

Gracieuseté de 

La TI et la petite entreprise

POUR

LES NULS^{MD}

Chapitre 5

**Gardez votre
ordinateur à l'abri
des virus!**

**À mettre
entre toutes
les mains!**

Conseils gratuits à dummies.com



Heather Ball

La TI et la petite entreprise Pour les Nuls^{4e}

Publié par

John Wiley & Sons Canada, Ltd.

6045 Freemont Blvd.

Mississauga (Ontario) L5R 4J3

www.wiley.com

© 2008 John Wiley & Sons Canada, Ltd. Tous droits réservés.

Toute reproduction, même partielle, du contenu, de la couverture ou des icônes, par quelque procédé que ce soit (électronique, photocopie, bande magnétique ou autre) est interdite sans l'autorisation écrite de la maison d'édition.

ISBN : 978-0-470-15983-5

Pour des détails sur la façon de créer un livre personnalisé pour votre compagnie ou organisation, ou pour obtenir plus de renseignements sur le programme d'édition personnalisée de John Wiley & Sons Canada, veuillez composer le 416-646-7992 ou envoyer un courriel à cupubcan@wiley.com.

Pour toute information d'ordre général sur John Wiley & Sons Canada, Ltd., y compris sur tous les livres publiés par Wiley Publishing, inc., veuillez communiquer avec notre dépôt au 1-800-567-4797. Pour toute information concernant les revendeurs, y compris les rabais et les ventes à primes, veuillez appeler notre service des ventes au 416-646-7992. Pour obtenir des copies des critiques de presse, des entrevues avec l'auteur ou toute autre information publicitaire, veuillez communiquer avec notre service de marketing par téléphone au 416-646-4584 ou par télécopieur au 416-236-4448.

LIMITE DE RESPONSABILITÉ/DÉNI DE GARANTIE : L'ÉDITEUR ET L'AUTEUR N'ÉMETTENT AUCUNE REPRÉSENTATION OU GARANTIE QUANT À L'EXACTITUDE OU À L'INTÉGRALITÉ DU CONTENU DU PRÉSENT OUVRAGE; EN PARTICULIER, ILS NIENT TOUTE GARANTIE, Y COMPRIS, SANS Y ÊTRE LIMITÉ, LES GARANTIES D'APPROPRIATION POUR UN USAGE PARTICULIER. AUCUNE GARANTIE NE PEUT ÊTRE CRÉÉE OU OFFERTE PAR LES REPRÉSENTANTS COMMERCIAUX OU DANS LES DOCUMENTS DE VENTE. LES CONSEILS ET STRATÉGIES CONTENUS DANS CET OUVRAGE PEUVENT NE PAS CONVENIR À VOTRE SITUATION. LE PRÉSENT OUVRAGE EST PUBLIÉ, ÉTANT ENTENDU QUE L'ÉDITEUR N'OFFRE PAS DE SERVICES JURIDIQUES, COMPTABLES OU AUTRES SERVICES PROFESSIONNELS. LES LECTEURS QUI VEULENT OBTENIR UNE AIDE PROFESSIONNELLE DOIVENT S'ADRESSER À UN PROFESSIONNEL COMPÉTENT. NI L'ÉDITEUR NI L'AUTEUR NE SERONT TENUS RESPONSABLES DE DOMMAGES QUELCONQUES DÉCOULANT DU CONTENU DU PRÉSENT OUVRAGE. LA MENTION D'UNE ORGANISATION OU D'UN SITE WEB DANS LE PRÉSENT OUVRAGE EN CITATION ET/OU COMME SOURCE POTENTIELLE DE RENSEIGNEMENTS NE SIGNIFIE PAS QUE L'AUTEUR OU L'ÉDITEUR ENTÉRINENT LES RENSEIGNEMENTS OU LES RECOMMANDATIONS QUE PEUVENT FOURNIR L'ORGANISATION OU LE SITE WEB. EN OUTRE, LES LECTEURS DOIVENT SAVOIR QUE LES SITES WEB MENTIONNÉS DANS LE PRÉSENT OUVRAGE PEUVENT AVOIR CHANGÉ OU DISPARU DEPUIS LA RÉDACTION DE L'OUVRAGE.

Marques de commerce : Wiley, le logo de Wiley Publishing, Pour les Nuls, le logo du personnage Dummies Man, A Reference for the Rest of Us!, À mettre entre toutes les mains!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com, ainsi que la présentation des produits sont des marques de commerce ou des marques déposées de John Wiley & Sons, inc. aux États-Unis, au Canada et tout autre pays, et ne doivent pas être utilisés sans autorisation écrite. La maison d'édition John Wiley & Sons Canada, Ltd. n'est pas associée aux produits ou aux fournisseurs mentionnés dans le présent ouvrage.



Chapitre 5

Votre ordinateur et la sécurité Internet

.....

Dans ce chapitre

- ▶ Protéger votre ordinateur
 - ▶ Savoir reconnaître vos ennemis
 - ▶ Préparer votre défense
 - ▶ Faire des copies de sauvegarde
-

Il est certain qu'Internet constitue une communauté en effervescence qui regorge d'information, mais votre ordinateur est-il en sécurité? De nos jours, presque tout le monde peut se connecter, et Internet étant un système ouvert, nombreux sont les voyous qui y sont à l'affût d'une proie. Ils créent des programmes qui peuvent faire des dégâts sur votre ordinateur si vous n'êtes pas vigilants.

Mais n'ayez crainte! Les moyens ne manquent pas pour protéger votre ordinateur contre tout programme indésirable et pour qu'il continue à ronronner paisiblement. Vous trouverez dans ce chapitre des explications sur ce qui menace potentiellement votre ordinateur et les mesures que vous pouvez prendre pour y remédier.

Commençons par le commencement

Pas besoin de ranger votre ordinateur dans une chambre forte, d'inscrire le code sur un petit bout de papier et de l'avaler pour que personne ne le trouve; pas besoin non plus

de l'enchaîner dans un coffre-fort avant de jeter le tout au fond de l'océan, à la Houdini. Non, les premières choses que vous pouvez faire pour protéger votre ordinateur sont en fait très simples et à la portée de tout le monde.

Suivez votre instinct

La première chose qui peut vous aider à éviter toute contamination ne se trouve pas sur un CD ou sur Internet. Non, votre première ligne de défense est votre bon sens.

En effet, les virus informatiques qui se sont le plus propagés ont réussi à le faire simplement grâce à la nature humaine. Les vauriens (et vauriennes!) misent sur les *caractéristiques humaines*, notamment votre capacité à vous laisser entraîner à faire quelque chose que vous ne feriez pas normalement, comme par exemple ouvrir une pièce jointe suspecte dans un courriel ou cliquer sur un hyperlien douteux, parce que l'on vous fait croire que votre ordinateur est en danger!



Si un site Web vous semble louche, ou si l'adresse de l'émetteur d'un de vos courriels ne vous inspire pas entièrement confiance, écoutez votre sixième sens! Mieux vaut prévenir que guérir! Il est bien plus facile (et moins onéreux) d'éviter les virus que d'essayer de s'en débarrasser une fois que le mal est fait.

Choisissez des mots de passe forts

Tout le monde n'active pas la fonction mot de passe pour empêcher que n'importe qui se serve de son ordinateur. Si vous voulez notre humble avis, vous devriez le faire! Même si cela n'élimine pas tous les risques, un simple mot de passe peut vous aider à éviter que l'information qui se trouve sur votre ordinateur ne finisse entre les mains de quelqu'un d'indésirable.

Les mots de passe forment souvent la première ligne de protection sur votre ordinateur.

Un identificateur d'utilisateur est un simple nom et ne permet pas de vérifier une identité, contrairement au mot de passe qui y est associé et qui, lui, sert d'identificateur.



Les mots de passe sont les clés qui permettent d'entrer dans votre ordinateur, et les pirates trouvent facilement les mots de passe faibles. Un seul mot de passe faible peut permettre à n'importe qui d'entrer dans votre ordinateur et donc d'avoir accès à tout ce qui s'y trouve.

Pour savoir comment choisir un mot de passe fort, consultez le chapitre 4.

Repérez vos ennemis et préparez votre ligne de défense

Votre ordinateur peut avoir la visite de tout un tas de voyous. Certains des noms mentionnés dans la présente section vous diront peut-être quelque chose. Comme c'est le cas pour tout ce qui se rapporte à l'informatique, les logiciels malveillants (*les maliciels*) ont souvent un nom super technique ou au contraire super bête. Ils sonnent bien, mais ne sont généralement pas très évocateurs. Vous trouverez ci-dessous les types de programmes malveillants et désagréables qui guettent votre ordinateur et se feront un plaisir de se jeter dessus.

L'hameçonnage

Connue en anglais sous le terme *phishing*, cette technique s'applique à une page Web ou un courriel qui vise à vous faire croire que vous avez affaire à un tiers de confiance, comme la page Web de votre banque. Ces sites ou courriels frauduleux vont à la pêche aux renseignements et essaient de vous soutirer vos numéros de compte et mots de passe. Vous ne vous méfiez pas et leur fournissez l'information demandée, puisqu'ils ont l'air légitimes. Mais ce n'est pas le cas.

Ce type d'escroquerie est très répandu, parce que les pirates réussissent à ce que des utilisateurs naïfs fassent des choses qu'ils ne feraient pas normalement. Par chance, de petits programmes bien pratiques, inclus dans votre navigateur Web (filtres ou protection anti-hameçonnage), réduisent vos risques de tomber dans les mailles du filet de ces pêcheurs mal intentionnés.

Ces *filtres* vérifient si les sites que vous visitez figurent sur la liste à jour des sites hameçonnés connus. Si vous vous retrouvez sur un site Web douteux, votre navigateur vous met en garde.

Si vous utilisez le navigateur Firefox, la protection anti-hameçonnage est activée par défaut. Vérifiez quand même le niveau de sécurité sélectionné et modifiez-le s'il ne vous convient pas.

Si vous utilisez Internet Explorer (IE), il se peut que le filtre ne soit pas activé. Pour vérifier quels paramètres sont sélectionnés, suivez les étapes suivantes :

1. Cliquez sur le bouton *Outils* de la barre d'outils.

Un menu déroulant apparaît.

2. Sélectionnez *Filtre d'hameçonnage*.

Le sous-menu Filtre d'hameçonnage apparaît. Quelle commande apparaît? Si c'est la commande Désactiver la vérification automatique de sites Web, cela veut dire que votre filtre est activé. Sinon, passez à l'étape 3.

3. Sélectionnez *Activer la vérification automatique de sites Web*.

La boîte de dialogue spéciale pour la sécurité, Filtre d'hameçonnage Microsoft, apparaît.

4. Cliquez sur OK dans la boîte de dialogue Filtre d'hameçonnage Microsoft.

Le filtre d'hameçonnage est alors activé.

Le filtre d'hameçonnage vous prévient lorsque tout hyperlien semble mener à des eaux troubles : le lien en question prétend mener à une page Web bien précise, mais en réalité elle vous redirige sur une autre page; ou bien le lien mène à un site qui « maltraite » les renseignements personnels des visiteurs. Dans tous les cas, le filtre vous met en garde.



Si vous avez des soupçons sur une page Web, cliquez sur le bouton *Outils* de la barre d'outils d'IE et sélectionnez *Filtre d'hameçonnage* puis. *Vérifier ce site Web*. Après avoir cliqué sur OK dans la fenêtre flash Filtre d'hameçonnage, IE effectue une vérification précise et en profondeur du site Web en question pour voir si vous êtes en train de vous faire duper.



Maintenant attention : restez sur vos gardes même si votre navigateur a un filtre d'hameçonnage. Les voyous comptent sur la nature humaine pour que leurs escroqueries fonctionnent. Aucune institution financière n'envoie d'information vitale par courriel. Non, aucune! Si vous avez un doute, appelez votre banquier pour vérifier si la banque est à l'origine du message que vous avez reçu. Souvent, ce n'est pas le cas. Même si c'est le cas, mieux vaut prévenir que guérir!

Fenêtres publicitaires intempestives

Une fenêtre publicitaire intempestive est une petite fenêtre qui contient des graphiques et du texte et qui apparaît soudainement à l'écran quand vous allez sur un site Web. Ça a l'air amusant, n'est-ce pas? Comme un pantin qui sort de sa boîte, les fenêtres publicitaires intempestives ne sont pas vraiment méchantes, mais comme leur nom l'indique, elles peuvent devenir désagréables, surtout quand plusieurs décident d'assaillir votre écran en même temps. Allez savoir pourquoi les spécialistes du marketing pensent que plusieurs fenêtres qui viennent vous déranger à l'improviste vous inciteront à acheter un produit quelconque. Toujours est-il que c'est la réalité, mais vous pouvez y mettre un terme.

Vous pouvez bloquer ces fenêtres facilement dans IE. Pour cela, suivez les étapes ci-dessous :

1. Cliquez sur le bouton *Outils* de la barre d'outils.

Le menu *Outils* apparaît alors.

2. Sélectionnez *Bloqueur de fenêtres publicitaires intempestives* dans le menu *Outils*.

Le sous-menu *Bloqueur de fenêtres publicitaires intempestives* apparaît.

3. Sélectionnez *Activer le bloqueur de fenêtres publicitaires intempestives*, s'il apparaît, puis cliquez sur *Oui* pour confirmer.

Quelle commande apparaît? Si c'est la commande *Désactiver le bloqueur de fenêtres publicitaires intempestives*, le tour est déjà joué.

Lorsqu'il est activé, le bloqueur de fenêtres publicitaires intempestives supprime l'apparition de quasiment toutes les fenêtres de ce style à votre écran. Du coup, vous manquez tout un tas de publicités. Oh, quel dommage!

Lorsqu'IE bloque une fenêtre publicitaire intempestive, une barre d'informations contenant le message « Une fenêtre publicitaire intempestive a été bloquée. Pour afficher cette fenêtre publicitaire intempestive ou des options supplémentaires, cliquez ici » apparaît juste au-dessus de l'espace dans lequel vous visionnez la page Web. Si vous cliquez sur la barre, un menu s'affiche.

Dans Firefox, le bloqueur de fenêtres publicitaires intempestives est activé par défaut. Si vous désirez le désactiver, par exemple lorsqu'un site a recours aux fenêtres de ce genre volontairement, allez dans le menu *Préférences*, sélectionnez l'onglet *Contenu* et enlevez la coche devant *Bloquer les fenêtres popup*. En cliquant sur le bouton *Exceptions*, vous pouvez aussi créer une liste de sites pour lesquels vous autorisez les fenêtres publicitaires intempestives, pour vous éviter d'avoir à constamment activer et désactiver le bloqueur.



Le blocage des fenêtres publicitaires intempestives peut aussi désactiver certaines fonctions sur des pages Web, comme une vidéo flash, un menu, ou tout autre affichage utile. Le cas échéant, vous pouvez autoriser les fenêtres publicitaires intempestives pour une fenêtre ou page Web en particulier : pour cela, cliquez sur la barre d'informations et sélectionnez « Autoriser temporairement les fenêtres publicitaires intempestives » dans le menu qui s'affiche.



Le bloqueur de fenêtres publicitaires intempestives dans IE ne peut pas bloquer certaines fenêtres animées : par exemple, les animations Flash peuvent afficher les fenêtres publicitaires, quels que soient les paramètres du bloqueur sélectionnés. Vous n'êtes donc pas à l'abri de quelques surprises. (Avez-vous aussi cette impression que les voyous ont toujours une longueur d'avance sur vous?)

Logiciels espions

Par *logiciel espion* ou *espionnage*, terme relativement large, on entend tout programme ou toute technique qui surveille ou épie ce que vous faites sur Internet. C'est un peu comme un cyber-harceleur électronique. Certains programmeurs-malfaitteurs créent des logiciels espions pour vendre à des annonceurs l'information qu'ils ont obtenue sur vos habitudes de navigation en ligne.

Si votre ordinateur utilise les systèmes d'exploitation Windows Vista ou XP Service Pack 2, il est doté de Windows Defender, excellent moyen de défense contre les logiciels espions. Windows Defender n'est pas un programme unique, mais se compose en réalité d'une multitude d'outils qui peuvent protéger votre ordinateur contre les attaques ennemies.

Plus précisément, Windows Defender vous aide à protéger votre ordinateur contre des programmes virulents qui cherchent à surveiller, voire contrôler, les activités qui s'y déroulent.

Pour démarrer Windows Defender, ouvrez le Panneau de configuration, double-cliquez sur l'icône du centre de sécurité Windows, et cliquez sur le lien *Windows Defender* dans la fenêtre qui apparaît.

La fenêtre principale de Windows Defender est tout ce qu'il y a de plus ennuyant — tout du moins si vous n'avez aucun problème. En effet, si tout va bien, Windows Defender fait un résumé de la situation indiquant que votre ordinateur fonctionne normalement. Ouf! Si vous voulez de l'action, cliquez sur le bouton Outils sur la barre d'outils. Les différentes options et outils qui apparaissent peuvent non seulement vous aider à repérer des programmes teigneux, mais aussi à les éliminer.

Les programmes troyens

Les *programmes troyens* (ou *chevaux de Troie*) sont des programmes qui prétendent faire une chose, mais en font une autre. Par exemple, un programme troyen bien connu est un écran de veille spécial qui sert bel et bien d'écran de veille, mais qui se sert aussi de votre ordinateur pour envoyer des images pornographiques sur Internet.



La meilleure façon de vous défendre contre ces envahisseurs qui n'ont rien de chevaleresque est d'avoir recours à Windows Defender et à un pare-feu. Un *pare-feu* est un dispositif de série sur la plupart des systèmes d'exploitation qui vous aide à fermer les fenêtres et à verrouiller les portes par lesquelles les voyous tentent de passer pour infecter votre ordinateur.

Les virus

Un *virus* est un programme néfaste qui réside dans votre ordinateur à votre insu et le contamine. Le programme peut se déclencher à tout moment; le virus peut alors envahir votre ordinateur, rediriger tous vos déplacements sur Internet, se servir de votre ordinateur pour envoyer des pourriels, ou toute autre activité désagréable.

La fenêtre du Centre de sécurité, qui est accessible à partir du Panneau de configuration, contient un espace réservé aux *logiciels anti-virus* que vous pouvez utiliser pour essayer d'éviter les contaminations. Cet espace se trouve dans la zone de protection contre les logiciels malveillants.

Sachez que Windows lui-même n'offre pas de programme anti-virus. C'est donc à vous d'en trouver un et de l'installer sur votre ordinateur pour renforcer votre protection, surtout contre les virus qui se répandent par les pièces jointes des courriels.

Les vers

Un *ver* est tout simplement un virus qui se multiplie tout seul. Par exemple, un ver qui contamine votre ordinateur peut envoyer des copies de lui-même aux personnes qui figurent dans votre liste de contacts. Comme nous l'avons mentionné au paragraphe précédent, vous pouvez installer sur votre ordinateur un bon programme anti-virus qui peut détecter les vers et les chasser qu'ils, comment dire, viennent lui tirer les vers du nez et que le ver soit dans le fruit!



Votre fournisseur d'accès Internet peut être plus qu'utile quand vous devez livrer bataille contre des programmes malveillants sur Internet. N'oubliez pas de lui demander de l'aide, surtout si vous avez déjà essayé en vain de régler le problème.



Si vous disposez de votre propre serveur de messagerie électronique, demandez à votre conseiller en TI d'installer les filtres anti-virus nécessaires pour que les messages contaminés ne puissent pas pénétrer sur votre réseau. (Consultez le chapitre 1 pour savoir comment choisir un conseiller en TI.)

Copies de sauvegarde

Supposons que votre ordinateur est contaminé par un virus qui provoque de sérieux dégâts. Vous pourriez perdre toute votre information. Faire des copies de sauvegarde est un peu comme utiliser la soie dentaire : tout le monde sait qu'on doit le faire fréquemment et avec soin, mais peu de personnes le font souvent, et encore moins de personnes le font correctement.

Le jour où votre ordinateur se met à faire des siennes, vous vous sentirez nettement moins vulnérable si vous avez des copies de tous les fichiers qui sont sur votre ordinateur. Vous avez fait des copies récemment, n'est-ce-pas?



Ne conservez pas vos copies de sauvegarde au même endroit que votre ou vos ordinateurs, car en cas de sinistre, comme un incendie ou une tornade, vous perdriez tout. Si vos copies de sauvegarde sont ailleurs, vous pouvez reprendre vos activités rapidement.

Quelle option choisir?

Il existe de nombreuses façons de faire des copies de sauvegarde. Voici les plus populaires :

- ✓ **Disque dur externe** : Votre ordinateur est équipé de son propre disque dur, mais vous pouvez vous en procurer un second qui se branche à un port USB. Un disque dur externe est un dispositif de petite taille et donc portatif qui vous permet de conserver une copie de tous les fichiers présents sur votre ordinateur.
- ✓ **Sauvegarde en ligne** : Vous pouvez avoir recours à un service de sauvegarde commercial sur Internet pour faire des copies de sauvegarde de vos fichiers (à condition d'avoir une connexion Internet à large bande, sinon vous allez y passer vos soirées avec un modem de 56 ko).

- ✔ **Clé USB** : Ce gadget est de la taille d'un porte-clé, fonctionne sans pile et est fait en un seul bloc! La clé USB fonctionne comme les appareils photos numériques et sauvegarde vos fichiers sur des cartes mémoires (amovibles ou internes).
- ✔ **CD ou DVD** : Un moyen peu coûteux de faire des copies de sauvegarde de vos fichiers consiste à les graver sur des disques. Cette méthode ne convient par contre que dans les cas où vous ne copiez que certains fichiers et non tout ce qui se trouve sur votre ordinateur.

Ayez un plan de sauvegarde!

La fréquence à laquelle vous devez faire des copies de sauvegarde de votre ordinateur dépend de l'usage que vous en faites. Voici un exemple de plan à adopter pour quelqu'un qui se sert de son ordinateur pour sa petite entreprise, mais vous pouvez l'adapter à votre propre niveau de confort!

- ✔ **Le premier jour de chaque semaine** : Procédez à la sauvegarde complète du système, y compris les fichiers qui se trouvent sur chacun des ordinateurs.
- ✔ **Les autres jours de la semaine** : Faites une sauvegarde incrémentielle, qui ne touche que les fichiers créés ou mis à jour depuis la dernière sauvegarde.
- ✔ **Une fois par mois** : Gardez l'une des copies de sauvegarde à des fins d'archivage. Ainsi, s'il vous faut restaurer votre système, vous n'aurez jamais à remonter à plus d'un mois.



Les copies de sauvegarde n'empêcheront pas les actes de piraterie ni les intrusions sur votre ordinateur, mais elles permettront de vous en remettre!