Internet Explorer comme voie d'accès.

Profondément dissimulées, les nombreuses améliorations liées à la sécurité de Vista sont invisibles et inaccessibles à l'utilisateur. Elles incluent les fonctionnalités suivantes :

- **Isolation de l'application** – Un programme ne peut pas prendre le contrôle de tâches importantes exécutées par Windows.
- **Durcissement des services Windows** – Les services Windows sont des programmes qui fonctionnent en arrière-plan : le gestionnaire d'impression qui est fourni avec Windows, les anti-virus d'autres éditeurs, etc. Les mécanismes Vista empêchent désormais les services frauduleux (ou les services qui ont été subrepticement modifiés par des pirates depuis Internet) d'apporter des modifications à des parties du système qu'ils ne sont pas supposés toucher ; par exemple, ils ne peuvent pas modifier des fichiers système importants ou le Registre (annexe B).
- **Mode protégé** – Le Mode protégé empêche Internet Explorer ou ses modules complémentaires d'entreprendre des actions contre le système d'exploitation. Donc, même si un logiciel malveillant parvient à franchir toutes les barrières de sécurité d'Internet Explorer, il ne peut pas nuire à votre PC car le Mode protégé enferme IE dans un coffre-fort. En d'autres termes, ce qui se produit dans Internet Explorer reste dans les limites d'Internet Explorer.
- **Address Space Layout Randomization (protection de l'espace mémoire)** – Lorsqu'un programme s'exécute, il conserve beaucoup d'informations dans la mémoire du système. Les concepteurs de codes malveillants exploitent les faiblesses des programmes qui ne gèrent pas très bien cette mémoire, d'autant que les anciennes versions de Windows chargeaient chaque portion de code à un emplacement mémoire prédéfini. Afin de tenter de les en empêcher, l'ASLR charge désormais les portions de code dans des emplacements mémoire aléatoires, ce qui complique singulièrement la tâche des pirates.
- **Protection d'accès au réseau** – Sur un réseau d'entreprise, cette fonctionnalité vous empêche de vous connecter à un réseau si les mises à jour de sécurité et ses signatures de virus du client ne sont pas actualisées.
- **PatchGuard** – Empêche les logiciels non-Microsoft d'atteindre le cœur de Windows.
- **Intégrité du code** – Les logiciels sont contrôlés en intégrité avant leur lancement pour s'assurer qu'ils n'ont pas été modifiés d'une manière ou d'une autre.

La suite de ce chapitre décrit des fonctionnalités liées à la sécurité que vous êtes en mesure d'administrer.

Notez cependant que les outils de sécurité intégrés n'assument pas seuls tous les aspects de la sécurité du PC ; vous avez également votre part de responsabilité. Avant que vous ou un autre membre de votre famille ne se connecte, respectez quelques règles de bon sens :

- **Ne vous fiez à personne** – Nul besoin d'être un expert pour construire un site Web attrayant. Ce n'est pas parce qu'un site Web semble digne de confiance que vous pouvez lui faire confiance. Si vous visitez un site Web peu connu, n'y faites pas n'importe quoi.
- **Ne téléchargez pas de fichiers provenant de sites que vous ne connaissez pas** – Le Web fourmille de logiciels gratuits qui peuvent s'avérer malveillants. Par logiciel malveillant, on désigne de manière générale les virus, les logiciels espions et les autres logiciels nuisibles. Soyez donc très prudent lors de tout téléchargement.
- **Ne cliquez pas sur des publicités** – Les fenêtres publicitaires sont plus que de simples nuisances ; certaines d'entre elles, lorsque vous cliquez dessus, téléchargent des logiciels espions sur votre PC. Comme vous le verrez plus loin dans ce chapitre, Internet Explorer intègre un outil de blocage (non systématique) de fenêtres publicitaires intempestives. Donc pour plus de sécurité, ne cliquez pas.

Cela étant dit, vous êtes prêt à découvrir comment surfer en toute sécurité.

Centre de sécurité

Toutes les versions

Si vous souhaitez obtenir des informations concises sur le niveau de sécurité Internet de votre ordinateur, consultez le Centre de sécurité en choisissant Panneau de configuration>Sécurité>Centre de sécurité.

Comme l'illustre la figure 10-1, la partie principale de l'écran indique l'état du pare-feu, des mises à jour automatique, de la protection contre les logiciels malveillants et d'autres paramètres de sécurité. Des voyants verts signifient que vous êtes protégé ; des voyants jaunes signifient que vous êtes partiellement protégé ; et des voyants rouges signifient que vous êtes vulnérable aux attaques.

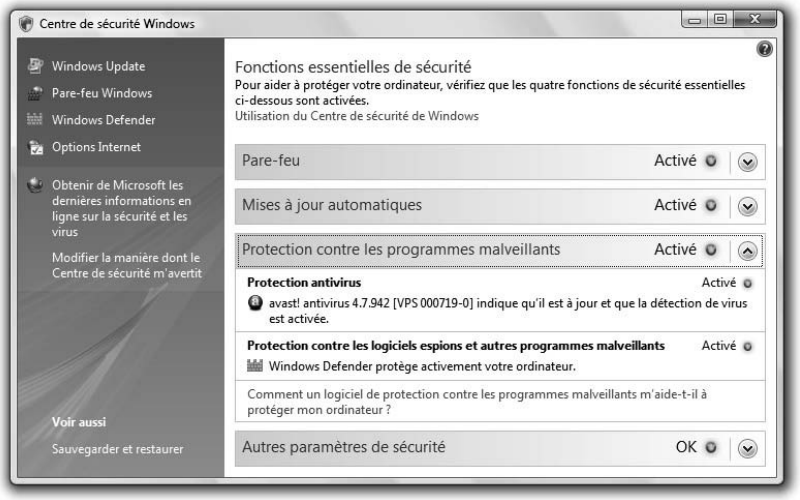
Sous la rubrique de protection contre les programmes malveillants, par exemple, le voyant est vert lorsque vous utilisez à la fois Windows Defender (la fonctionnalité anti-espions de Vista) et un logiciel antivirus ; le voyant est jaune si vous n'utilisez que l'un des deux ; il est rouge si aucun des deux n'est activé. Pour accéder à plus de détails, développez le panneau en cliquant sur le bouton coloré ou sur la flèche dirigée vers le bas.

Le Centre de sécurité n'est pas qu'un indicateur d'états. Il vous alerte aussi (à l'aide d'une icône de couleur dans la zone de notification, assortie d'une info-bulle) lorsque l'un de vos paramètres de sécurité passe dans le jaune ou dans le rouge. Double-cliquez sur l'icône pour ouvrir le Centre de sécurité et voir ce qui mérite votre attention.

Astuce : Si vous, utilisateur expérimenté, compétent et très sûr de vous, préférez que le Centre de sécurité arrête de vous harceler en affichant ses icônes colorées dans la zone de notification, vous pouvez y mettre le holà. Dans le Centre de sécurité, cliquez sur Modifier la manière dont le Centre de sécurité m'avertit. Dans la fenêtre qui apparaît, sélectionnez les options Ne pas m'avertir, mais afficher l'icône ou Ne pas m'avertir et ne pas afficher l'icône (non recommandé).

Le Centre de sécurité est aussi un panneau de configuration central dont les liens permettent de modifier les paramètres de sécurité cruciaux liés à Internet : Pare-feu Windows, Windows Update, Windows Defender et les Options Internet générales. Ils sont tous décrits dans ce chapitre.

Figure 10-1
Le Centre de sécurité révèle au premier coup d'œil où vous êtes protégé et où vous ne l'êtes pas. Cliquez sur les boutons ou sur les flèches sur le côté droit de l'écran pour obtenir plus de détails sur la sécurité dans une catégorie. Mais si vous voulez modifier ces paramètres, utilisez les liens sur le côté gauche de l'écran.



Centre de sécurité et antivirus

Le Centre de sécurité vous avertit lorsqu'il découvre que vous n'avez pas installé de logiciel antivirus sur votre PC. Vista étant fourni sans antivirus, vous verrez probablement ces avertissements jusqu'à ce que vous vous décidiez à en télécharger un et à l'installer.

Attention : Vista exige un logiciel antivirus écrit spécialement pour lui. Les logiciels antivirus de l'époque de Windows XP ne fonctionneront pas.

Certains PC sont livrés avec une version d'essai d'un programme antivirus ; vous devez verser une redevance annuelle pour le maintenir à jour. Si votre PC n'a pas été fourni avec un logiciel antivirus ou si vous avez mis à niveau votre PC à partir d'une version précédente de Windows, l'acquisition d'un logiciel antivirus doit figurer en tête de liste de vos priorités.

Astuce : L'installation d'un logiciel antivirus ne signifie pas nécessairement qu'il vous faudra encore dépenser de l'argent. Plusieurs très bons antivirus sont gratuits dans le cadre d'un usage personnel, comme Avast (*www.avast.com*).

Pare-feu Windows

Toutes les versions

Si vous disposez d'une connexion permanente haut débit, vous êtes donc connecté à Internet 24 heures sur 24. Il est théoriquement possible pour certains mauvais esprits utilisant un logiciel de piratage automatisé de saturer vos ressources ou de prendre le contrôle de votre ordinateur. Heureusement, la fonctionnalité de pare-feu de Vista dresse un barrage contre ce type d'invasion.

Le pare-feu fait office de garde-fou entre Internet et vous. Il examine le trafic Internet et laisse passer les communications qu'il pense être sûres ; le reste des flux est ignoré ou rejeté.

Mode de fonctionnement

Avant d'aborder le rôle du pare-feu dans Vista, une explication (élémentaire) préalable s'impose sur la façon dont votre ordinateur communique avec l'extérieur.

Toutes les données (messagerie instantanée, partage de musique, partage de fichiers, etc.) émises et reçues par votre PC, transitent par un canal de communication spécifique, également nommé port. On peut imaginer les ports comme des tunnels numérotés servant à acheminer certains types de données sur Internet. Si, dans Windows XP, Microsoft a laissé tous les ports ouverts pour simplifier la vie de l'utilisateur (et par-là même celles des pirates), ce n'est à présent plus le cas dans Vista dans lequel tous ces canaux de communication sont fermés.

Le rôle du pare-feu consiste à bloquer ou à autoriser des signaux en se basant sur un ensemble de règles prédéfinies. Ces dernières décident des programmes qui sont autorisés à utiliser votre connexion réseau ou les ports qui peuvent être exploités pour établir une communication. Le pare-feu de Vista présente des améliorations par rapport à son prédécesseur car il protège le trafic à la fois entrant et sortant (le pare-feu Windows XP ne traitait que le trafic entrant), c'est-à-dire les données qui sont envoyées à partir de votre PC et celles qui y sont reçues. Sur ce point, le pare-feu de Vista se met au diapason de ses concurrents, qui proposent cette fonction en natif depuis maintenant plusieurs mois.

Vous vous demandez sans doute, et à juste titre, comment un ordinateur peut être endommagé par le simple fait d'émettre des informations (et non d'en recevoir) sur Internet.

C'est très simple. Si un logiciel malveillant (logiciel espion, cheval de Troie) sommeille déjà sur votre PC, celui-ci peut envoyer des signaux furtifs pour indiquer aux cybercriminels qu'il est prêt à passer à l'offensive. Si, par exemple, votre ordinateur fait partie d'un réseau (professionnel ou domestique) dont les défenses internes sont moindres, ce logiciel malveillant peut donc s'en prendre aux autres ordinateurs. Le pirate n'a plus qu'à prendre le contrôle à distance de votre ordinateur pour faire à peu près tout ce qu'il veut. Il peut, par exemple, s'en servir de poste relais pour acheminer des milliers de courriers indésirables sans que vous ne vous en rendiez compte (dans le jargon, votre poste devient ainsi un « PC zombie »). Par ailleurs, certains logiciels espions enregistrent vos faits et gestes et envoient régulièrement des rapports détaillés à des inconnus. C'est pour toutes ces raisons que le pare-feu de Windows Vista bloque ces communications vers l'extérieur.

Vous n'avez rien à faire pour activer le Pare-feu Windows, car il fonctionne déjà lorsque vous démarrez Windows Vista. En revanche, vous pouvez le désactiver en cliquant sur Modifier les paramètres. Pour vérifier qu'il fonctionne correctement, choisissez Panneau de configuration>Sécurité>Pare-feu Windows. S'il fonctionne correctement, un voyant vert le signale. S'il est désactivé, un voyant rouge vous en avertit.

Gestion des règles du pare-feu

Il arrive que le pare-feu vous cause quelques désagréments. Il peut parfois empêcher un programme parfaitement inoffensif de communiquer avec le monde extérieur (un programme de messagerie instantanée, par exemple).

Dans ce type de situation, Windows vous en informe par un message comme celui illustré à la figure 10-2. En règle générale, il s'agit souvent d'un programme que vous venez juste de lancer et non d'un quelconque logiciel espion implanté sur votre ordinateur. Pour poursuivre votre travail, cliquez sur Autoriser.

Figure 10-2
De temps en temps, vous serez interrompu par ce message. Le pare-feu vous informe qu'un programme cherche à se connecter à votre insu. La plupart du temps, il suffit de cliquer sur Autoriser et de continuer à travailler normalement.

Info : Attention toutefois ! Si les mécanismes offerts par les pare-feu personnels offrent une certaine sécurité, c'est l'utilisateur qui affaiblit le dispositif : avec l'usage quotidien d'Internet, il a tendance à autoriser de plus en plus d'applications ; malheureusement, certaines ne sont pas toujours fiables. Il faut donc rester vigilant et s'assurer qu'une application est inoffensive avant de lui donner des droits.

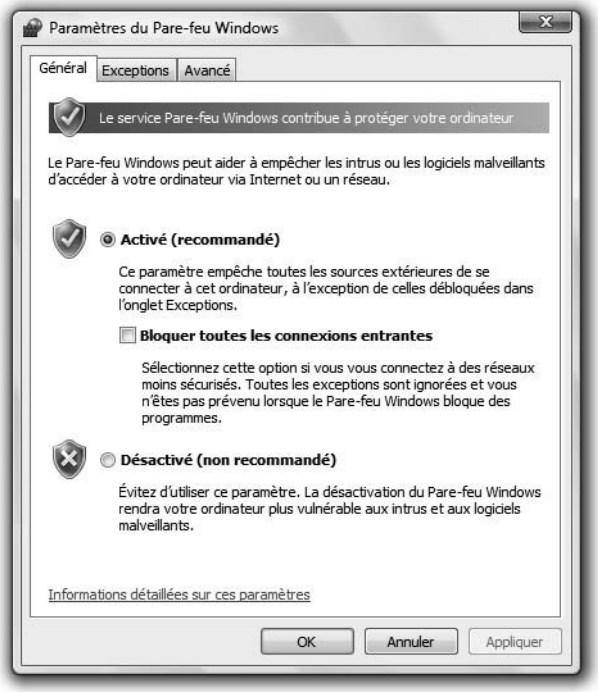
Affiner les réglages du pare-feu

Si vous vous sentez prêt à faire une petite excursion dans la jungle de la haute technologie, vous y gagnerez en maturité et vous apprendrez à régler le pare-feu en utilisant les Paramètres du Pare-feu Windows (figure 10-3). Pour atteindre cette fenêtre, vous

devez transiter par le Panneau de configuration>Sécurité>Pare-feu Windows>Modifier les paramètres, puis vous identifier (voir l'encadré « Identifiez-vous : contrôle de compte d'utilisateur », au début du chapitre 6). Voici à quoi sert chaque onglet :

- **Général** – C'est là que le pare-feu est activé et désactivé. Vous pouvez aussi bloquer entièrement toutes les connexions entrantes (pour être absolument certain que personne n'essaye de pénétrer dans votre ordinateur portable quand vous êtes dans un cybercafé, par exemple) en activant Bloquer toutes les connexions entrantes.

Figure 10-3
L'onglet Général des Paramètres du Pare-feu Windows permet d'activer et de désactiver le pare-feu, et même de bloquer les connexions entrantes. Vous aurez rarement l'occasion de toucher aux autres onglets. Si le Pare-feu empêche un de vos programmes de fonctionner, dirigez-vous vers l'onglet Exceptions pour y remédier. L'onglet Avancé permet d'activer et de désactiver le pare-feu pour différents réseaux auxquels vous vous connectez, tels que votre réseau domestique ou un point d'accès sans fil.



Astuce : Des éditeurs commercialisent des pare-feu beaucoup plus puissants (c'est-à-dire avec plus d'options complexes). N'en utilisez jamais un autre en même temps que le Pare-feu Windows ; vous risquez d'être plongé dans un véritable cauchemar de défaillances. Donc, si vous utilisez un pare-feu comme *ZoneAlarm* ou *Norton Personal Firewall*, désactivez le Pare-feu Windows. La plupart des programmes de pare-feu le font automatiquement lorsque vous les installez, mais pensez à vérifier.

- **Exceptions** – Ouvrez cet onglet si le Pare-feu bloque un programme. Vous pouvez ainsi demander au Pare-feu Windows de faire une exception pour ce programme et lui accorder un laissez-passer.

Une coche signifie que le programme est autorisé à franchir le Pare-feu Windows. Parcourez la liste et regardez si le programme problématique y figure. Si c'est le cas, activez sa case à cocher, puis cliquez sur OK. S'il n'y figure pas, cliquez sur Ajouter un programme, trouvez et sélectionnez le programme, puis cliquez sur OK pour l'ajouter à la liste.

Enfin, activez sa case à cocher et cliquez sur OK. Il devrait maintenant fonctionner en bonne entente avec le Pare-feu Windows.

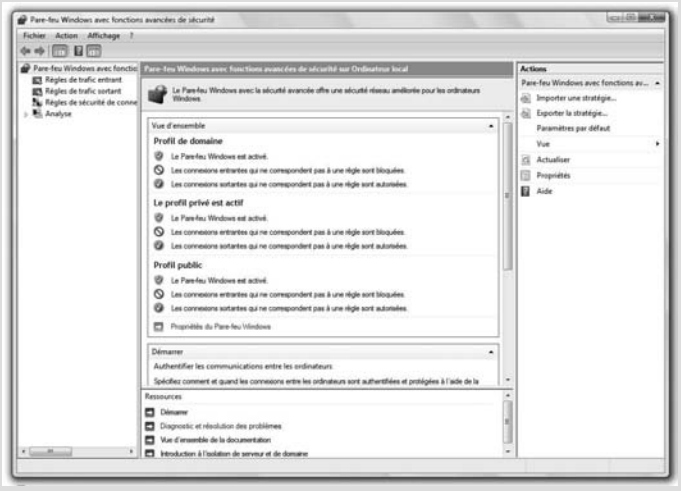
- **Avancé** – Cet onglet répertorie tous les réseaux qui sont protégés par le Pare-feu Windows. Si vous vous connectez à plusieurs réseaux, tels qu'un point d'accès, un réseau domestique, etc., ils devraient tous apparaître ici ; les coches indiquent quels réseaux sont protégés. En règle générale, il est préférable que le Pare-feu Windows protège tous vos réseaux.

LE COIN DES EXPERTS

Personnalisation du Pare-feu : une méthode plus performante

La boîte de dialogue des Paramètres du Pare-feu Windows permet de contrôler assez précisément le mode de fonctionnement du Pare-feu Windows. Mais il régit uniquement le trafic réseau entrant et non le trafic sortant. Il ne permet pas non plus de créer un journal (un enregistrement des événements sous la forme d'un fichier texte) de toutes les tentatives de connexion sur votre PC depuis le réseau ou Internet, ce qui pourrait être utile lorsque vous soupçonnez un pirate d'avoir tenté de s'infiltrer sur votre ordinateur au milieu de la nuit.

Il existe toutefois une interface de configuration avancée du pare-feu. Pour éviter de terrifier les débutants, Microsoft l'a dissimulé mais il s'ouvre assez facilement. Il s'agit du module « Pare-feu Windows avec fonctions avancées de sécurité ».



Pour le lancer, saisissez « wf.msc » dans la zone de recherche du menu Démarrer, puis double-cliquez sur le résultat affiché. Le module permet de personnaliser les connexions sortantes et entrantes. Vous pouvez aussi demander au Pare-feu Windows de créer un journal répertoriant toutes ses activités que vous pourrez ensuite lire dans le Bloc-notes ou un autre éditeur de texte.

Windows Defender

Toutes les versions

Un logiciel espion est un logiciel qui s'installe en cachette sur votre ordinateur. Deux techniques reviennent fréquemment pour vous injecter ces petits programmes malveillants (bien qu'il en existe de nombreuses autres). Premièrement, un site Web peut essayer de vous inciter à le télécharger. Une fausse boîte de dialogue (ou encore une boîte de dialogue de dialogue vide) munie d'un bouton Fermer apparaît et le simple fait

de cliquer sur celui-ci déclenche l'installation. Deuxièmement, un logiciel espion peut s'immiscer dans votre PC lorsque vous téléchargez un programme que vous souhaitez installer. Les logiciels « déplombés » (des programmes commercialisés dont la protection contre la copie a été « craquée ») en sont un exemple classique. Vous ne vous rendez pas compte qu'un programme est clandestinement joint au téléchargement.

Une fois installé, le logiciel espion peut modifier d'importants fichiers système, installer des publicités sur votre Bureau (même lorsque vous n'êtes pas connecté) ou transmettre des informations sur vos habitudes de navigation à un site Web qui bombarde alors votre PC de fenêtres publicitaires qui correspondent à votre comportement en ligne.

Ce type de logiciel peut occasionner de gros dégâts car il ne se contente pas toujours d'observer ce que vous faites sur Internet. Par exemple, en détournant votre page de démarrage ou de recherche, il peut faire en sorte que, chaque fois que vous ouvrez votre navigateur, vous vous retrouviez sur une page Web qui provoque un déluge de fenêtres sur votre écran au point de paralyser votre ordinateur. Les logiciels espions dits *keyloggers* (littéralement, enregistreurs de touches) peuvent enregistrer toutes vos frappes au clavier (mots de passe ou autres) et envoyer des rapports détaillés à des inconnus.

Heureusement, Microsoft fournit dans Windows Vista son tout premier programme anti-espions. Il se nomme Windows Defender (Panneau de configuration>Sécurité>Windows Defender).

Info : Auparavant, Defender se nommait *Microsoft AntiSpyware*. Microsoft l'a rebaptisé car ce programme non seulement recherche la présence de logiciels espions sur votre PC, comme quelques programmes gratuits, mais il surveille aussi quelques recoins importants du système d'exploitation, cibles de prédilection des logiciels espions. Les zones sous surveillance incluent les programmes de démarrage, les paramètres des préférences système, les paramètres Internet Explorer, les téléchargements, etc.

MIEUX COMPRENDRE

Est-ce un logiciel espion (spyware) ou publicitaire (adware) ?

Le logiciel espion a un cousin moins malveillant nommé logiciel publicitaire mais la frontière qui les sépare est extrêmement mince.

Comment les distinguer ?

Si le programme reste discret et transmet à l'extérieur des rapports détaillés sur vos activités, la configuration de votre machine ou les données personnelles (ou professionnelles) sensibles que vous manipulez, c'est un logiciel espion.

Le logiciel publicitaire, lui, est un logiciel gratuit qui affiche des publicités (la version gratuite d'*Eudora*, par exemple). Pour cibler les publicités en fonction de vos centres d'intérêt, il peut transmettre des rapports sur vos habitudes de navigation à ses auteurs. Sachez que Windows Defender ne fournit pas de protection contre ce type de logiciel.

Les défenseurs du logiciel publicitaire justifient l'existence de ce type de programme comme un moyen de faire payer l'utilisateur pour son logiciel gratuit. Comme l'utilisateur dont on espionne les habitudes de navigation reste anonyme, il ne s'agit pas vraiment, à leurs yeux, d'un logiciel espion. Quant à ses opposants, ils rétorquent que tout logiciel transmettant des informations sur vos activités est un logiciel espion, quoi qu'on en dise.

Windows Defender vous protége contre les logiciels espions de deux manières. D'une part, c'est une sorte de sentinelle silencieuse qui surveille votre système en arrière-plan. Lorsqu'il découvre qu'un logiciel espion essaye de s'installer, Defender lui barre la route

et le détruit. D'autre part, il analyse quotidiennement votre disque dur en quête d'infections et supprime les fauteurs de troubles.

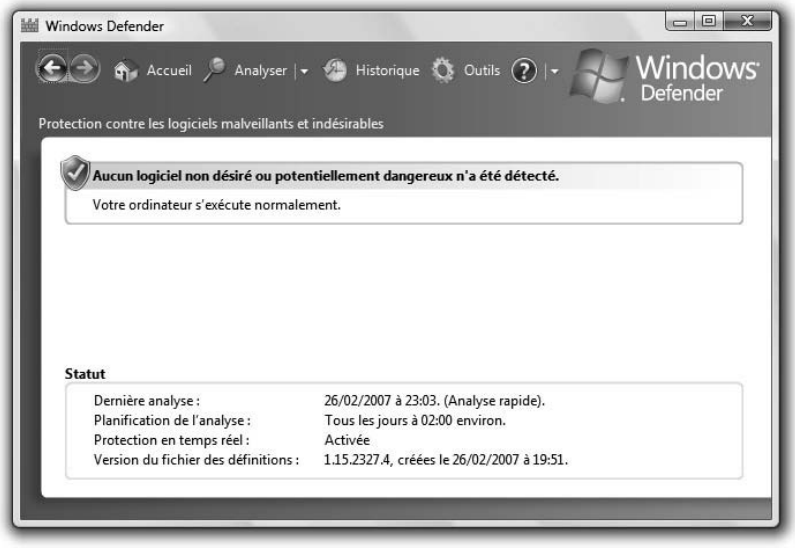
Vous n'avez pas besoin d'activer Windows Defender. Il fonctionne dès que vous démarrez Windows. Et toutes les nuits, à deux heures du matin (il est possible de modifier l'heure ; consultez la section « Outils » plus loin), si votre PC est allumé, Defender analyse votre système, éliminant tous les logiciels espions qu'il trouve.

Pour consulter les dernières activités de Windows Defender, sélectionnez Panneau de configuration>Sécurité>Windows Defender. Vous saurez au premier coup d'œil si Defender estime que votre PC est sain.

En général, comme illustré à la figure 10-4, Windows Defender ne trouve pas de logiciels espions. Si cela lui arrivait, Windows vous en informerait. Un message d'avertissement surgit et vous demande si vous voulez autoriser le logiciel douteux à continuer à fonctionner ou si vous préférez le supprimer. Voici ce que vous devez répondre :

- Si le niveau d'alerte est **Grave, Élevé ou Moyen**, demandez à Windows Defender de supprimer immédiatement le logiciel espion.
- Si le niveau d'alerte est **Faible**, lisez le message en détail. Si cela ne vous dit rien qui vaille ou si vous ne reconnaissez pas l'éditeur du logiciel, demandez à Windows Defender de bloquer ou de supprimer le logiciel.
- **Non encore classifié** signale généralement un programme inoffensif. Si vous reconnaissez le nom du logiciel, laissez-le fonctionner normalement. Sinon, faites une recherche sur le nom du programme dans Google pour vous aider à prendre une décision le concernant.

Figure 10-4
Cette fenêtre indique la date de la dernière analyse, si Defender a trouvé des logiciels espions et les analyses quotidiennes planifiées. Faites particulièrement attention à la Version du fichier des définitions. Elle indique à quand remonte la dernière mise à jour des définitions des logiciels espions. Si elle date de plus d'une semaine, utilisez Windows Update (chapitre 20) pour récupérer les dernières définitions.



À présent, vous connaissez les fonctions élémentaires de Windows Defender. Passons maintenant à des fonctionnalités plus avancées extrêmement intéressantes se présentant sous la forme des liens Analyser, Historique et Outils.

Analyser

Ce lien analyse votre PC à la recherche de logiciels espions. Cliquez dessus pour lancer un examen ou cliquez sur le bouton X pour définir le type d'analyse. Les choix suivants s'offrent à vous :

- L'**Analyse rapide** est ce que fait Windows Defender toutes les nuits. Il analyse les parties de votre PC susceptibles d'être infectées par des logiciels espions, ainsi que tous les programmes en cours de fonctionnement. Pourquoi lancer une analyse rapide si elle a déjà été faite la nuit dernière ? Parce que vous venez d'installer un logiciel ou que vous avez visité un site Web douteux.
- L'**Analyse complète** est plus approfondie ; elle examine le moindre fichier sur tous les disques durs, ainsi que de nombreux programmes en cours de fonctionnement. Si vous pensez avoir été infecté par un logiciel espion, lancez l'Analyse complète pour le débusquer. Elle prend beaucoup plus de temps qu'une Analyse rapide.
- L'**Analyse personnalisée** permet de préciser les dossiers devant être analysés, au cas où un logiciel espion aurait réussi à s'infiltrer en un lieu bien caché.

Historique

Cet onglet propose le journal de toutes les actions entreprises par Windows Defender (figure 10-5). Lorsqu'il est intervenu pour traiter des programmes, il en présente le nom, le niveau d'alerte, l'action entreprise, la date et la réussite ou l'échec de l'action. Cliquez sur une entrée pour afficher plus de détails la concernant, comme l'emplacement, le nom de fichier et la description de la raison pour laquelle Defender a considéré le programme comme douteux.

Les techniciens apprécieront de voir figurer ici des informations pointues, telles que la clé de Registre employée par chaque programme.

Outils

Microsoft y a réuni les outils avancés de Windows Defender :

- **Options** – Programmez le moment et le type d'exécution de Windows Defender, ainsi que les actions devant être prises face à un logiciel suspect, parmi d'autres options.

  Les paramètres par défaut prévoient une analyse du système toutes les nuits à deux heures du matin. Évidemment, il est fort probable que votre PC ne sera pas allumé à cette heure avancée de la nuit. Utilisez ces options pour indiquer une heure à laquelle le PC est allumé.

  Vous pouvez aussi sélectionner une analyse rapide ou une analyse complète. L'Analyse rapide est définie par défaut, mais n'hésitez pas à programmer une analyse

complète de votre PC à une heure qui vous dérange le moins. Cette rubrique permet aussi de préciser le comportement de Defender en présence d'un niveau d'alerte élevée, moyenne ou faible. Le meilleur réglage reste « Basée sur les définitions (par défaut) », qui indique à Defender de se baser sur son propre jugement.

Figure 10-5
Windows Defender affiche toutes les mesures qu'il a prises. Dans l'Historique figurent généralement des décisions visant à autoriser l'exécution d'un logiciel car il ne semble pas malveillant. Dans cette figure, Windows Defender autorise le logiciel anti-virus Avast à fonctionner.

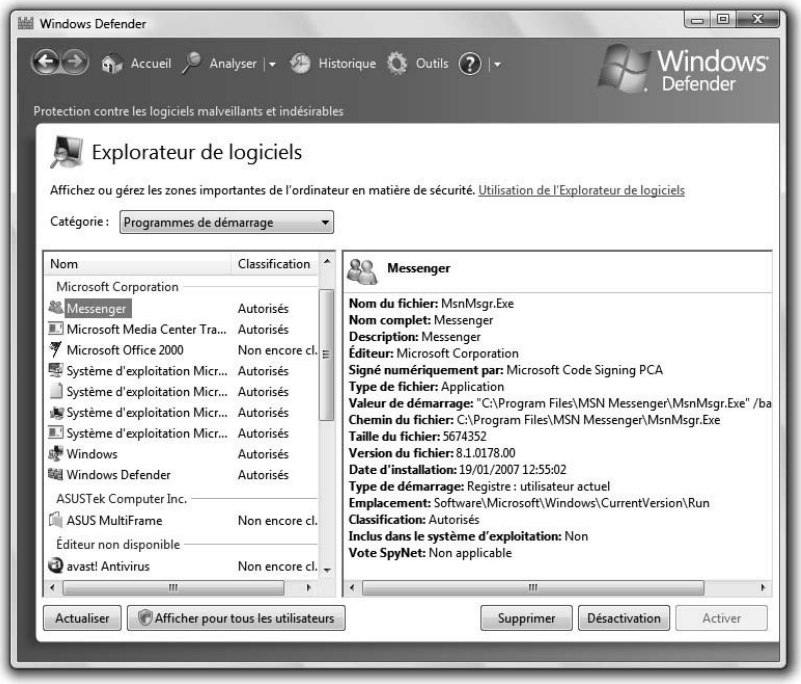
- **Éléments en quarantaine** – Quand Defender trouve un logiciel espion, il le place dans une zone de quarantaine depuis laquelle il ne peut pas nuire. Cet onglet permet de voir les logiciels en quarantaine, de les supprimer, de les restaurer (de lever la quarantaine). En général, la restauration des logiciels espions n'est pas une initiative judicieuse.
- **Éléments autorisés** – Si Defender annonce qu'il a trouvé un logiciel potentiellement malveillant, mais que vous l'autorisez néanmoins à fonctionner, il est considéré comme étant un Élément autorisé. Dorénavant, Defender l'ignore, ce qui signifie que vous faites totalement confiance au programme. Le nom des programmes autorisés figure dans cette liste.

  Si vous sélectionnez le nom d'un programme, puis que vous cliquez sur Supprimer de la liste, il disparaît de la liste des Éléments autorisés et Defender recommence à le surveiller.
- **Explorateur de logiciels** – Cette fenêtre (figure 10-6) est essentiellement destinée aux experts qui veulent examiner en détail les programmes sur leur PC et supprimer tous ceux qui ont l'air suspect.

Windows Defender

Dans la liste déroulante, choisissez la catégorie de programmes que vous voulez examiner, comme Programmes de démarrage. Cliquez sur une entrée de la liste pour lire le nom de l'éditeur, une description, le fichier exécutable correspondant et tant d'autres détails que vous en aurez le vertige. Vous pouvez cliquer sur Supprimer, Désactivation ou Activer (lorsque vous avez déjà désactivé un programme mais que vous voulez à nouveau l'autoriser à fonctionner). Si ces boutons sont grisés, cliquez tout d'abord sur Afficher pour tous les utilisateurs.

Figure 10-6
De nombreux programmes configurent le système pour se lancer automatiquement au démarrage de Windows, sans prendre la peine de vous en informer. Cela peut plomber votre système. L'Explorateur de logiciels est un moyen idéal pour les débusquer. Désactivez ceux qui ne doivent pas être lancés au démarrage. Vous pouvez toujours le faire manuellement, sans que cela nuise à leur bon fonctionnement.



- **Microsoft SpyNet** – L'une des aptitudes les plus appréciées de Defender est sa capacité à se tenir informé des nouveaux types de logiciels espions via le réseau Microsoft SpyNet, qui fédère la connaissance collective des utilisateurs de Vista à travers tout l'Internet.

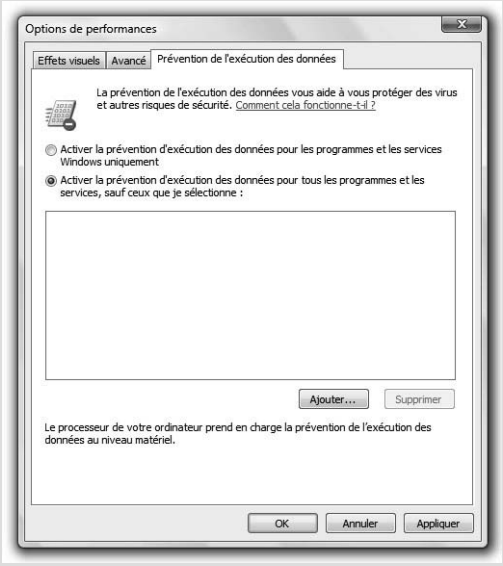
  Supposons que Windows Defender ne parvienne pas à définir si un nouveau programme est ou n'est pas un logiciel espion. Il peut envoyer une demande d'informations en ligne pour savoir comment les membres du réseau ont traité le même programme, puis il se base sur les réponses obtenues pour traiter votre exemplaire du programme. Si les autres utilisateurs de Vista le suppriment car ils sont parvenus à déterminer qu'il s'agit bien d'un logiciel espion, il fait de même.

D'après Microsoft, toutes ces informations sont anonymes. Si vous êtes d'accord, vous pouvez aussi rejoindre la communauté SpyNet.

LE COIN DES EXPERTS

Prévention de l'exécution des données (DEP, Data Prevention Execution)

L'une des nouvelles fonctionnalités méconnue de sécurité de Windows Vista, la Prévention de l'exécution des données vous protège contre les attaques dissimulées dans les données (débordements de tampons par exemple). Elle surveille d'importants services (programmes fonctionnant à l'arrière-plan) et programmes Windows, en veillant notamment à ce qu'aucun code malveillant ne parvienne à corrompre la mémoire système afin de détourner le fonctionnement desdits services et prendre ainsi le contrôle de votre PC. Si le mécanisme de prévention débusque une attaque en cours, il arrête automatiquement le service ou le programme menacé.



Le service DEP est configuré initialement pour ne protéger que Windows et non les autres programmes. Toutefois, vous pouvez le paramétrer pour surveiller certains programmes installés sur le système ou la totalité d'entre eux. Vous bénéficiez alors d'une meilleure protection. En revanche, le DEP peut entrer en conflit avec ces programmes, provoquant alors un comportement fantaisiste ou une impossibilité d'exécution de ceux-ci. Dans ce cas, vous pouvez désactiver la fonction DEP pour ces programmes.

Remarque : si la Prévention de l'exécution des données commence subitement à interférer avec les fichiers et les fonctionnalités importantes de Windows, un programme récemment installé peut en être la cause. Essayez de le désinstaller ou renseignez-vous auprès de l'éditeur pour savoir si une version compatible avec la Prévention de l'exécution des données est disponible ; cela peut résoudre le problème.

Pour activer la Prévention de l'exécution des données pour tous les programmes ou certains seulement, ouvrez le Panneau de configuration>Système et maintenance>Système>Paramètres système avancés. Sous la rubrique Performances, cliquez sur Paramètres, puis cliquez sur l'onglet Prévention de l'exécution des données, illustré ici. Sélectionnez l'option Activez la prévention d'exécution des données pour tous les programmes et les services, sauf ceux que je sélectionne, puis cliquez sur OK.

Si vous constatez que la prévention nuit au fonctionnement d'un programme, cliquez sur Ajouter, puis suivez les instructions pour le sélectionner.

Dans le bas de la boîte de dialogue figure une mention indiquant si votre PC prend ou non en charge la prévention au niveau matériel, ce qui améliore les performances de la machine. Si ce n'est pas le cas, Windows utilise une version logicielle de cette fonction.

- **Site Web de Windows Defender** – Ce lien vous mène au site de Windows Defender, qui contient quelques sources d'aide modérément utiles sur les logiciels espions.

Le filtre anti-hameçonnage

Toutes les versions

L'esprit criminel ne connaît pas de limites. Comment pourrait-on expliquer autrement les malversations perpétrées par l'hameçonnage ?

Lorsque vous êtes victime d'hameçonnage, vous recevez ce qui paraît être un courrier ordinaire provenant d'une banque, d'eBay, de PayPal ou d'un autre site Web de transactions financières. Le message vous informe que le site a besoin d'une confirmation des informations qu'il détient sur votre compte ou vous avertit que votre compte a été piraté et qu'il a besoin de votre aide pour le protéger.

En adulte responsable, vous cliquez sur le lien fourni pour résoudre le soi-disant problème, et êtes dirigé sur un pseudo site Web (soigneusement conçu pour ressembler au vrai) de validations des transactions d'eBay ou de PayPal. Pour rendre ce site encore plus réaliste, le faussaire y insère souvent des liens véritables, en plus des liens détournés. Si vous saisissez votre identifiant et votre mot de passe, comme demandé, vous ne tarderez pas à recevoir des notes d'hôtels grand luxe à Las Vegas qui s'élèvent à la modique somme de 10 000 dollars et qui sont débitées sur votre compte.

Les sites des faussaires ressemblent tant aux vrais qu'il peut être très difficile de les différencier. Certains sites sont cependant identifiables, notamment en raison des nombreuses fautes d'orthographe qu'ils comportent.

Le nouveau filtre anti-hameçonnage d'Internet Explorer 7 vous protége de ces contrevenants. Vous n'avez rien à faire pour l'activer, car il fonctionne en permanence.

Attendez-vous donc, un jour ou l'autre, à voir un avertissement vous signalant que vous tentez d'accéder à un site répertorié comme frauduleux (figure 10-7).

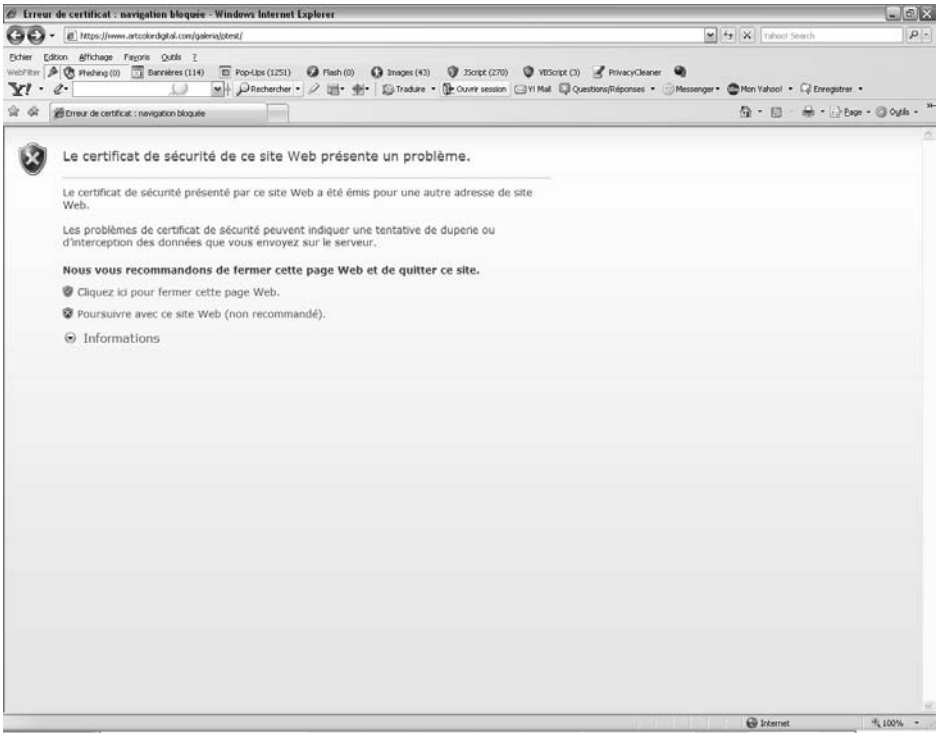


Figure 10-7
N'y allez pas : Internet Explorer vous empêche de visiter des sites d'hameçonnage connus. Il utilise diverses méthodes pour distinguer un site authentique d'un site d'hameçonnage, il se sert notamment de listes noires constamment mises à jour, dans lesquelles sont référencés les sites d'hameçonnage démasqués.

Si vous êtes confronté à cette situation, cliquez sur le bouton marqué d'une coche verte pour fermer la page. Ne cliquez par sur le bouton au X rouge, sinon vous arriverez sur le faux site.

Si Internet Explorer doute de la fiabilité d'un site, un bouton jaune apparaît à côté de la barre d'adresse pour signaler « Site Web suspect ». À moins d'être absolument certain que le site est authentique, il est préférable d'aller voir ailleurs.

Réglages du filtre anti-hameçonnage

Le contrôle de la fonctionnalité du filtre anti-hameçonnage est rudimentaire : vous pouvez l'activer ou le désactiver et vérifier l'authenticité d'un site Web particulier. Choisissez Outils>Filtre anti-hameçonnage pour accéder aux options suivantes :

- **Vérifier ce site Web** – Cette commande transmet l'adresse du site Web que vous consultez aux serveurs de Microsoft, qui la comparent à la gigantesque base de données temps réel de sites d'hameçonnage.

Info : Lors de la première utilisation de cette commande, vous obtenez un message vous expliquant, dans le but d'apaiser vos craintes paranoïaques, que vous allez transmettre des informations anonymes à Microsoft. Cliquez sur OK pour continuer ; si vous ne voulez plus que ce message apparaisse, cochez la case Ne plus afficher ce message.

Quelques instant plus tard, un message apparaît indiquant s'il s'agit d'un site authentique, suspect ou d'hameçonnage. S'il est authentique, le message l'indique clairement (figure 10-8, en haut) ; s'il s'agit d'un site douteux ou d'hameçonnage, l'avertissement apparaît dans la barre d'adresse (figure 10-8, en bas).

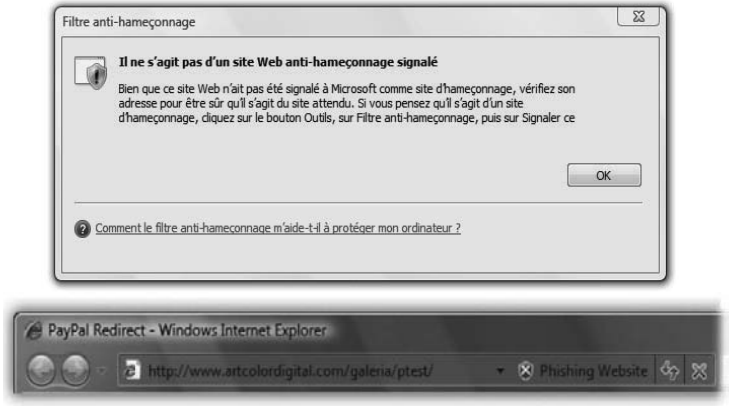


Figure 10-8
En haut : Lorsque vous demandez la vérification d'un site soupçonné d'hameçonnage, Internet Explorer consulte une base de données Microsoft. Dans le cas illustré, le site est authentique.
En bas : Danger! Vous vous trouvez sur un site d'hameçonnage connu. Ce site était particulièrement malveillant ; si vous y cliquiez sur un lien, le site en profitait pour installer subrepticement un virus sur votre PC.

- **Désactiver/Activer la vérification automatique de sites Web** – Contrairement à ce que vous pourriez penser, cette option ne désactive pas le filtre anti-hameçonnage, mais uniquement l'un des moyens de défense contre ce type de site : l'envoi

à Microsoft d'une liste de sites Web que vous visitez, afin que les éléments qu'elle contient soient comparés avec ceux de la base de données Microsoft.

Info : En fait, la vérification automatique de sites Web ne se contente pas d'envoyer l'adresse des sites que vous visitez à Microsoft. Elle envoie aussi l'adresse IP de votre ordinateur, le type de navigateur utilisé et le numéro de version du filtre anti-hameçonnage. Ces informations sont chiffrées avant d'être envoyées. Aucune information associée au site n'est communiquée, telles que les critères de recherche que vous avez utilisés, les informations que vous avez saisies dans les formulaires ou les cookies.

FAQ

Sherlock Explorer

Comment Internet Explorer fait-il la différence entre un site d'hameçonnage et un site authentique ?

IE utilise trois types d'informations pour débusquer un site frauduleux.

Sa première ligne de défense est une base de données compilée par Microsoft et fréquemment mise à jour, répertoriant les sites d'hameçonnage connus. Une image de cette base de données se trouve tout simplement sur votre propre disque dur. Chaque fois que vous vous dirigez vers un site Web, Internet Explorer consulte sa base de données. Si l'URL du site Web y figure, vous êtes alerté. La base de données est renseignée par plusieurs organismes spécialisés dans la chasse aux sites frauduleux, notamment Cyota, Internet Identity et MarkMonitor, ainsi que par les informations directement fournies par les utilisateurs.

Ensuite, Internet Explorer utilise une méthode heuristique, une forme d'intelligence artificielle de bas niveau. Elle compare les caractéristiques du site consulté aux caractéristiques fréquentes des sites d'hameçonnage. Cette méthode permet à IE de dépister les sites d'hameçonnage qui ne sont pas encore répertoriés dans la base de données de sites connus.

Enfin, Internet Explorer envoie discrètement les adresses de certains des sites que vous visitez à Microsoft, qui les compare à ceux d'une liste fréquemment mise à jour de sites d'hameçonnage connus (différente de la base de données sur votre PC).

Vous continuez néanmoins à être protégé grâce à la vérification de la base de données de sites d'hameçonnage sur votre PC et la recherche heuristique.

Microsoft déclare ne pas enregistrer les adresses de sites Web qu'elle récupère et, par conséquent, qu'elle n'est pas en mesure de les associer à vous. Si vous préférez ne pas tenir Microsoft, informé de vos allées et venues, vous pouvez désactiver cette fonctionnalité.

- **Signaler ce site Web** – Si vous tombez sur un site Web que vous soupçonnez être un site d'hameçonnage, cliquez ici. Une nouvelle fenêtre de navigateur apparaît ; activez l'option Je pense qu'il s'agit d'un site Web d'hameçonnage. Choisissez la langue du site, puis cliquez sur Envoyer.

  Utilisez aussi cette option dans la situation inverse : lorsque vous visitez un site que vous savez être authentique mais qu'Internet Explorer signale comme étant un site d'hameçonnage. Deux choix vous sont proposés juste au-dessus du bouton Envoyer : l'un pour signaler ce que vous pensez être un site d'hameçonnage et l'autre pour signaler ce que vous savez ne pas être un leurre et pour cause : vous en êtes l'auteur.

- **Paramètres du filtre anti-hameçonnage** – Lorsque vous sélectionnez cette option, l'onglet Avancés de la boîte de dialogue Options Internet apparaît. Il

propose de nombreux paramètres d'Internet Explorer qui concernent le navigateur dans ses moindres détails. Pour accéder aux paramètres du filtre anti-hameçonnage, faites défiler la liste presque jusqu'en bas.

Choisissez Désactiver le filtre anti-hameçonnage si vous êtes certain de démasquer les faussaires tout seul. Parmi les autres options, vous trouverez un autre endroit où désactiver ou activer la transmission d'un message d'informations sur les sites Web (« automatic website checking »).

Confidentialité et cookies

Toutes les versions

Les cookies sont, en quelque sorte, des fichiers de préférences des pages Web. Certains sites Web, surtout les sites marchands comme Amazon, les déposent sur votre disque dur à la manière de petits signets, afin de se souvenir de vous à votre prochaine visite. Sur Amazon, un message d'accueil vous souhaite même personnellement la bienvenue en citant votre nom, grâce au cookie qu'il utilise pour vous reconnaître. La plupart des cookies sont parfaitement inoffensifs et sont même extrêmement utiles. Ils permettent à votre PC de s'identifier automatiquement sur un site ou vous permettent de personnaliser l'apparence du site et son mode d'emploi.

Toutefois, il arrive que certains sites Web se servent de cookies pour enregistrer les pages que vous consultez sur un site, le temps que vous y passez, le type d'informations que vous aimez consulter, etc.

LE COIN DES EXPERTS

Gestionnaire de modules complémentaires

Internet Explorer est plus qu'un simple navigateur. En fait, c'est quasiment un mini-système d'exploitation qui nourrit en son sein plein de petits programmes complémentaires. La catégorie la plus fournie en modules complémentaires comprend les contrôles ActiveX. Ils fournissent tout un arsenal de supers pouvoirs à Internet Explorer ; par exemple, le module Flash permet de lire les animations et les films sur *YouTube* et bien d'autres sites.

Attention toutefois, car les contrôles ActiveX et d'autres modules complémentaires peuvent engendrer des problèmes. Si vous en installez trop, votre navigateur s'en trouvera ralenti. Les modules complémentaires entrent parfois en conflit, ce qui fait planter Internet Explorer. Et certains (en réalité les pires), contiennent des codes malveillants conçus pour endommager votre navigateur ou votre PC.

Pour vous aider à maîtriser la prolifération de vos modules, choisissez Outils>Gérer les modules complémentaires>Activer ou désactiver les modules complémentaires ; la liste de vos modules complémentaires et contrôles ActiveX s'affiche. Ils sont répartis sous diverses catégories, telles que ceux qui sont actuellement chargés dans Internet Explorer et les contrôles ActiveX que vous avez téléchargés.

Sélectionnez-en un pour lire plus d'informations à son sujet et pour avoir accès aux options Désactiver, Activer et Supprimer. Remarque : avant de cliquer sur l'une de ces options, faites une recherche Google sur le nom ou le nom de fichier du module. Vous saurez assez vite si le module est digne de confiance. Soyez particulièrement méfiant avec les modules du type BHO (Browser Helper Objet) Applications d'assistance du navigateur. Ils peuvent être utiles mais aussi très nuisibles.

Si vous craignez pour la protection de votre vie privée, et si vous êtes prêt à vous passer de certains des avantages apportés par les cookies, Internet Explorer est en mesure de vous protéger.

La terminologie des cookies

Avant d'élaborer votre stratégie de lutte contre la prolifération des cookies, vous devez vous familiariser avec leur terminologie. Voici quelques explications qui vous seront utiles dans un premier temps :

- Un **cookie interne** est créé par le site que vous êtes en train de consulter. Comme le cookie d'Amazon décrit plus haut, ce type de cookies ne s'intéresse généralement pas à votre vie privée. Il est conçu pour vous identifier ou pour se souvenir de la manière dont vous avez personnalisé la page d'accueil de Google, par exemple.
- Les **cookies tiers** sont déposés sur votre disque dur par un site autre que celui en cours de consultation, souvent par un publicitaire. Inutile de préciser que ce type de cookie est davantage sujet à caution. Il peut pister vos habitudes de navigation et créer des profils sur vos centres d'intérêt et votre comportement.
- Une **stratégie de confidentialité compacte** est la politique de respect de la vie privé, affichée aux yeux de tous sur un site Web, qui décrit comment les cookies sont exploités. Vous y découvrirez pourquoi des cookies sont utilisés et leur durée de vie sur votre PC. Certains cookies sont automatiquement supprimés lorsque vous quittez un site Web et d'autres sont valides jusqu'à une date précise.
- **Consentement explicite** signifie que vous avez autorisé un site Web à réunir des informations sur vos activités en ligne.
- **Consentement implicite** signifie que vous n'avez pas donné votre accord explicite pour la collecte d'informations, mais le site suppose que vous êtes d'accord puisque vous le consultez. Si un site Web se base sur la politique du consentement implicite, il vous considère comme d'accord jusqu'à preuve du contraire.

Options des cookies

Choisissez Outils>Options Internet>Confidentialité pour accéder à l'onglet Confidentialité illustré à la figure 10-9.

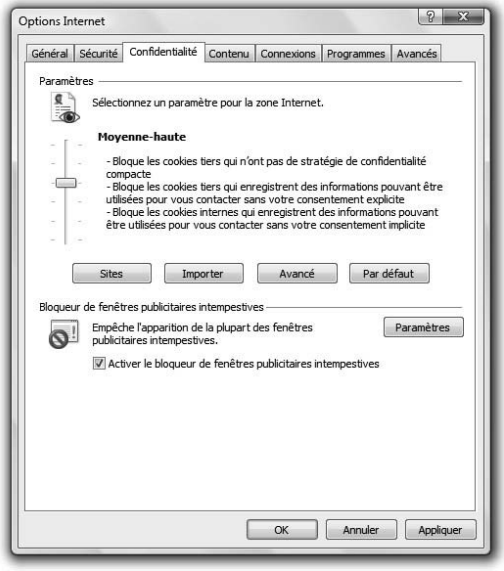
Astuce : Vous pouvez aussi accepter ou refuser les cookies au cas par cas. À cette fin, cliquez sur le bouton Sites sous l'onglet Confidentialité (figure 10-9). La boîte de dialogue Actions de confidentialité par site apparaît. Saisissez le nom du site, puis cliquez sur Refuser ou Autoriser.

Le curseur sur le côté gauche permet de définir le meilleur compromis entre le niveau de sécurité et la facilité d'utilisation. La fourchette est comprise entre Accepter tous les cookies et Bloquer tous les cookies. Voici quelques exemples (reportez-vous à la terminologie proposée plus haut) :

- **Bloquer tous les cookies** – Aucun cookie, sans exception. Les sites Web ne peuvent pas non plus lire les cookies existants.
- **Haute** – Aucun cookie d'aucun site Web qui n'a pas de stratégie de confidentialité compacte. Aucun cookie de sites qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement explicite.

- **Moyenne-haute** – Bloque tous les cookies tiers provenant de sites qui n'ont pas de stratégie de confidentialité compacte ou qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement explicite. Bloque les cookies internes qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement implicite.

Figure 10-9
Cette boîte de dialogue vous aide à protéger vos informations confidentielles. Vous pouvez y spécifier comment votre PC gère les cookies, qui restent avant tout des données placées sur votre disque dur par des sites Web extérieurs. « Moyenne-haute » est un bon compromis entre la protection de votre vie privée et les besoins des sites Web qui utilisent des cookies pour automatiser l'identification de l'internaute, notamment.



LE COIN DES EXPERTS

Examiner les cookies

Voulez-vous voir à quoi ressemblent les fichiers de cookies, tels qu'ils se trouvent sur votre disque dur ?

Vous les trouverez sur votre disque dur dans votre dossier personnel>AppData>Roaming>Microsoft>Windows>Cookies.

Leur nom est construit sur le modèle *dany@abc-news.com[1].txt*. Le nom du site Web ou du réseau publicitaire apparaît habituellement après l'arobase @, mais pas toujours ; parfois seul un nombre y figure.

Pour inspecter un cookie, ouvrez le fichier comme un quelconque fichier texte (dans Notepad ou dans WordPad, par exemple). Si en général, il ne contient qu'une liste de nombres et de lettres, vous trouverez parfois des informations utiles comme votre identifiant et votre mot de passe pour le site Web.

Si vous ne voulez plus du cookie sur votre disque dur, supprimez-le de la même manière que vous le feriez pour un autre fichier texte.

- **Moyenne (par défaut)** – Bloque les cookies tiers provenant de sites qui n'ont pas de stratégie de confidentialité compacte ou qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement implicite. Accepte les cookies internes de sites qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement implicite, mais les supprime à la fermeture d'Internet Explorer.

- **Basse** – Bloque les cookies tiers provenant de sites qui n'ont pas de stratégie de confidentialité compacte. Accepte les cookies tiers qui enregistrent des informations pouvant être utilisées pour vous contacter sans votre consentement implicite, mais les supprime à la fermeture d'Internet Explorer.
- **Accepter tous les cookies** – Tous les cookies sont bienvenus. Les sites Web peuvent lire les cookies existants.

Choisissez le paramètre voulu, puis cliquez sur OK. Vous êtes prêt à commencer à naviguer.

Info : Certains sites ne fonctionnent pas correctement (ou pas du tout) si vous choisissez de bloquer tous les cookies (avec la plupart des sites, vous ne pourrez par exemple effectuer aucune opération d'achat sans activer les cookies). Donc si vous choisissez le niveau de confidentialité Haute et si vous rencontrez des difficultés lorsque vous consultez vos sites favoris, revenez sur cet écran et essayez le réglage Moyenne-haute. Le réglage par défaut d'Internet Explorer est Moyenne.

Si vous êtes curieux de savoir si un site Web visité a placé des cookies sur votre disque dur pendant la session en cours, appuyez sur la touche Alt pour faire apparaître la barre de menus d'Internet Explorer. Choisissez Affichage>Déclaration de confidentialité de la page Web. Vous voyez ainsi la liste des sites consultés et les éventuels cookies qu'ils ont enregistrés sur votre PC.

Astuce : Si vous ne vous sentez pas concerné par les problèmes de sécurité, pensez à sauvegarder vos cookies par exemple pour les transférer sur un autre PC (pour faciliter votre identification) ou au cas où vos cookies seraient effacés.

Pour exporter ou sauvegarder vos cookies, ouvrez Internet Explorer. Appuyez sur la touche Alt pour faire apparaître les menus. Ensuite, choisissez Fichiers>Importer et exporter. L'Assistant Importation/Exportation démarre. Choisissez Exporter les cookies et suivez les instructions. Un simple fichier texte contenant tous vos cookies est créé dans votre dossier Documents (ou le dossier indiqué).

Pour importer les cookies sur un autre ordinateur (ou sur le même, suite à un désastre), lancez l'Assistant Importation/Exportation, choisissez Importer les cookies, puis recherchez le dossier dans lequel vous avez placé le fichier de sauvegarde.

À noter que le paranoïaque en sécurité choisit plutôt l'opération inverse : il cherche à se débarrasser systématiquement des cookies, quels qu'ils soient, le plus souvent possible.

Historique : effacez vos traces

Toutes les versions

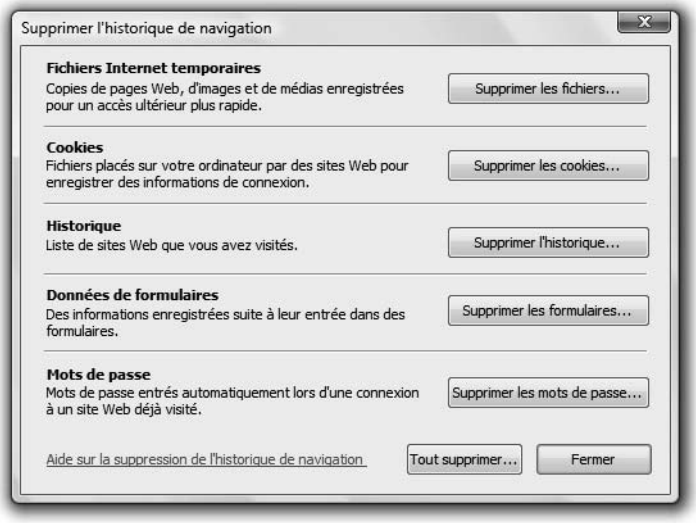
Vous seriez surpris d'apprendre tout ce qu'Internet Explorer conserve à votre sujet. En coulisses, il mémorise le moindre site Web auquel vous avez rendu visite. Il stocke vos cookies, bien sûr, ainsi que les mots de passe et les informations que vous saisissez dans les formulaires Web (vos nom et adresse, par exemple). Votre disque dur garde aussi des fichiers en mémoire cache : par exemple les images et les fichiers texte composant les pages Web proprement dites, et dont le stockage sur votre machine accélère considérablement l'affichage lors de vos prochaines visites sur l'un de ces sites.

Certaines personnes ne voient pas d'un très bon œil qu'Internet Explorer conserve la liste complète de tous les sites Web récemment consultés, à portée de main de tous les membres de la famille ou collègues qui viendraient à passer.

Heureusement, vous pouvez facilement effacer ces traces partiellement ou en totalité.

- Pour n'effacer qu'une entrée particulièrement compromettante de l'Historique, cliquez dessus avec le bouton droit de la souris dans l'Historique (section « Historique », chapitre 11). Dans le menu contextuel, choisissez Supprimer.
- Vous pouvez aussi supprimer n'importe quelle autre icône de l'Historique : l'un des petits dossiers d'un site Web ou l'un des dossiers de calendrier tel que celui nommé « il y a 3 semaines ».
- Pour vider tout l'Historique, choisissez Outils>Supprimer l'historique de navigation, puis cliquez sur Supprimer l'historique.
- La même boîte de dialogue (figure 10-10) comporte des boutons permettant d'effacer d'autres types de traces (les mots de passe, les fichiers temporaires, etc. Ou, si vous voulez faire table rase, vous pouvez cliquer sur Tout supprimer pour tout effacer en une seule opération.

Figure 10-10
La boîte de dialogue Supprimer l'historique de navigation permet d'effacer les traces de vos activités sur Internet, y compris l'historique, les cookies, les fichiers temporaires, les mots de passe et les données des formulaires. Souvenez-vous que lorsque vous supprimez l'une de ces catégories d'informations, la navigation Web en pâtira éventuellement. Si vous supprimez vos cookies, par exemple, vous devrez saisir à nouveau vos nom et mot de passe chaque fois que vous visitez un site tel qu'Amazon.



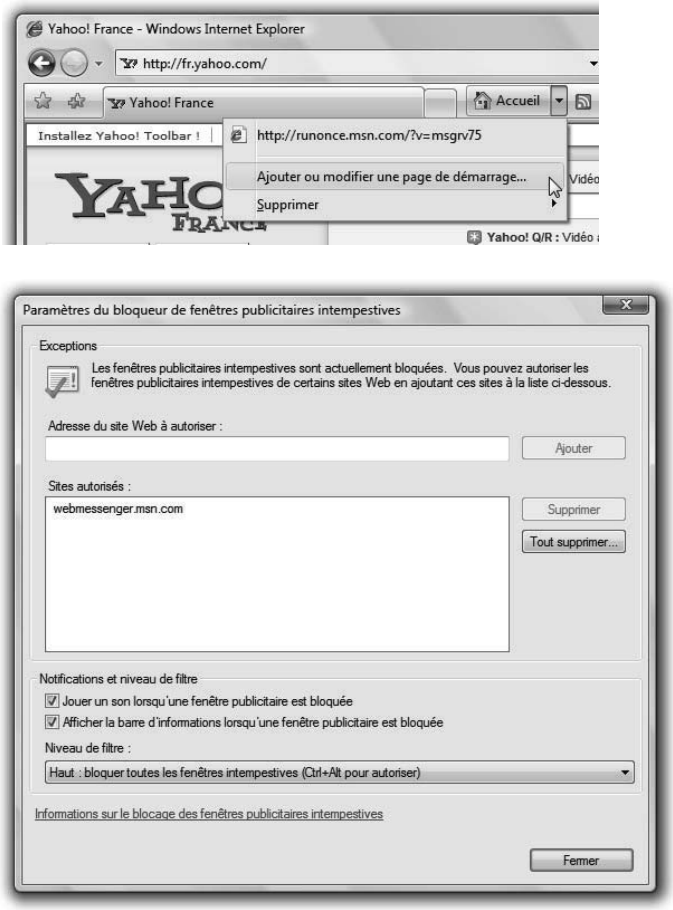
Le bloqueur de fenêtres publicitaires intempestives

Toutes les versions

Les bannières publicitaires, placées en haut de toutes les pages Web, sont déjà assez pénibles. Mais c'est malheureusement sans compter sur des publicitaires très malins qui parviennent à vous inonder de publicités sous forme de fenêtres surgissantes : celles-ci

jaillissent devant la fenêtre du navigateur ou au moment où vous vous apprêtez à la fermer. Elles sont souvent trompeuses, imitant des messages d'erreur ou des boîtes de dialogue et sont prêtes à tout pour que vous cliquiez dessus (figure 10-11).

Figure 10-11
En haut : Si vous cliquez sur le message « Une fenêtre publicitaire intempestive a été bloquée », vous pouvez choisir l'option Autoriser temporairement les fenêtres publicitaires intempestives ou appuyez simplement sur Ctrl+Alt pour voir ce qu'IE vient de stopper. Si les fenêtres surgissantes sont nécessaires au bon fonctionnement d'une page (tel qu'un écran de confirmation sur le site d'une agence de voyage), choisissez Toujours autoriser les fenêtres publicitaires intempestives de ce site.
En bas : Vous pouvez gérer la liste des sites dont les fenêtres publicitaires sont autorisées en choisissant Outils>Bloqueur de fenêtres publicitaires intempestives>Paramètres du bloqueur de fenêtres publicitaires intempestives. Cette boîte de dialogue apparaît, énumérant tous les sites Web autorisés (et proposant un bouton Supprimer si vous changiez d'avis). Vous pouvez aussi désactiver le signal sonore associé au blocage d'une fenêtre, éliminer la barre d'informations et ajuster le niveau de filtre des fenêtres intempestives (Haut, Moyen ou Bas).

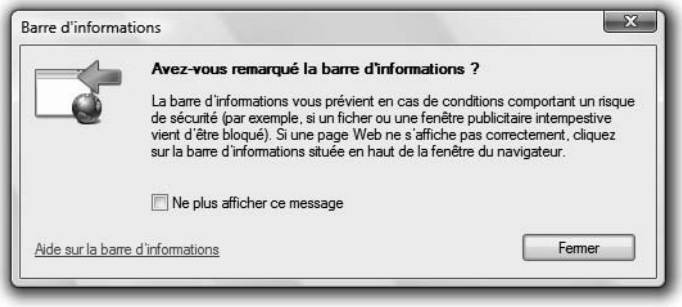


Les fenêtres publicitaires ne se contentent pas d'être pénibles ; elles sont aussi potentiellement nuisibles. Ce sont l'une des ruses favorites auxquelles les pirates ont recours pour déposer des logiciels espions sur votre PC. Un clic sur une fenêtre publicitaire peut lancer une procédure de téléchargement furtif. Cela vaut aussi lorsque la fenêtre publicitaire semble servir un objectif légitime, en vous demandant de répondre à un sondage, par exemple.

Internet Explorer est muni d'un bloqueur de fenêtres publicitaires intempestives. Il est automatiquement activé ; vous n'avez donc pas besoin d'intervenir. Au fil de la navigation, vous verrez s'afficher le message « Une fenêtre publicitaire intempestive a été bloquée » dans une barre d'informations jaune (figure 10-11, en haut).

Astuce : Au départ, IE ne se contente pas d'afficher le message dans la barre d'informations. Il ouvre aussi une petite boîte de dialogue (oui, une fenêtre surgissante) pour se vanter d'avoir bloqué une fenêtre publicitaire (figure 10-12). Pour éviter ce désagrément, cliquez sur Ne plus afficher ce message, puis cliquez sur OK. Comme la barre d'informations continue à s'afficher, vous êtes toujours informé lorsqu'une fenêtre publicitaire a été désamorcée.

Figure 10-12
Cet avertissement peut aussi devenir pénible à la longue, donc pensez à le désactiver en cliquant sur l'option Ne plus afficher ce message, puis sur OK.



Notez qu'IE bloque uniquement les fenêtres intempestives qui surgissent automatiquement et pas celles qui apparaissent lorsque vous cliquez sur quelque chose (tel que le plan d'une salle sur un site de vente de billets de spectacle). Il ne bloque pas non plus les fenêtres de votre réseau local ou des sites Web que vous avez définis comme étant des Sites de confiance (choisissez Outils>Options Internet>Sécurité, cliquez sur Sites de confiance, puis cliquez sur Sites).

Astuce : Dans la boîte de dialogue illustrée à la figure 10-11, le réglage Haut bloque toutes les fenêtres surgissantes, même celles qui apparaissent lorsque vous cliquez sur un lien. Dans ce cas, vous disposez quand même d'une solution pour voir la fenêtre en dépit du réglage : maintenez la touche Ctrl enfoncée au cours du chargement de la page Web.

Contourner le blocage des fenêtres

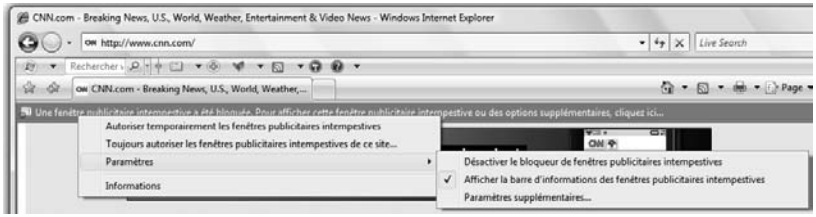
Dans certaines situations cependant, vous souhaiterez voir apparaître la fenêtre surgissante. En effet, certains sites utilisent ce type de fenêtre pour communiquer des informations (le plan d'une salle de concert ou la répartition des sièges dans un avion, par exemple).

Astuce : Lorsqu'une fenêtre utile parvient à franchir le Bloqueur de fenêtres publicitaires intempestives, elle apparaît généralement dans une petite fenêtre distincte. Vous pouvez également exploiter la nouvelle fonctionnalité des onglets de navigation d'Internet Explorer (chapitre 11) en demandant l'ouverture de la fenêtre surgissante dans un nouvel onglet.

Choisissez Outils>Options Internet, cliquez sur l'onglet Général, puis, sous la rubrique Onglets, cliquez sur Paramètres. Dans la boîte de dialogue Paramètres des onglets de navigation, cliquez sur Toujours ouvrir les fenêtres publicitaires intempestives dans un nouvel onglet, puis cliquez sur OK.

Pour autoriser l'affichage d'une telle fenêtre, cliquez sur la barre d'informations ; une boîte de dialogue apparaît. Vous pouvez y gérer les fenêtres surgissantes utilisées par un site Web particulier (figure 10-13).

Figure 10-13
Au blocage d'une fenêtre publicitaire, cliquez dans la barre d'informations pour accéder à diverses options. Si le site utilise des fenêtres surgissantes pour communiquer des informations utiles dans une nouvelle fenêtre, sélectionnez Toujours autoriser les fenêtres publicitaires intempestives de ce site.



Vous disposez des options suivantes :

- **Autoriser temporairement les fenêtres publicitaires intempestives** – Autorise les fenêtres surgissantes de ce site Web, mais uniquement pour la session de navigation en cours. À la prochaine session, les fenêtres surgissantes seront à nouveau bloquées.
- **Toujours autoriser les fenêtres publicitaires intempestives de ce site** – Cette option se passe de commentaires.
- **Paramètres** – Cette option permet de configurer le Bloqueur de fenêtres publicitaires intempestives. Dans le menu qui apparaît, sélectionnez Désactiver le bloqueur de fenêtres publicitaires intempestives pour empêcher le fonctionnement du bloqueur. Désactivez Afficher la barre d'informations des fenêtres publicitaires intempestives si vous ne voulez pas non plus voir la barre d'informations jaune qui apparaît lorsqu'une fenêtre est bloquée. Sélectionnez Paramètres supplémentaires pour afficher une fenêtre dans laquelle vous pouvez autoriser ou bloquer les fenêtres de sites particuliers (figure 10-14).

  Grâce à cette boîte de dialogue, vous contrôlez également la manière dont vous êtes averti du blocage d'une fenêtre publicitaire intempestive : par un son, par un message dans la barre d'informations ou par ni l'un ni l'autre. Vous pouvez aussi utiliser le menu Niveau de filtre pour abaisser ou augmenter le seuil de tolérance d'Internet Explorer envers des fenêtres publicitaires. Le niveau Haut, par exemple, bloque toutes les fenêtres surgissantes, même celles qu'Internet Explorer juge nécessaire au bon fonctionnement d'un site.

Info : Si vous avez installé le bloqueur de fenêtres publicitaires intempestives proposé par un autre éditeur, vous pouvez désactiver la version d'IE en choisissant Outils>Bloqueur de fenêtres publicitaires intempestives>Désactiver le bloqueur de fenêtres publicitaires intempestives.

Zones de sécurité Internet

Toutes les versions

Dans le monde réel, vous savez probablement où se trouvent les quartiers mal famés et vous évitez d'y aller après la nuit tombée. Sur le Web, ce n'est pas aussi simple. La page Web la plus agréable à regarder peut être un piège conçu par des hackers sournois pour installer des virus sur votre PC.

Figure 10-14
Voici une autre méthode permettant d'autoriser les fenêtres publicitaires de certains sites Web : saisissez une adresse, puis cliquez sur Ajouter. Cette même boîte de dialogue apparaît aussi lorsque vous cliquez sur la barre d'informations après le blocage d'une fenêtre et que vous sélectionnez Paramètres.

Les Zones de sécurité sont une autre fonctionnalité d'Internet Explorer (pré-Vista) élaborée dans le but de limiter les voies empruntées par les pirates pour pénétrer dans votre PC. Comme leur mode de fonctionnement est assez complexe, peu de gens s'en préoccupent.

Si vous avez beaucoup de temps devant vous, vous pouvez vous amuser à affecter les sites Web à différents niveaux de protection du navigateur (zones) en fonction du niveau de confiance que vous leur accordez. Internet Explorer refuse de télécharger des objets potentiellement dangereux (comme des modules ActiveX) provenant de sites appartenant aux zones sensibles.

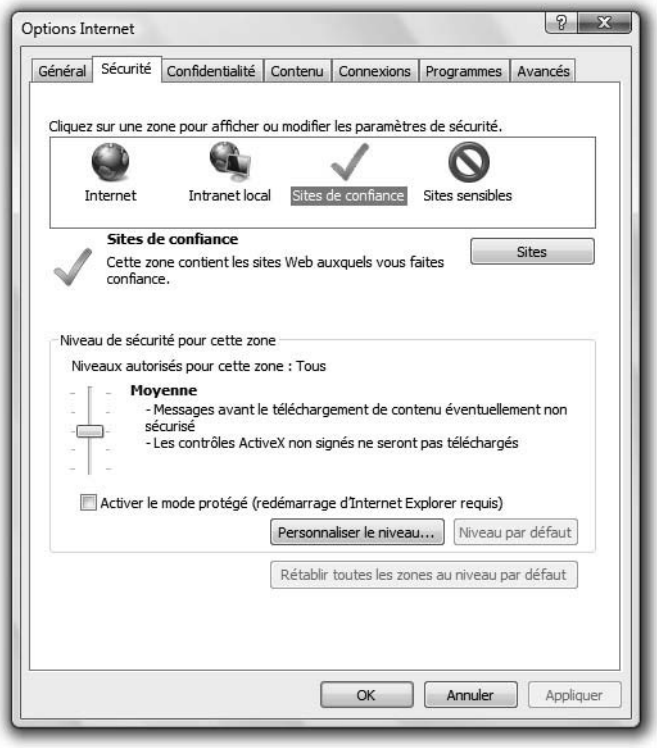
Ainsi, les sites Web internes, sur le réseau de votre entreprise, ont peu de chances d'être infectés par des logiciels espions et des virus (à moins que l'administrateur réseau ne

soit lui-même corrompu). Ces sites internes font automatiquement partie de la zone Intranet local ayant un niveau de sécurité faible. Si vous gérez un site Web de chez vous, il appartient aussi à cette zone.

Il existe également des zones nommées Sites de confiance (sécurité faible) et Sites sensibles (sécurité élevée), mais vous devez placer manuellement des sites Web dans ces zones, comme décrit plus loin. Tout site n'ayant pas été placé manuellement dans une zone appartient automatiquement à la zone Internet (sécurité moyenne).

Pour voir les différentes options, choisissez Outils>Options Internet>Sécurité depuis Internet Explorer (figure 10-15).

Figure 10-15
L'onglet Sécurité des Options Internet permet de contrôler les paramètres de sécurité relatifs à la navigation sur le Web avec Internet Explorer. Personnalisez les paramètres de chaque zone en faisant glisser le curseur vers le haut pour une sécurité renfoncée ou vers le bas pour une sécurité moindre.



Niveau de sécurité

Que signifie exactement « sécurité moyenne » ou « sécurité haute »? Ces paramètres définissent le comportement du navigateur lorsqu'il se trouve dans des situations qui ont potentiellement à voir avec la sécurité. Par exemple, ils régissent l'autorisation ou l'interdiction de télécharger des fichiers, ou bien l'utilisation par Internet Explorer de petits programmes intégrés aux pages Web, comme les applets Java ou les contrôles ActiveX. Les applets Java sont des petits programmes qui dotent les pages Web de composants interactifs, tels que des jeux ou des cartes météo.

Voici ce qui est prévu par les différents niveaux de sécurité :

- **Haute** – Bloque toutes les fonctionnalités qui pourraient être des vecteurs d'infection du navigateur : contrôles ActiveX, Java et applets Java, téléchargements.
- **Moyenne** – Signifie que chaque fois qu'un site Web déclenche l'exécution d'un contrôle ActiveX, un message vous demande votre permission. Les contrôles ActiveX non signés, c'est-à-dire ceux dont Internet Explorer n'est pas sûr de l'origine, ne sont pas exécutés. Les téléchargements et les applets Java sont autorisés.
- **Moyenne-basse** – Identique à Moyenne, mais certains programmes ActiveX sont exécutés sans votre autorisation préalable.
- **Basse** – Tous les contrôles ActiveX et les autres petits programmes Web sont exécutés. Votre avis est rarement sollicité.

LE COIN DES EXPERTS

Personnalisation à l'infini

Si les paramètres de sécurité de chaque zone ne vous conviennent pas, vous pouvez les modifier. Si, par exemple, vous ne disposez d'aucun objet précieux sur votre machine (données sensibles, fichiers musicaux, etc.), vous pouvez demander à Internet Explorer de traiter la zone Internet avec un niveau de sécurité Moyenne-basse.

Dans Internet Explorer, choisissez Outils>Options Internet>Sécurité pour accéder à la boîte de dialogue illustrée à la figure 10-15. Pour Intranet local et Sites de confiance, cliquez sur la zone, puis faites glisser le curseur. Pour Internet et Sites sensibles, cliquez sur la zone. Ensuite, cliquez sur Personnaliser le niveau ; dans la boîte de dialogue Paramètres de sécurité, sélectionnez le nouveau niveau de sécurité requis dans la liste « Rétablir », puis cliquez sur OK.

Et, à propos des réglages que peu de personnes se donnent la peine d'ajuster, sachez que vous pouvez aussi modifier le paramétrage d'une zone, c'est-à-dire agir individuellement sur chacun des nombreux paramètres qui définit le comportement du navigateur par rapport à cette zone (téléchargements ou non de codes mobiles, autorisation ou non d'exécution des scripts, le lancement ou non de programmes dans un IFRAME, etc.). Ces paramètres vous offrent des réglages beaucoup plus fins que les simples niveaux Haute, Moyen-haut, Moyenne, Moyenne-basse et Basse.

À cette fin, cliquez sur une zone, puis sélectionnez Personnaliser le niveau. La boîte de dialogue Paramètres de sécurité apparaît. Définissez vos propres choix en ce qui concerne, entres autres, l'installation des éléments sur le Bureau, la manière de traiter les contrôles ActiveX, etc. Puis, cliquez sur OK.

Classification manuelle des sites

Vous ne devez pas nécessairement vous fier au jugement de Microsoft sur la répartition des sites dans les différentes zones : vous pouvez les classer vous-même. Si vous faites confiance à un site Web particulier, vous pouvez le placer dans la zone Sites de confiance.

À cette fin, sélectionnez une zone, cliquez sur Sites puis, dans la boîte de dialogue qui apparaît, saisissez l'URL du site Web et cliquez sur Ajouter.

Sécurité des points d'accès

Toutes les versions

En ce début du nouveau millénaire, l'un des progrès les plus appréciables de l'informatique est le point d'accès sans fil public qui permet de connecter votre ordinateur portable WiFi à Internet, en haut débit et souvent gratuitement. Vous trouverez des points

d'accès dans des cafés, des hôtels, des aéroports et d'autres lieux publics (le site *www.linternaute.com/wifi* propose un annuaire des points d'accès WiFi).

Mais, à moins d'être prudent, il vous en coûtera plus qu'un expresso au café du coin si vous vous connectez à ces points d'accès ; on risque de vous y espionner. En théorie, quiconque assis non loin de vous peut utiliser des programmes gratuits et faciles à se procurer pour espionner les informations transmises à partir de votre portable. Les messages envoyés, vos nom et mot de passe, et même les images des pages Web que vous consultez peuvent être interceptés.

Il n'y a cependant pas vraiment de quoi s'alarmer ; ce n'est pas une raison pour vendre votre ordinateur portable et partir vivre dans une région reculée. Il suffit de prendre quelques précautions pour être à l'abri des déconvenues :

- **Informez Windows que c'est un réseau public** – Lors de la première connexion à un réseau sans fil, Windows Vista vous demande si c'est un réseau public ou privé. Choisissez Public pour bénéficier d'un seuil de protection intégrée supplémentaire. Techniquement parlant, Vista désactive la fonction de détection de réseaux, grâce à laquelle votre PC annonce sa présence aux autres ordinateurs du réseau. Malheureusement, des personnes malveillantes utilisant des logiciels de détection spéciaux peuvent quand même vous trouver s'ils sont persévérants.
- **Désactivez le partage de fichiers** – Vous ne voulez certainement pas que vos voisins accros à la caféine puissent accéder à vos fichiers. Désactivez le partage de fichiers en choisissant Panneau de configuration>Configurer le partage de fichiers. Désactivez le partage de fichiers et le partage de dossiers publics.
- **Surveillez le cadenas** – Vous n'avez généralement pas de raison de vous méfier des boutiques et des banques en ligne. Lorsque vous voyez l'icône du petit verrou dans Internet Explorer (ou lorsque l'URL figurant dans la barre d'adresse commence par « https » au lieu de « http »), cela signifie que vous vous trouvez sur un site Web sécurisé. Vos transmissions sont chiffrées dans les deux directions et ne peuvent pas être espionnées.
- **Regardez par-dessus votre épaule** – Le piratage n'implique pas toujours des moyens techniques ; il suffit que la personne regarde par-dessus votre épaule pour voir le mot de passe que vous saisissez. Prenez garde à ce que personne ne voit ce que vous tapez.
- **Ne laissez pas votre portable sans surveillance** – Le café est bien connu pour ses propriétés diurétiques, alors si vous aviez besoin de vous soulager, ne laissez pas votre portable sans surveillance. Remettez-le dans sa sacoche et emportez-le avec vous ou prévoyez une chaîne et un cadenas pour l'attacher à la table.
- **Utilisez un réseau privé virtuel (VPN)** – Si quelqu'un intercepte le courrier que vous envoyez à votre mère, ce ne sera pas la fin du monde. Mais si vous travaillez sur un projet confidentiel exigeant une protection maximale, vous pouvez employer un logiciel de réseau privé virtuel (*virtual private network* ou VPN) sans fil qui chiffre toutes les données que vous envoyez ou recevez. Personne ne pourra s'en emparer depuis le point d'accès en utilisant un logiciel d'espionnage. Par exemple, Thalès commercialise le produit Minicita, actuellement l'une des meilleures offres du marché, qui permet d'échanger en toute sécurité des fichiers

confidentiels à partir de votre poste nomade et n'importe quel un point d'accès public. Les flux sont chiffrés au travers d'un VPN bâti sur des mécanismes cryptologiques issus du monde de la défense (*http://www.thales-esecurity.com/*).

Allez au Panneau de configuration>Réseau et Internet>Centre réseau et partage>Configurer une connexion ou un réseau. Sélectionnez Connexion à votre espace de travail et suivez les instructions selon la documentation du constructeur.

Protection de votre réseau sans fil domestique

Toutes les versions

Les points d'accès sans fil publics ne sont pas les seuls à présenter un risque théorique pour la sécurité ; votre réseau sans fil à la maison peut aussi être attaqué par des pirates. Il est possible, bien que rare, que des *war drivers* (des gens qui se promènent avec un ordinateur portable à la recherche de réseaux WiFi domestiques non sécurisés) se connectent à votre réseau pour télécharger des vidéos de pornographie enfantine ou envoyer du courrier indésirable.

On les neutralise assez facilement :

- **Activez le chiffrement sans fil** – Lorsque vous configurez votre routeur WiFi (également nommé station de base ou point d'accès), vous avez la possibilité de protéger votre réseau par un mot de passe. Faites-le. Les routeurs sans fil récents proposent trois types de chiffres : WEP, WPA et WPA2. Dans la mesure du possible, utilisez WPA2 ou, à la rigueur, WPA ; WEP n'offre pratiquement aucune protection.

  Vous devez ensuite utiliser le chiffre correspondant sur chaque PC sans fil relié au réseau. Ouvrez le Panneau de configuration>Réseau et Internet>Centre réseau et partage>Gérer les réseaux sans fil, puis faites un clic droit sur votre réseau. Choisissez Propriétés>Sécurité. Saisissiez les informations de chiffrement qui correspondent à ce que vous avez saisi pour le routeur.

Info : Vous n'avez pas besoin de saisir ce mot de passe chaque fois que vous voulez vous connecter au réseau ! Vista vous propose de le mémoriser.

- **Interdire les PC indésirables** – De nombreux routeurs incluent une fonctionnalité qui permet de limiter l'accès au réseau à certains ordinateurs sans fil. Un PC ne figurant pas dans la liste ne sera pas autorisé à se connecter. La fonctionnalité se nomme Filtrage par adresse MAC (et n'a aucun rapport avec les ordinateurs Macintosh). Une adresse MAC est un numéro de série censé identifier de manière unique un composant matériel réseau.

  Tous les routeurs ne prennent pas en charge cette fonctionnalité et la marche à suivre varie en fonction du routeur employé. Consultez éventuellement la documentation d'accompagnement. Pour un Linksys SRX 400, par exemple, connectez-vous à l'écran d'administration du routeur par l'intermédiaire de votre navigateur Web, puis sélectionnez Sans fil>Accès réseau sans fil. Sur l'écran rempli de champs vides, saisissez l'adresse MAC du PC que vous voulez autoriser à accéder au réseau.

Astuce : Pour découvrir l'adresse MAC d'un PC, dans le menu Démarrer ouvrez la boîte de dialogue Exécuter, puis saisissez *cmd* et cliquez sur OK. Dans l'invite de commande, saisissez *ipconfig /all* et appuyez sur Entrée. Dans la liste d'informations qui apparaît, recherchez l'entrée « Adresse physique ». Il s'agit de l'adresse MAC.

Renseignez toutes les adresses MAC dans les champs du routeur Linksys, cliquez sur Enregistrer les paramètres et c'est tout.

- **Placez judicieusement votre routeur** – En plaçant votre routeur WiFi au cœur de la maison, vous réduisez les risques de « fuite » du signal dans le proche voisinage.

Contrôles parentaux

Toutes les versions

Les sites aux contenus dérangeants sur Internet (violence, pornographie, incitation à la haine, sites de vente illégale de médicaments, etc) sont trop facilement accessibles aux enfants. Et c'est à juste titre que les parents s'en inquiètent.

Une nouvelle fonctionnalité Vista vous offre un moyen d'empêcher ces contenus d'être vus sur votre PC : il s'agit des contrôles parentaux. Ils sont simples d'emploi et assez exhaustifs.

Allez au Panneau de configuration>Configurer le contrôle parental pour un utilisateur (sous la catégorie Compte d'utilisateurs et protection des utilisateurs). Identifiez-vous (voir l'encadré « Identifiez-vous : contrôle de compte d'utilisateur », au début du chapitre 6).

La boîte de dialogue illustrée à la figure 10-16 apparaît. Elle énumère tous les comptes d'utilisateurs du PC (chapitre 23). L'un des principaux avantages du système de comptes est que vous pouvez configurer des environnements séparés pour chaque membre de la famille. C'est ici que vous êtes récompensé de vos efforts.

Cliquez sur le compte de vos enfants pour ouvrir son écran de contrôles parentaux. Si vous n'avez pas encore créé de compte pour vos enfants, vous pouvez commencer par les créer ici.

Sous la rubrique Contrôle parental, cliquez sur « Activé, les paramètres actuels sont appliqués ». Vous pouvez maintenant définir le cadre de l'utilisation du PC par vos enfants :

- **Filtre Windows Vista de restrictions d'accès au Web** – Bloque l'accès aux sites Web douteux et empêche tout téléchargement Web.

  Lorsque vous cliquez sur ce lien, une fenêtre de configuration permet de définir la sévérité des contrôles appliqués. Vous pouvez définir un blocage automatique basé sur le contenu de chaque site en utilisant les paramètres prédéfinis Haute, Moyen, Aucun ou Personnalisé (figure 10-17).

Astuce : Le paramètre Haute indique à Internet Explorer de n'ouvrir que des sites Web spécialement conçus pour les enfants.

Vous pouvez aussi saisir l'adresse de certains sites Web auquel vous voulez interdire l'accès. Dans ce cas, activez Autoriser uniquement les sites Web de la liste verte, puis cliquez sur Modifier la liste verte et rouge.

Figure 10-16
Les contrôles parentaux permettent de contrôler l'usage que font vos enfants du PC et d'Internet. De nombreux parents seront intéressés par le Filtre Windows Vista de restrictions d'accès au Web, qui permet de filtrer les sites Web au contenu douteux et d'empêcher les enfants de télécharger des logiciels.

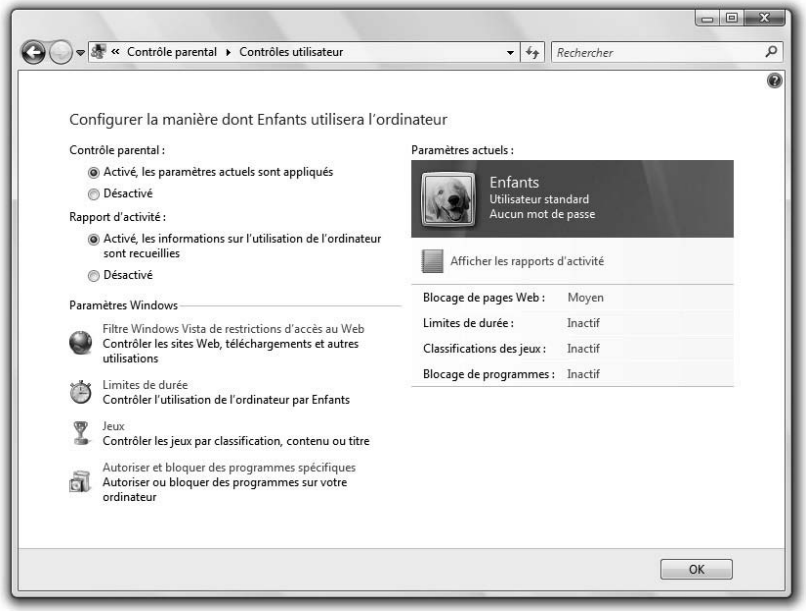
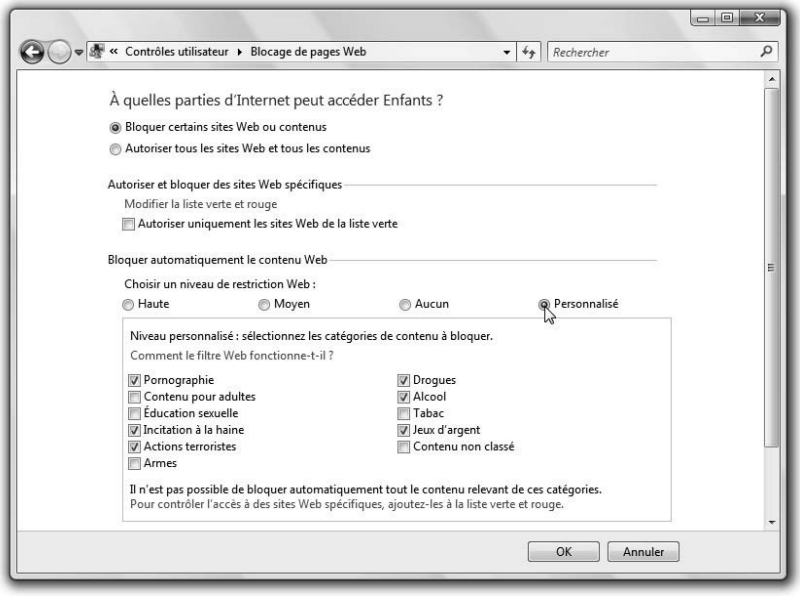


Figure 10-17
L'option Personnalisé permet d'indiquer exactement ce que vous considérez comme douteux. Ne laissez pas votre enfant de 12 ans voir cette liste ; elle pourrait lui servir de source d'inspiration.



Enfin, ne ratez pas la case à cocher Bloquer les téléchargements de fichiers. Si vous voulez que votre PC reste sain, activez cette option. Vos enfants ne pourront rien télécharger depuis le Web (pas de chansons, de jeux, de vidéos, et donc pas de virus, de logiciels espions et de vers).

LE COIN DES NOSTALGIQUES

Contrôle d'accès

Une autre fonctionnalité d'Internet Explorer liée à la sécurité vaut la peine d'être mentionnée : le Contrôle d'accès.

À l'époque, Microsoft souhaitait permettre aux parents de contrôler ce que leurs enfants pouvaient voir sur le Web. À l'aide de cette fonctionnalité, vous indiquez les sites que vous approuvez, ainsi que les sites que vous voulez bloquer. Si quelqu'un essaye de consulter un site Web auquel vous avez interdit l'accès en recourant à cette fonctionnalité, un message s'affiche pour signaler que ce site n'est pas disponible.

Le Contrôle d'accès n'a pas grand intérêt car il n'est pas aussi utile et facile à définir que les Contrôles parentaux. Son efficacité est également toute relative, car il repose en partie sur l'évaluation des sites Web, à ceci près que ce sont les sites Web qui procèdent à leur propre évaluation. Autant dire que la fiabilité de ce sytème laisse vraiment à désirer.

Si cette fonctionnalité vous intéresse, vous en apprendrez davantage dans le fichier Content Advisor.pdf (en anglais et téléchargeable gratuitement). Vous le trouverez sous la rubrique « Missing CD-ROM » de ce manuel à l'adresse *www.missingmanuals.com.*

- **Limites de durée** – Permet de définir les jours et créneaux horaires auxquels vos tornades blondes ont accès à l'Internet. Vous pouvez, par exemple, décider d'empêcher vos enfants d'utiliser le PC les soirs d'école. Lorsque vous cliquez sur Limites de durée, un calendrier apparaît et vous pouvez y bloquer certains horaires en les sélectionnant.
- **Jeux** – Empêche votre progéniture de jouer à n'importe quel jeu ou permet d'indiquer le type de jeux auxquels vos enfants peuvent jouer : 3 ans et plus, 18 ans et plus. Vous pouvez aussi personnaliser chaque niveau en bloquant des types de contenus particuliers à l'intérieur des jeux (drogues, violence, etc.).

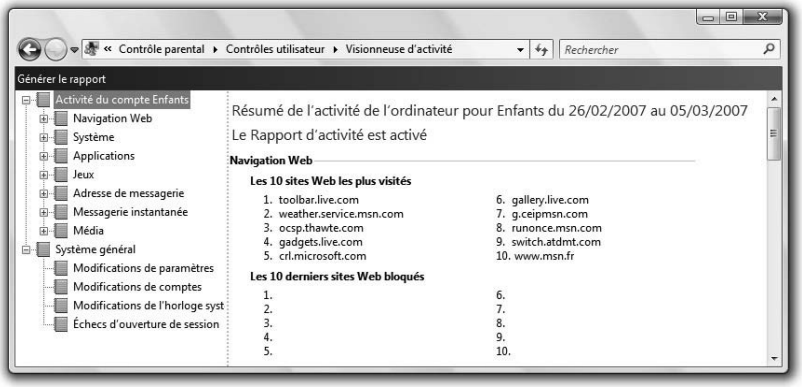
Info : Pour permettre la mise en oeuvre de cette fonctionnalité, Vista consulte un petit fichier GDF (fichier de définition de jeux) que les éditeurs de logiciels peuvent ajouter à leur jeu. Les éditeurs de jeux utilisent habituellement des classifications définies par des organismes tels que l'Entertainment Software Ratings Board (ESRB).

Si un éditeur utilise des informations obéissant à une autre norme ou s'il ne fournit pas de fichier de classification GDF, Vista consulte la base de données de Microsoft répertoriant plus de 2 000 jeux. Et si cette source n'a pas non plus eu vent de ce jeu, Vista considère le jeu comme étant sans classification. Vous avez peut-être remarqué que la fenêtre des Restrictions de jeu des Contrôles parentaux comporte une option Bloquer les jeux sans classification, qui a été conçue pour ce type de situations.

- **Autoriser et bloquer des programmes spécifiques** – Permet de déclarer certains programmes de votre PC comme étant interdits. Dans la fenêtre de configuration, activez Tim [ou quiconque] peut uniquement utiliser les programmes que j'autorise. Windows présente une liste contenant le moindre programme installé sur votre PC ; activez les cases à cocher des programmes que votre enfant a le droit d'utiliser. Cliquez sur OK.

- **Afficher les rapports d'activité** – Les rapports des contrôles parentaux sont particulièrement détaillés ; ils vous donnent une bonne vision de tout ce que vos enfants ont fait sur le PC. Par exemple, ils affichent les 10 sites Web qu'ils ont le plus visités, les 10 derniers sites Web bloqués, les fichiers téléchargés et les téléchargements de fichiers bloqués. Vous voyez aussi l'heure à laquelle votre enfant a ouvert une session sur le PC et la durée de chaque session. Et ce n'est qu'un début (figure 10-18).

Figure 10-18
Le rapport parental présente le moindre programme ou jeu que votre enfant a utilisé, quand il l'a utilisé et pendant combien de temps. Il indique aussi si le programme était bloqué. Vous y voyez également la musique ou les vidéos qu'il a lues, les informations concernant les sessions de messagerie instantanée et les courriers électroniques envoyés.



Il ne vous reste plus qu'à faire valoir les nouvelles limites que vous imposez au jeune détenteur de compte. Windows Vista ne propose pas de nouvelles fonctionnalités qui vous viendraient en aide ici.