symantec™

Norton Internet Security 2003™

Guide de l'utilisateur

10028080-FR

Guide de l'utilisateur Norton Internet Security™ 2003

Documentation version 6.0

Référence : 10028080-FR

Copyright

Bibliothèque de modèles standard

Marques

Imprimé en Irlande.

Si vous installez Norton Internet Security pour la première fois

Démarrez ici

Déterminer le système de fichiers utilisé par l'ordinateur.

1. **Sur le bureau, cliquez deux fois sur Poste de travail, effectuez un clic droit sur le lecteur C, puis cliquez sur Propriétés.**

2. **Quel système de fichiers utilisez-vous ?**

   - FAT (Windows 98/Me/2000/XP)
     Se reporter à "Si vous utilisez un système de fichiers FAT" à la page 4.
   - NTFS (Windows 2000/XP uniquement)
     Se reporter à "Si vous utilisez un système de fichiers NFTS" à la page 5.

Consultez www.service.symantec.com/installtutorial pour obtenir des instructions détaillées et un didacticiel Web qui vous guidera tout au long du processus

Si vous utilisez un système de fichiers FAT

Rechercher les virus affectant l'installation.

Insérez le CD-ROM Norton Internet Security dans le lecteur et relancez l'ordinateur.

Si vous ne disposez pas d'un CD-ROM Norton Internet Security, ou si vous ne parvenez pas à lancer l'ordinateur à partir d'un CD-ROM, créez des disquettes d'urgence sur un autre ordinateur non infecté.

Se reporter à "Création de disquettes d'urgence" à la page 30.

Exécutez une analyse complète du système.

Un virus a-t-il été détecté ?

- Oui
  Exécutez une nouvelle analyse en utilisant la touche Suppr.
- Non
  Se reporter à "Terminer l'installation" à la page 6.

Consultez www.service.symantec.com/installtutorial pour obtenir des instructions détaillées et une démo Web qui vous guidera tout au long du processus

Si vous utilisez un système de fichiers NFTS

Rechercher les virus affectant l'installation.

Pouvez-vous établir une connexion avec Internet ?

- Oui
  Allez à l'adresse http://security.symantec.com et suivez les instructions à l'écran pour rechercher les menaces.
- Non
  Pour Windows XP : Allez à l'adresse service.symantec.com
  Pour Windows 2000 : Allez à l'adresse service.symantec.com

  Se reporter à "Terminer l'installation" à la page 6.

Un virus a-t-il été détecté ?

- Oui
  Notez le nom du virus et allez à l'adresse http://securityresponse.symantec.com pour obtenir des instructions de suppression spécifiques.
- Non
  Si ce n'est déjà fait, installez Norton Internet Security.

  Se reporter à "Terminer l'installation" à la page 6.

Consultez www.service.symantec.com/installtutorial pour obtenir des instructions détaillées et un didacticiel Web qui vous guidera tout au long du processus

Terminer l'installation

Après avoir recherché les virus, vous pouvez installer Norton Internet Security en toute sécurité.

1. **Désinstallez tous les autres programmes antivirus sur l'ordinateur.**

   Sur le bureau, utilisez le Panneau de configuration Ajout/Suppression de programmes pour sélectionner le programme à désinstaller.

2. **Fermez tous les programmes en cours d'exécution, y compris les éléments de la barre d'état du système Windows.**

3. **Installez Norton Internet Security depuis le CD-ROM Norton Internet Security.**
   Se reporter à "Installation de Norton Internet Security" **à la page 27.**

? **Avez-vous vu s'afficher le message "Norton Internet Security a été installé avec succès" ?**

- Oui
  Se reporter à "Après l'installation" à la page 38.
- Non
  Notez le message d'erreur à l'écran et rendez-vous sur le site http://www.symantec.fr/frsupport/ pour obtenir de l'aide.

Table des matières

Chapitre 8 Protection antivirus des disques, des fichiers et des données

Chapitre 9 Comment procéder en cas d'infection

Annexe A Dépannage de Norton Internet Security

Réponse aux urgences

1

En cas d'urgence, reportez-vous à cette section pour trouver la solution à votre problème. Les problèmes courants comprennent les menaces de virus et les tentatives d'intrusion.

Si vous soupçonnez la présence d'un virus

Si votre ordinateur est infecté par un *virus* et que vous avez besoin de le démarrer à partir d'un disque non infecté pour supprimer le virus, vous pouvez utiliser le CD-ROM Norton Internet Security comme disquette d'urgence. Le programme DOS Norton AntiVirus utilise les définitions de virus du CD-ROM Norton Internet Security et ne dispose pas des définitions de virus les plus récentes, telles que celles téléchargées via LiveUpdate.

Se reporter à "Impossible de démarrer depuis le lecteur A" à la page 228.

vous pouvez être contraint de modifier les options du BIOS de l'ordinateur pour démarrer à partir du lecteur de CD.

Pour démarrer l'ordinateur à partir du CD-ROM Norton Internet Security et rechercher les virus

1. Insérez le CD-ROM Norton Internet Security dans le lecteur.
2. Redémarrez l'ordinateur.
   Le programme d'urgence analyse l'ordinateur et supprime les virus.

Réponse aux menaces de virus

Se reporter à "Comment procéder en cas d'infection" à la page 139.

Si vous avez déjà installé Norton Internet Security et que Norton AntiVirus détecte un virus sur l'ordinateur, vous disposez de trois solutions pour résoudre le problème :

- Réparer le fichier
  Cette action supprime le virus du fichier.

Se reporter à "Si des fichiers sont en quarantaine" à la page 145.

- Mettre le fichier en quarantaine
  Cette action rend le fichier inaccessible à tout programme autre que Norton AntiVirus. Vous ne pouvez pas ouvrir ce fichier accidentellement et propager le virus, mais vous pouvez toujours l'analyser et le soumettre éventuellement à Symantec.
- Supprimer le fichier
  Cette action supprime le virus de l'ordinateur en supprimant le fichier qui le contient. Cette option ne doit être utilisée que si le fichier est irréparable ou impossible à mettre en quarantaine.

Si vous pensez que votre ordinateur fait l'objet d'une attaque

Si l'ordinateur répond de manière anormale et que vous avez déterminé qu'il ne s'agit pas d'un virus ou d'un fichier corrompu, vous faites peut-être l'objet d'une attaque.

Si vous soupçonnez une attaque de pirate, déconnectez immédiatement l'ordinateur d'Internet. Si vous n'avez pas encore installé Norton Internet Security, installez-le maintenant.

Si vous avez installé Norton Internet Security, vous pouvez utiliser ses outils de sécurité pour bloquer l'attaque, rechercher l'attaquant et éviter les attaques à l'avenir.

Pour bloquer et analyser une attaque

1. Ouvrez Norton Internet Security.

Se reporter à "Arrêt d'une communication Internet avec la fonction Bloquer le trafic" à la page 60.

2. Cliquez sur **Bloquer le trafic**.
   Cela bloque immédiatement toute communication entrante et sortante avec les autres ordinateurs.
3. Si vous utilisez Security Monitor, cliquez sur **Security Center**.
4. Dans Security Center, cliquez sur **Statistiques**.
5. Cliquez sur **Détails de l'attaquant**.
   Votre navigateur ouvre la page Web Visual Tracking.

Se reporter à "Identification de la source de communications" à la page 59.

6 Visual Tracking permet d'identifier l'adresse IP de l'ordinateur utilisé par l'attaquant.
Vous pouvez vous servir de cette information pour signaler l'attaque au FAI propriétaire de l'adresse.

Se reporter à "Ajout d'un ordinateur bloqué à la zone Restreints" à la page 128.

7 Pour bloquer toute connexion future de cette adresse IP, ajoutez l'ordinateur à votre zone Restreints.

Si vous pensez qu'un pirate a déjà investi l'ordinateur, installez Norton Internet Security, puis consultez l'adresse http://security.symantec.com où sont disponibles des outils permettant de réparer et d'éradiquer toute menace qu'un pirate aurait pu placer sur l'ordinateur.

Restauration après incident

Quand vous avez résolu le problème, vous pouvez installer Norton Internet Security et procéder aux activités suivantes :

Action	Description
Installation de Norton Internet Security.	Norton Internet Security peut protéger votre ordinateur contre toute attaque ultérieure. Se reporter à "Installation de Norton Internet Security" à la page 27.
Mise à jour de la protection.	Une fois l'installation effectuée, exécutez LiveUpdate pour vérifier que vous disposez des protections les plus récentes. Se reporter à "Mises à jour avec LiveUpdate" à la page 83.
Définissez une programmation de protection antivirus.	Norton AntiVirus peut analyser l'ordinateur à intervalles réguliers pour vérifier qu'il est protégé Se reporter à "Planification d'analyses antivirus" à la page 135.
Configuration du pare-feu.	L'installation par défaut de Norton Internet Security doit fournir une protection suffisante aux utilisateurs, mais il est possible de personnaliser la protection en définissant les paramètres du pare-feu. Se reporter à "Personnalisation de la protection du pare-feu" à la page 107.
Consultation régulière des journaux et des statistiques.	Norton Internet Security conserve des rapports complets de toutes les opérations entreprises pour protéger l'ordinateur. Consultez régulièrement ces journaux pour identifier les problèmes potentiels. Se reporter à "Contrôle de Norton Internet Security" à la page 207.

Prévention des problèmes ultérieurs

Se reporter à "Risques et menaces liés à Internet" à la page 245.

Norton Internet Security peut protéger votre ordinateur contre la plupart des attaques par Internet et infections de virus.

Pour préparer votre ordinateur aux situations d'urgence

- Tenez-vous informé sur les virus et les risques relatifs à la sécurité en visitant le *site Web* de Symantec Security Response (securityresponse.symantec.com).
- Actualisez votre *navigateur*. Les éditeurs de logiciels publient de nouvelles versions pour remédier aux vulnérabilités de leurs navigateurs.
- Utilisez intelligemment les *mots de passe*. Pour protéger les données importantes, utilisez des mots de passe complexes composés de majuscules, de minuscules, de chiffres et de symboles. N'utilisez pas le même mot de passe en plusieurs endroits.
- N'exécutez pas un logiciel si vous ne faites pas confiance à son éditeur et à la source qui vous l'a fourni.
- N'ouvrez une pièce jointe de *courrier électronique* que si vous l'attendiez et que vous faites confiance à son expéditeur.
- Soyez prudent lorsque vous décidez de transmettre des informations personnelles. Bien souvent, les sites demandent des informations dont ils n'ont pas besoin.
- Consultez la politique de confidentialité des sites auxquels vous envisagez d'envoyer des informations.
- Indiquez aux enfants de ne jamais révéler d'informations personnelles sur des messageries instantanées.
- Sauvegardez régulièrement vos fichiers et conservez à portée de main une copie des dernières sauvegardes.

A propos de Norton Internet Security

2

Norton Internet Security est une suite d'applications de sécurité qui protège les ordinateurs contre les attaques et les virus Internet, protège la confidentialité de vos informations, accélère la navigation sur Internet en éliminant les publicités et bloque les contenus Internet inadaptés.

Nouveautés de Norton Internet Security 2003

Norton Internet Security 2003 inclut à présent :

- Security Monitor
  Vous assure un accès rapide aux outils de Norton Internet Security les plus utilisés.
- Alerte spam
  Permet d'identifier et de bloquer les courriers électroniques non sollicités.
- Visual Tracking
  Identifie la source des attaques et d'autres communications Internet.
- Protection par mot de passe
  Renforce la sécurité des options de Norton Internet Security et Norton AntiVirus.
- Blocage du trafic
  Permet d'empêcher immédiatement d'autres ordinateurs de communiquer avec le vôtre.
- Assistant Alerte
  Vous permet de comprendre les alertes et les problèmes de sécurité éventuels.

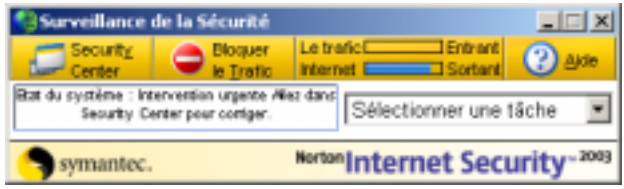
- Afficheur du journal
  Cette version améliorée permet de voir toutes les actions entreprises par Norton Internet Security pour protéger votre ordinateur
- Confidentialité
  Cette version améliorée bloque les informations confidentielles envoyées dans les courriers électroniques et les programmes de messagerie instantanée.
- Contrôle parental
  Cette version améliorée permet aux parents de choisir les sites Web, les groupes de discussion et les programmes que leurs enfants peuvent utiliser.

Norton AntiVirus 2003 contient les nouveautés suivantes :

- Fonctions étendues de réparation et de suppression de fichier
  Norton AntiVirus tente à présent automatiquement de réparer les fichiers infectés sans intervention de votre part.
- Prise en charge et options de messagerie instantanée
  Norton AntiVirus analyse à présent les fichiers reçus des programmes America Online, Yahoo! et MSN Instant Messenger.
- Blocage de ver
  Norton AntiVirus analyse les annexes des courriers sortants pour chercher des vers et vous alerte avant d'envoyer des *fichiers infectés*.

Fonctionnalités de Norton Internet Security

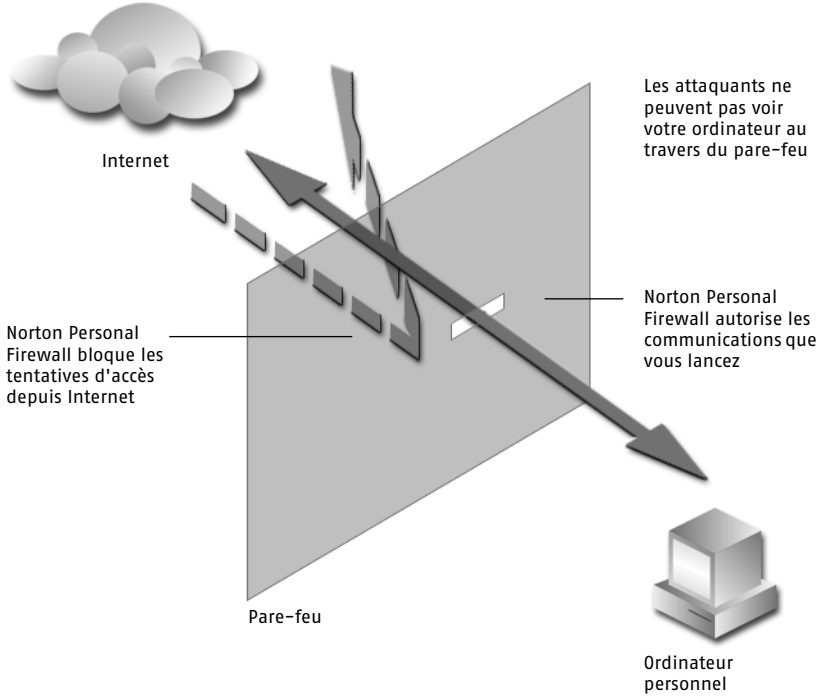
Norton Internet Security inclut Norton Personal Firewall, Norton AntiVirus et une série d'autres outils de sécurité qui contribuent à protéger votre ordinateur. Vous pouvez accéder rapidement à tous les outils de Norton Internet Security depuis la Security Monitor.



La sécurité sur Internet peut s'avérer une question complexe. Norton Internet Security inclut désormais l'assistant Alerte, qui aide à comprendre les questions de sécurité, suggère des méthodes de résolution des problèmes et propose des conseils pour éviter les problèmes de sécurité.

A propos de Norton Personal Firewall

Norton Internet Security inclut Norton Personal Firewall, qui constitue une barrière de protection entre votre ordinateur et Internet. Un *pare-feu* interdit aux utilisateurs non autorisés d'accéder aux ordinateurs privés et aux *réseaux* connectés à Internet.



Le composant Norton Personal Firewall de Norton Internet Security inclut des fonctionnalités qui interdisent l'accès non autorisé à votre ordinateur quand vous êtes sur Internet, détectent les attaques Internet éventuelles, protègent vos informations personnelles, bloquent les publicités Internet pour accélérer votre navigation, éliminent les courriers non sollicités dans votre boîte de réception et protègent les membres de votre famille contre les contenus en ligne inadaptés.

Fonctionnalités de Norton Internet Security

Détection d'intrusion	La fonction de Détection d'intrusion contribue à protéger votre ordinateur contre les attaques Internet en analysant chaque information qui entre sur votre ordinateur et en sort. Si elle identifie une attaque éventuelle, la Détection d'intrusion vous prévient et bloque automatiquement la connexion à l'origine de l'attaque. Se reporter à "Protection contre les tentatives d'intrusion" à la page 103.
Confidentialité	La fonction de Confidentialité propose différents niveaux de contrôle sur le type d'informations que les utilisateurs peuvent envoyer par le Web, le courrier électronique et les programmes de messagerie instantanée. Vous pouvez également contrôler la manière dont la fonction Confidentialité réagit lorsque des sites Web tentent de configurer et d'utiliser des cookies ou d'obtenir des informations sur votre navigateur. Se reporter à "Protection de votre confidentialité" à la page 163.
Blocage des publicités	Le Blocage des publicités accélère votre navigation sur le Web en éliminant les bannières publicitaires et autres contenus importuns ou lents à charger. Norton Internet Security bloque également les publicités créées avec Macromedia Flash et empêche les sites d'ouvrir des fenêtres de publicité déroulantes. Se reporter à "Blocage des publicités sur Internet" à la page 175.

Alerte spam	Les courriers "spam" (courriers non sollicités et parfois déplaisants) sont un problème de plus en plus important. La fonction Alerte spam permet de diminuer le nombre de courriers non sollicités que vous recevez en filtrant intelligemment les messages entrants et en marquant distinctement les courriers spam éventuels. Cela permet de créer facilement des filtres pour votre programme de messagerie qui suppriment automatiquement les courriers spam avant même que vous ne les voyiez. Se reporter à "Suppression des courriers indésirables" à la page 185.
Contrôle parental	La fonction Contrôle parental contribue à écarter du foyer les contenus Internet inadaptés en permettant aux parents de contrôler les sites Web et les groupes de discussion que leurs enfants peuvent consulter. Les parents peuvent également choisir les types d'applications Internet auxquelles les enfants pourront accéder, en bloquant efficacement l'accès Internet aux logiciels de discussion ou autres applications. Se reporter à "Protection des enfants avec le Contrôle parental" à la page 193.

A propos de Norton AntiVirus

Norton AntiVirus fournit à votre ordinateur un système complet pour prévenir, détecter et éliminer les infections de virus. Il recherche et répare les fichiers infectés afin de garantir la sécurité des données. La mise à jour du service de définitions de virus sur Internet est facile et prépare Norton AntiVirus à lutter contre les menaces les plus récentes.

Se reporter à "Accès aux fichiers PDF du guide de l'utilisateur" à la page 80.

Le *Manuel de l'utilisateur de Norton AntiVirus* au format PDF, Nav2003.pdf, inclut des informations complètes sur les virus et leur mode de propagation.

Norton AntiVirus se compose d'un programme résident en mémoire, d'Auto-Protect et d'une fonction d'analyse que vous pouvez programmer ou exécuter manuellement.

Fonctionnalités de Norton AntiVirus

Service de définitions de virus	Met automatiquement à jour vos définitions de virus. Se reporter à "Mises à jour avec LiveUpdate" à la page 83.
Bloodhound, technologie	Détecte les virus nouveaux ou inconnus en analysant la structure d'un fichier exécutable, son comportement et d'autres attributs comme la logique de programmation, les instructions machine et toutes les données contenues dans le fichier. Se reporter à "Comment procéder en cas d'infection" à la page 139.
Blocage de script	Détecte les virus basés sur Visual Basic et JavaScript, sans avoir recours à des définitions de virus spécifiques. Il surveille les scripts pour détecter les comportements suspects et vous avertit lorsqu'il en détecte. Se reporter à "Comment procéder en cas d'infection" à la page 139.
Auto-Protect	Se charge en mémoire au démarrage de Windows et vous protège en permanence pendant que vous travaillez. Recherche les virus chaque fois que vous utilisez des logiciels sur l'ordinateur, que vous insérez des disquettes ou d'autres supports amovibles dans les lecteurs, que vous accédez à Internet ou utilisez des fichiers document reçus ou créés. Surveille l'ordinateur pour détecter les symptômes inhabituels pouvant indiquer un virus actif. Se reporter à "Si le virus a été détecté par Auto-Protect" à la page 141.

Installation de Norton Internet Security

3

Avant d'installer Norton Internet Security, prenez le temps d'examiner la configuration requise décrite dans ce chapitre. Les utilisateurs de Windows 98 et Windows Me doivent disposer de plusieurs disquettes vierges de 1,44 Mo pour créer des jeux de sauvetage.

Configuration système requise

Pour utiliser Norton Internet Security, l'un des systèmes d'exploitation Windows suivants doit être installé sur l'ordinateur :

- Windows 98, 98SE
- Windows Me
- Windows 2000 Professional
- Windows XP Professional ou Windows XP Home Edition

Windows 95 et NT, les versions serveur de Windows 2000/XP et Windows XP version 64 bits ne sont pas pris en charge.

L'ordinateur doit également répondre aux spécifications suivantes.

système d'exploitation	Configuration requise
Windows 98/ 98SE/Me	■ Processeur Intel Pentium (ou compatible) à 150 MHz ou supérieur ■ 48 Mo de RAM (64 Mo recommandés) ■ 90 Mo d'espace disque (60 Mo si vous n'installez pas le Contrôle parental) ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM
Windows 2000 Professional	■ Processeur Intel Pentium (ou compatible) à 150 MHz ou supérieur ■ 64 Mo de RAM (96 Mo recommandés) ■ 90 Mo d'espace disque (60 Mo si vous n'installez pas le Contrôle parental) ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM
Windows XP Professional ou Home Edition	■ Processeur Intel Pentium II (ou compatible) à 300 MHz ou supérieur ■ 128 Mo de RAM ■ 90 Mo d'espace disque (60 Mo si vous n'installez pas le Contrôle parental) ■ Internet Explorer 5.01 ou ultérieur (5.5 recommandé) ■ Lecteur de CD-ROM ou de DVD-ROM

Clients de messagerie pris en charge

Norton Internet Security peut analyser les courriers électroniques pour rechercher des informations confidentielles, des virus et du spam, dans tout client de messagerie compatible POP3, notamment :

- Microsoft® Outlook® Express 4.0/5.X
- Microsoft Outlook 97/98/2000/XP
- Netscape® Messenger 4.X, Netscape Mail 6.0
- Eudora® Light 3.0, Eudora Pro 4.0, Eudora 5.0

L'analyse du courrier électronique ne prend pas en charge les clients de messagerie suivants :

- Clients IMAP
- Clients AOL
- POP3 avec SSL (Secure Socket Layer)
- Courrier électronique Web comme Hotmail et Yahoo!
- Messagerie Lotus Notes

Clients de messagerie instantanée pris en charge

- AOL Instant Messenger, version 4.3 ou ultérieure
- MSN Instant Messenger, version 3.6 ou ultérieure
- Windows Messenger, version 4.0 ou ultérieure

Avant l'installation

Avant d'installer Norton Internet Security, préparez l'ordinateur. Si l'ordinateur ne peut pas démarrer à partir d'un CD, créez des disquettes d'urgence.

Préparation de l'ordinateur

Se reporter à "Si vous devez désinstaller Norton Internet Security" à la page 47.

Si vous disposez d'une ancienne version de Norton Internet Security ou de Norton AntiVirus, la nouvelle version vous propose de la remplacer.

Vous devez également désinstaller tout programme antivirus installé sur l'ordinateur. Pour plus d'informations, reportez-vous à la documentation du programme concerné.

Avant d'installer Norton Internet Security, fermez tous les programmes Windows ouverts. D'autres programmes en cours d'exécution risqueraient d'entrer en conflit lors de l'installation et de diminuer la protection.

Si vous utilisez Windows XP

Windows XP inclut un *pare-feu* pouvant entrer en conflit avec les fonctions de protection de Norton Internet Security. Il est donc nécessaire de désactiver le pare-feu de Windows XP avant d'installer Norton Internet Security.

Pour désactiver le pare-feu de Windows XP

1. Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Panneau de configuration** > **Connexions réseau**.
2. Si vous avez créé plus d'une connexion modem ou réseau, sélectionnez la connexion active.
3. Cliquez sur **Tâches de réseau**.
4. Cliquez sur **Modifier les paramètres pour cette connexion**.
5. Dans la section Pare-feu pour la connexion Internet de l'onglet Avancés, désélectionnez l'option **Protéger mon ordinateur et le réseau en limitant l'accès à cet ordinateur depuis Internet**.
6. Cliquez sur **OK** pour fermer la fenêtre des paramètres.
7. Cliquez sur **OK** pour fermer la fenêtre Tâches de réseau.

Recherche de virus

Il est conseillé de vérifier l'absence de virus avant d'installer Norton Internet Security. Cela garantit que l'ordinateur est protégé et que l'installation se déroulera sans problème.

Se reporter à "Si vous utilisez le CD comme disquette d'urgence" à la page 149.

Si votre ordinateur peut démarrer depuis un CD, redémarrez-le à partir du CD-ROM Norton Internet Security et rechercher les virus sur le disque dur. Si l'ordinateur ne peut pas démarrer à partir d'un CD, créez des disquettes d'urgence.

Le programme d'urgence de Norton AntiVirus utilise les définitions de virus du CD-ROM Norton Internet Security et ne dispose pas des définitions de virus les plus récentes, telles que celles téléchargées via LiveUpdate. Il est conseillé d'effectuer une nouvelle analyse antivirus après l'installation.

Création de disquettes d'urgence

Se reporter à "Si vous avez besoin d'utiliser des disquettes d'urgence" à la page 149.

Les disquettes d'urgence servent à démarrer l'ordinateur et à rechercher les virus en cas de problème. Si l'ordinateur peut démarrer depuis un CD, vous pouvez utiliser le CD Norton Internet Security à la place des disquettes d'urgence et vous n'avez pas besoin de créer celles-ci.

Si l'ordinateur ne peut pas démarrer depuis un CD, utilisez ces instructions pour créer des disquettes d'urgence sur un autre ordinateur ou allez sur http://www.symantec.com/techsupp/ebd.html et téléchargez le programme Emergency Disk. Suivez les instructions incluses dans le téléchargement pour créer le jeu de disquettes d'urgence.

Vous devez disposer de plusieurs disquettes formatées de 1,44 Mo.

Pour créer des disques d'urgence à partir du CD

1. Insérez le CD-ROM Norton Internet Security dans le lecteur de CD-ROM.
2. Dans la fenêtre du CD Norton Internet Security, cliquez sur **Parcourir le CD**.
3. Dans l'Explorateur Windows, cliquez deux fois sur le dossier **Support**.
4. Cliquez deux fois sur le dossier **Edisk**.
5. Cliquez deux fois sur **Ned.exe**.
6. Dans la fenêtre de bienvenue, cliquez sur **OK**.
7. Etiquetez la première disquette comme indiqué et insérez-la dans le lecteur A.
8. Cliquez sur **Oui**.
9. Répétez les étapes 7 et 8 pour les disquettes suivantes.
10. A la fin de la procédure, cliquez sur **OK**.
11. Retirez la dernière disquette du lecteur A et stockez le jeu de disquettes d'urgence en lieu sûr.

Installation de Norton Internet Security

Installez Norton Internet Security depuis le CD-ROM Norton Internet Security. Installez un exemplaire de Norton Internet Security sur chaque ordinateur à protéger.

Pour installer Norton Internet Security

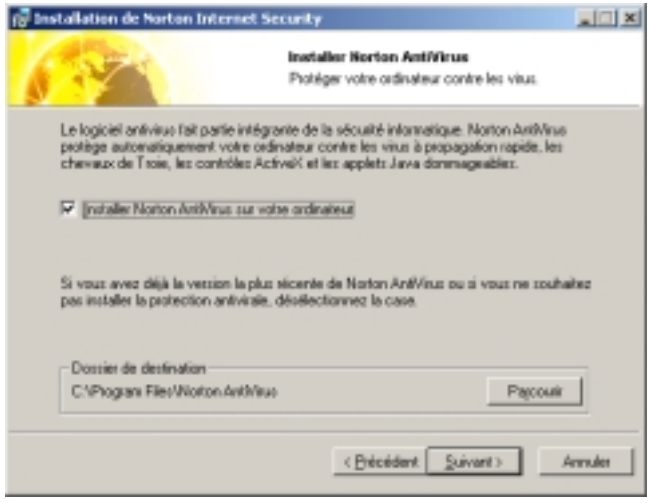
1. Insérez le CD-ROM Norton Internet Security dans le lecteur.
2. Dans la fenêtre du CD Norton Internet Security, cliquez sur **Installer Norton Internet Security**.
   Si l'ordinateur n'est pas configuré pour exécuter automatiquement un CD, vous devez ouvrir le CD vous-même.
   La première fenêtre d'installation vous rappelle de fermer tous les autres programmes Windows.

Se reporter à "Si l'écran d'ouverture n'apparaît pas" à la page 35.

3 Cliquez sur **Suivant**.

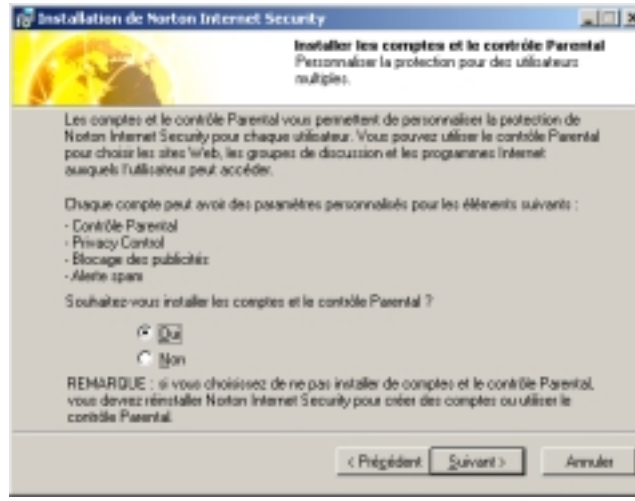
4 Lisez l'accord de licence et cliquez sur **J'accepte les termes du contrat de licence**.
Si vous n'acceptez pas les termes de l'accord, vous ne pourrez pas poursuivre l'installation.

5 Cliquez sur **Suivant**.



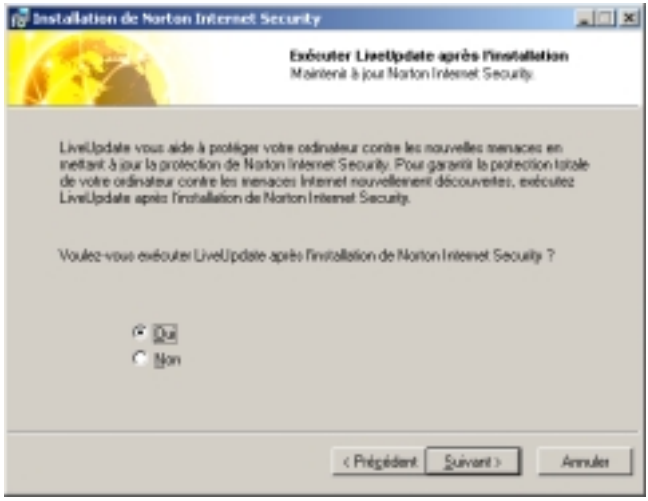
6 Pour installer Norton AntiVirus, cochez l'option **Installer Norton AntiVirus** et cliquez sur **Parcourir** pour indiquer l'emplacement où vous souhaitez installer le programme.
Si une version actualisée de Norton Antivirus est déjà installée sur l'ordinateur, cette fenêtre n'apparaît pas.

7 Cliquez sur **Suivant**.



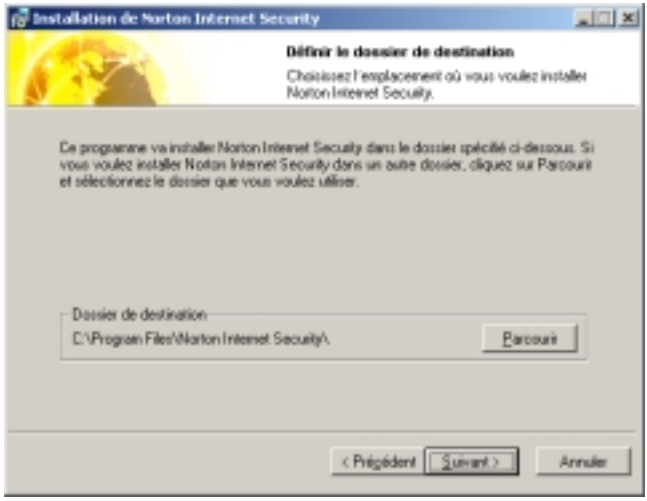
8 Dans la fenêtre Installer les comptes et le Contrôle parental, indiquez si vous voulez installer ces fonctionnalités.
Si vous choisissez de ne pas installer les comptes et le Contrôle parental, vous devrez réinstaller Norton Internet Security pour créer des comptes ou utiliser le Contrôle parental.

9 Cliquez sur **Suivant**.



10 Dans la fenêtre Exécuter LiveUpdate après l'installation, décidez si vous souhaitez exécuter LiveUpdate à la fin de l'installation.

11 Cliquez sur **Suivant**.

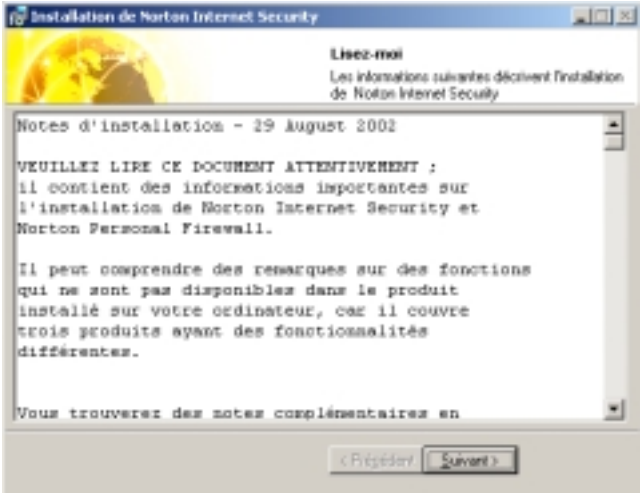


12 Cliquez sur **Parcourir** pour sélectionner le dossier dans lequel vous souhaitez installer Norton Internet Security, s'il s'agit d'un autre emplacement que celui par défaut.

13 Cliquez sur **Suivant**.

Se reporter à "Enregistrement du logiciel" à la page 36.

14 Cliquez sur **Suivant** pour commencer l'installation de Norton Internet Security.
Une fois Norton Internet Security installé, l'assistant Enregistrement apparaît.



15 Lisez le texte du fichier LisezMoi, puis cliquez sur **Suivant**.

16 Cliquez sur **Terminer** pour quitter l'installation.

Si l'écran d'ouverture n'apparaît pas

Il peut arriver que le lecteur de CD de l'ordinateur ne lance pas automatiquement le CD.

Pour démarrer l'installation depuis le CD Norton Internet Security

1 Sur votre bureau, cliquez deux fois sur **Poste de travail**.

2 Dans la boîte de dialogue Poste de travail, cliquez deux fois sur l'icône représentant le lecteur de CD.

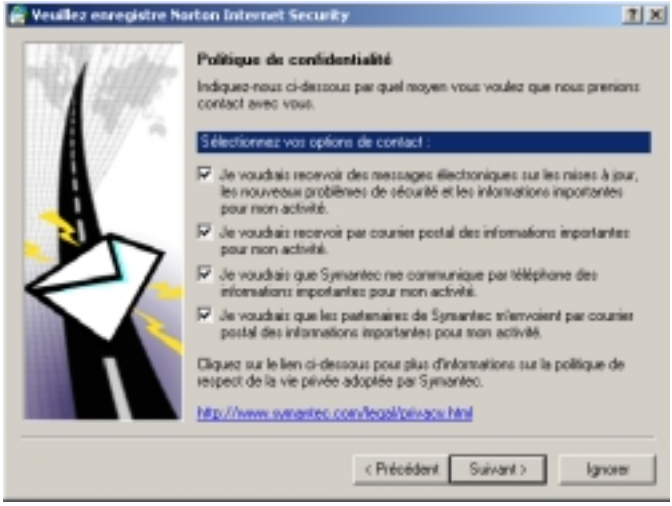
3 Dans la liste de fichiers, cliquez deux fois sur **Cdstart.exe**.

Enregistrement du logiciel

Utilisez l'assistant Enregistrement pour enregistrer votre logiciel en ligne. Si vous ignorez l'enregistrement en ligne, vous pourrez l'effectuer ultérieurement avec l'option Enregistrement du menu Aide.

Pour enregistrer votre logiciel

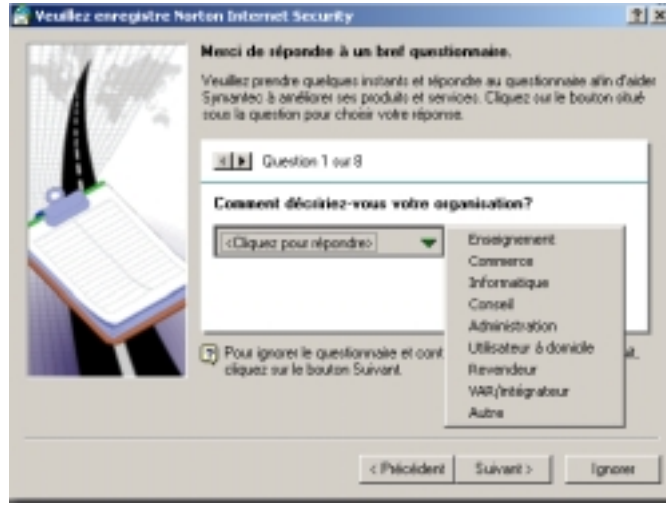
1 Dans la première fenêtre d'enregistrement, sélectionnez le pays depuis lequel vous vous enregistrez et celui où vous vivez (s'il est différent), puis cliquez sur **Suivant**.



2 Si vous souhaitez obtenir des informations de Symantec sur Norton Internet Security, sélectionnez la méthode par laquelle vous voulez recevoir ces informations et cliquez sur **Suivant**.

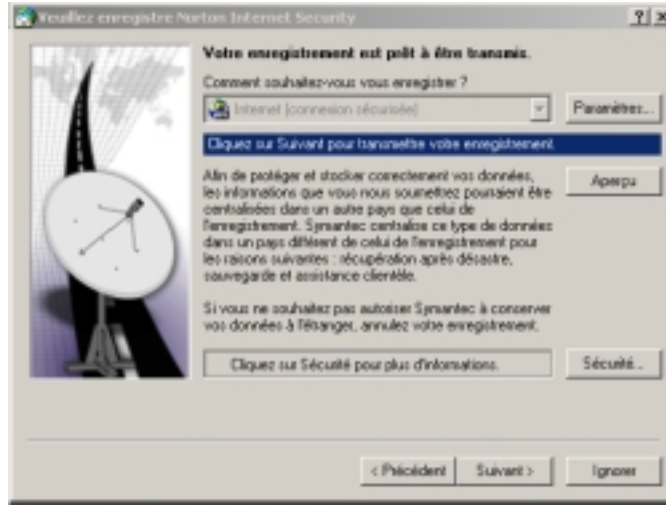
3 Indiquez votre nom et cliquez sur **Suivant**.

4 Indiquez votre adresse et cliquez sur **Suivant**.



5 Effectuez l'une des opérations suivantes :

- Répondez au questionnaire afin d'aider Symantec à améliorer ses produits et services, puis cliquez sur **Suivant**.
- Sautez l'enquête en cliquant sur **Suivant**.



6 Choisissez l'enregistrement de Norton Internet Security par Internet ou par courrier.
Pour vous enregistrer par courrier, l'ordinateur doit être connecté à une imprimante que l'assistant Enregistrement utilisera pour imprimer le formulaire. Pour vous enregistrer par Internet, vous devez être connecté à Internet.

7 Cliquez sur **Suivant**.

8 Pour obtenir une copie de vos informations d'inscription pour référence ultérieure, effectuez l'une des opérations suivantes :

- Notez le numéro de série.
- Cliquez sur **Imprimer**.

9 Cliquez sur **Suivant**.

10 Choisissez si vous voulez utiliser votre profil existant pour l'enregistrement ultérieur d'un produit Symantec ou tapez les informations dans le cadre de l'enregistrement.

11 Cliquez sur **Terminer**.

Après l'installation

Une fois Norton Internet Security installé, une boîte de dialogue apparaît et vous donne la possibilité de redémarrer immédiatement l'ordinateur. Lorsque l'ordinateur a redémarré, l'assistant Sécurité apparaît et indique la marche à suivre pour configurer Norton Internet Security.

Redémarrage de l'ordinateur

Après l'installation, un message vous demande de redémarrer l'ordinateur pour que les modifications prennent effet.

Pour redémarrer l'ordinateur

❖ Dans la boîte de dialogue Informations du programme d'installation, cliquez sur **Oui**.
La configuration de Norton Internet Security n'est pas terminée tant que l'ordinateur n'a pas redémarré.

Utilisation de l'assistant Sécurité

L'assistant Sécurité vous aide à configurer rapidement votre protection Norton Internet Security.L'assistant Sécurité se divise en cinq catégories :

- Réseau personnel
- Contrôle des programmes
- Confidentialité
- Protection par mot de passe
- Contrôle parental

Configuration du Réseau personnel

Se reporter à "Connexion à un réseau" à la page 91.

Utilisez le Réseau personnel pour identifier les ordinateurs que vous savez inoffensifs et ceux dont vous souhaitez limiter l'accès à votre ordinateur. L'assistant de Contrôle de zone peut configurer automatiquement votre *réseau* et ajouter des ordinateurs à la zone Approuvés.

Pour configurer le Réseau personnel

1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Réseau personnel**.

2 Dans le volet Réseau personnel, cliquez sur **Configuration du Réseau personnel**.

3 Dans l'Assistant de Contrôle de zone, cliquez sur **Suivant**.

4 Suivez les instructions affichées pour configurer le réseau.

Configuration du Contrôle des programmes

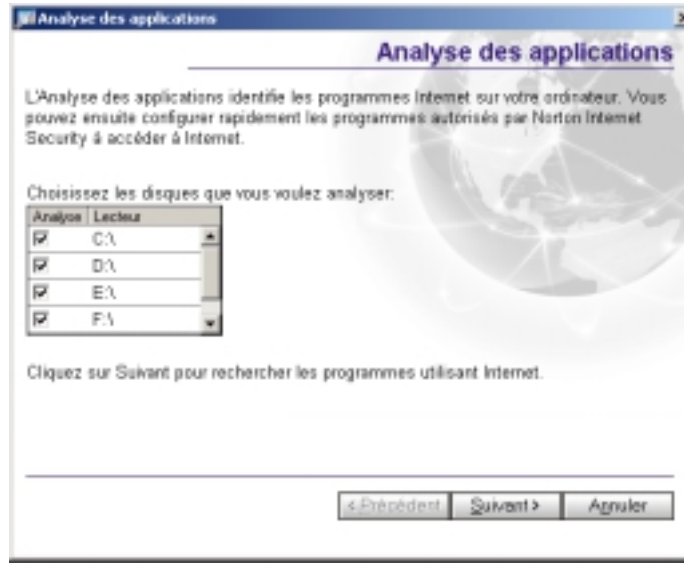
Se reporter à "Recherche des applications utilisant Internet" à la page 115.

Norton Internet Security peut analyser votre ordinateur pour rechercher les applications capables d'accéder à Internet et créer des règles d'accès. Quand l'analyse est terminée, vous pouvez utiliser ses résultats pour déterminer quelles applications doivent accéder à Internet et, si nécessaire, ajuster leurs règles d'accès.

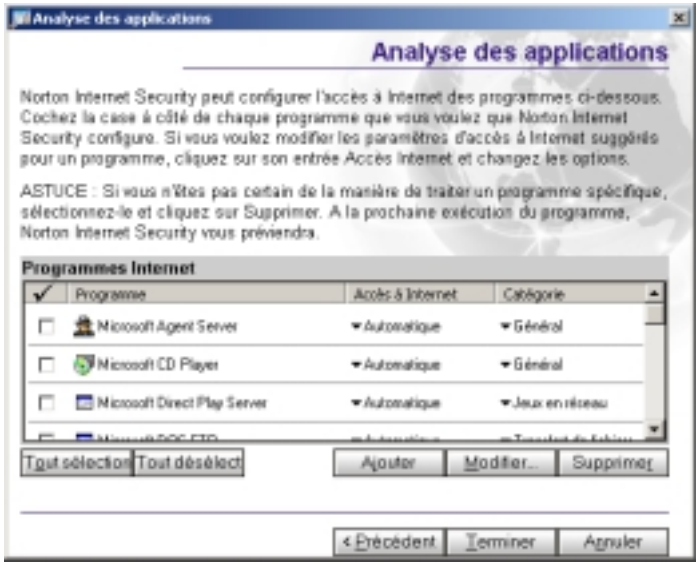
Pour configurer le Contrôle des programmes

1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Analyse des applications**.

2 Sur le volet Analyse des applications, cliquez sur **Analyser les programmes automatiquement**.



3 Dans la fenêtre Analyse des applications, cliquez sur **Suivant** pour lancer l'analyse.
Lorsque l'analyse est terminée, toutes les applications qui se connectent à Internet sont indiquées.



4 Pour autoriser une application à accéder à Internet, cochez la case en regard de son nom.

5 Pour modifier la règle d'accès à Internet ou la catégorie d'une application, sélectionnez le paramètre souhaité dans la liste déroulante Accès à Internet ou Catégorie.

6 Cliquez sur **Terminer** lorsque vous avez fini.

Configuration de la Confidentialité

Se reporter à "Identification des informations confidentielles à protéger" à la page 166.

La fonction Confidentialité permet d'établir la liste des informations qui doivent bénéficier d'une protection supplémentaire. Le Contrôle de confidentialité empêche alors les utilisateurs d'envoyer des informations sur des *sites Web*, dans des *courriers électroniques*, dans des pièces jointes Microsoft Office files ou dans des programmes de messagerie instantanée.

Pour configurer le Contrôle de la confidentialité

1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Confidentialité**.

2 Dans la fenêtre Confidentialité, cliquez sur **Ajouter des informations confidentielles à protéger**.

3 Dans la boîte de dialogue Ajouter des informations confidentielles, sélectionnez une catégorie dans la zone Type d'informations à protéger.

4 Dans le champ Nom descriptif, indiquez pour mémoire la raison pour laquelle vous souhaitez protéger ces données.

Se reporter à "Conseils de saisie des informations confidentielles" à la page 166.

5 Dans le champ Informations à protéger, tapez les cinq ou six derniers caractères de l'information dont vous souhaitez empêcher la transmission sur des connexions Internet non sécurisées.
En indiquant seulement des informations partielles, vous évitez que des individus malhonnêtes accédant à votre ordinateur ne dérobe des informations complètes.

6 Cliquez sur **OK**.

Protection par mot de passe

Se reporter à "Utilisation de Security Monitor" à la page 53.

Pour une sécurité optimale, il est recommandé d'exiger un *mot de passe* avant toute modification des paramètres de Norton Internet Security. Cela vous garantit que seul des personnes de confiance pourront désactiver la protection, le *pare-feu* et la Détection d'intrusion ou apporter des modifications aux options de Norton Internet Security.

Quand la Protection par mot de passe est activée, les utilisateurs doivent fournir leur mot de passe pour modifier les paramètres de Norton Internet Security. Si l'utilisateur en cours ne possède pas de mot de passe de compte, vous devez en créer un.

Pour protéger les options de Norton Internet Security avec un mot de passe

1 Dans l'Itinéraire de l'assistant Sécurité, cliquez sur **Protection par mot de passe**.

2 Dans le volet Protection par mot de passe, cliquez sur **Activer la protection par mot de passe**.

3 Dans les champs Mot de passe et Confirmation du mot de passe, saisissez un mot de passe.

4 Cliquez sur **OK**.

Configuration du Contrôle parental

Le Contrôle parental vous permet de contrôler l'accès des membres de la famille à Internet. Vous pouvez interdire l'accès à des *Sites Web* et des groupes de discussion que vous jugez inappropriés, ainsi qu'à des applications comme les programmes de discussion auxquels vous ne voulez pas que des membres de la famille accèdent. Par défaut, le Contrôle parental est désactivé.

Pour activer le Contrôle parental

1 Dans l'Itinéraire de l'Assistant Sécurité, cliquez sur **Contrôle parental**.

2 Sur le volet Contrôle parental, cliquez sur **Créer des comptes utilisateur**.

3 Dans la fenêtre Superviseur, choisissez un nom et un mot de passe pour le compte Superviseur.
Le Superviseur peut modifier tous les comptes. Choisissez un mot de passe difficile à deviner.

4 Cliquez sur **Suivant**.

Se reporter à "Création de comptes pour utilisateurs multiples" à la page 153.

5 Dans la fenêtre Sélection d'un gestionnaire de compte, effectuez l'une des opérations suivantes :

- Pour utiliser des comptes Windows existants, cliquez sur **Oui, utiliser les comptes Windows existant (recommandé)** .
- Pour créer de nouveaux comptes Norton Internet Security, cliquez sur **Créer des comptes de Norton Internet Security**.

6 Cliquez sur **Suivant**.

7 Suivez les instructions affichées pour configurer de nouveaux comptes.

Si Norton SystemWorks est installé

Si Norton SystemWorks est installé sur votre ordinateur quand vous installez Norton Internet Security, le programme d'installation ajoute un onglet Norton Internet Security à la fenêtre principale de Norton SystemWorks et un onglet Norton SystemWorks à Security Center.

Pour installer Norton Internet Security depuis Norton SystemWorks

1 Ouvrez Norton SystemWorks.

2 Sur l'onglet Norton Internet Security, cliquez sur **Lancer Norton Internet Security**.

Pour ouvrir Norton SystemWorks depuis Norton Internet Security

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre Norton SystemWorks 2002, cliquez sur **Lancer Norton SystemWorks**.

Si vous devez désinstaller Norton Internet Security

Si vous avez besoin de désinstaller Norton Internet Security de l'ordinateur, ouvrez le menu Démarrer de Windows et utilisez l'option Désinstallation de Norton Internet Security. Il est également possible de désinstaller uniquement le composant Norton AntiVirus de Norton Internet Security.

Au cours de la désinstallation, Windows peut indiquer qu'il effectue l'installation d'un logiciel. Il s'agit d'un message général du programme d'installation de Microsoft, dont vous pouvez ne pas tenir compte.

Pour désinstaller Norton Internet Security

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer > Programmes > Norton Internet Security > Désinstaller Norton Internet Security**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer > Autres programmes > Norton Internet Security > Désinstallation de Norton Internet Security**.
2. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Supprimer NAV** pour désinstaller le composant Norton AntiVirus de Norton Internet Security.
   - Cliquez sur **Tout supprimer** pour désinstaller l'ensemble du produit.

3 Si vous avez des fichiers en quarantaine, le système vous demande si vous souhaitez les supprimer. Les options sont les suivantes :

Oui	Supprime de votre ordinateur les fichiers mis en quarantaine.
Non	Laisse les fichiers en quarantaine sur l'ordinateur mais les rend inaccessibles. Pour réparer ou transmettre les fichiers à Symantec pour analyse, réinstallez Norton Internet Security.

4 Dans la boîte de dialogue Informations du programme d'installation, cliquez sur**Oui** pour redémarrer l'ordinateur.

Si aucun autre produit Symantec ne se trouve sur l'ordinateur, vous devez également désinstaller LiveReg et LiveUpdate.

Pour désinstaller LiveReg et LiveUpdate

1 Effectuez l'une des opérations suivantes :
- Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
- Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Panneau de configuration**.

2 Dans le Panneau de configuration, cliquez deux fois sur **Ajout/ Suppression de programmes**.

3 Dans la liste des programmes actuellement installés, sélectionnez **LiveReg**.

4 Effectuez l'une des opérations suivantes :
- Sous Windows 2000/Me, cliquez sur **Modifier/Supprimer**.
- Sous Windows 98, cliquez sur **Ajouter/Supprimer**.
- Dans Windows XP, cliquez sur **Supprimer**.

5 Cliquez sur **Oui** pour confirmer la désinstallation du produit.

6 Pour désinstaller LiveUpdate, répétez les étapes 1 à 5 en sélectionnant LiveUpdate à l'étape 3.

Bases de Norton Internet Security

4

Après son installation, Norton Internet Security protège automatiquement l'ordinateur sur lequel il est installé. Vous n'avez pas besoin de lancer le programme pour activer la protection.

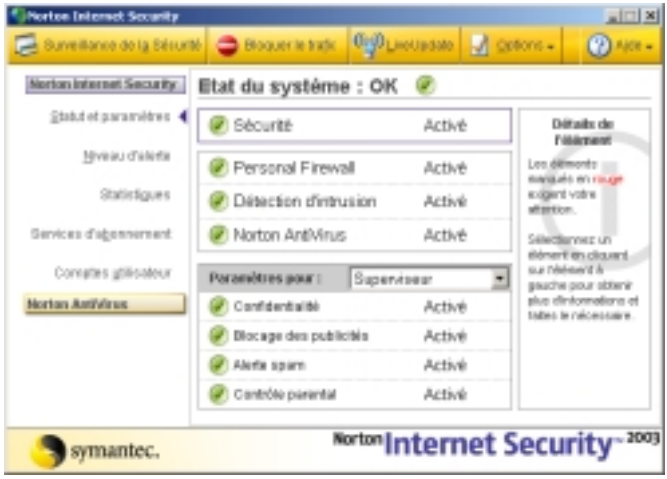
Accès à Norton Internet Security

Lancez Norton Internet Security afin de modifier les paramètres de protection ou de contrôler ses activités.

Pour accéder à Norton Internet Security

- Effectuez l'une des opérations suivantes :
  - Dans la barre des tâches de Windows, cliquez sur **Démarrer > Programmes > Norton Internet Security > Norton Internet Security**.
  - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer > Autres programmes > Norton Internet Security > Norton Internet Security**.

- Sur le Bureau de Windows, cliquez deux fois sur **Norton Internet Security**.



Accès à Norton Internet Security depuis la barre d'état système

Norton Internet Security ajoute une icône à la barre d'état système de Windows. Sur la plupart des ordinateurs, la barre d'état est située à l'extrême droite de la barre des tâches de Windows en bas de l'écran. Cliquez sur cette icône pour ouvrir un menu qui contient les outils de Norton Internet Security fréquemment utilisés.

Pour utiliser le menu de la barre d'état système de Norton Internet Security

1. Dans la barre d'état système, cliquez avec le bouton droit sur l'icône de Norton Internet Security.
2. Dans le menu qui apparaît, sélectionnez un élément. Les éléments du menu sont les suivants :

Norton Internet Security	Ouvre une fenêtre Norton Internet Security.
Pour masquer/ afficher AlertTracker	Affiche ou masque Alert Tracker. Se reporter à "Utilisation d'Alert Tracker" à la page 57.

Bloquer le trafic	Arrête immédiatement toutes les informations entrantes et sortantes. Se reporter à "Arrêt d'une communication Internet avec la fonction Bloquer le trafic" à la page 60.
Connexion/ Déconnexion	Permet de changer le compte connecté à Norton Personal Firewall. Se reporter à "Ouverture d'une session Norton Internet Security" à la page 162.
A propos de Norton Internet Security	Affiche des informations détaillées sur les composants de Norton Internet Security.
LiveUpdate	Met à jour votre protection. Se reporter à "Mises à jour avec LiveUpdate" à la page 83.
Aide	Affiche l'aide en ligne de Norton Internet Security. Se reporter à "Utilisation de l'aide en ligne" à la page 77.
Désactiver	Désactive toutes les fonctions de protection de Norton Internet Security. Se reporter à "Désactivation temporaire de Norton Internet Security" à la page 73.

Se reporter à "A propos des paramètres globaux" à la page 65.

Utilisez les options de Norton Internet Security pour ajouter d'autres outils au menu.

Accès à Norton AntiVirus depuis la barre d'outils de l'Explorateur Windows

Norton AntiVirus ajoute un bouton et un menu à l'Explorateur Windows. Le bouton permet de lancer l'analyse des éléments sélectionnés dans le volet de l'Explorateur. Pour accéder aux outils supplémentaires de Norton AntiVirus, cliquez sur la flèche située à droite du bouton.

Lors de la première ouverture de l'Explorateur Windows après l'installation de Norton Internet Security, le bouton et le menu de Norton AntiVirus n'apparaissent pas toujours.

Pour afficher le bouton et le menu de Norton AntiVirus

1. Dans le menu Affichage de l'Explorateur Windows, cliquez sur **Barres d'outils**.
2. Cliquez sur **Norton AntiVirus**.

L'accès à Norton AntiVirus à partir du menu de l'Explorateur Windows dépend de la configuration de l'ordinateur.

Utilisation de Norton Internet Security

Norton Internet Security fonctionne en arrière-plan, ce qui vous donne la possibilité d'agir sur le programme uniquement lorsqu'il vous avertit d'une nouvelle *connexion* réseau ou d'un problème potentiel. Vous pouvez choisir d'afficher le nouveau Security Monitor ou la fenêtre standard de Security Center, de répondre aux problèmes de sécurité et de contrôler le nombre d'*alertes* que vous recevez ainsi que la manière dont le programme résout les problèmes de sécurité potentiels.

Accès aux fonctions de protection de Norton Internet Security

Les paramètres par défaut de Norton Internet Security offrent une méthode sûre, automatique et efficace pour protéger votre ordinateur. Si vous voulez modifier ou personnaliser votre protection, vous pouvez accéder à tous les outils de Norton Internet Security depuis la fenêtre Statut et paramètres.

Les utilisateurs de type Enfant ne peuvent pas modifier les paramètres de Norton Internet Security. Tous les utilisateurs, indépendamment de leur niveau d'accès, peuvent modifier les paramètres de Norton AntiVirus. Pour protéger vos paramètres contre toute modification indésirable, définissez un mot de passe pour les options Norton Internet Security et Norton AntiVirus. Se reporter à "Options de protection par mot de passe" à la page 70.

Pour modifier les paramètres de fonctions individuelles

1. Ouvrez Norton Internet Security.
2. Dans Security Center, effectuez l'une des opérations suivantes :
   - Cliquez deux fois sur une fonction que vous souhaitez personnaliser.
   - Sélectionnez une fonction, puis dans l'angle inférieur droit de la fenêtre, cliquez sur **Personnaliser**.

3 Configurez la fonction.

4 Lorsque que vous avez terminé les modifications, cliquez sur **OK**.

Si vous avez installé des comptes, vous pouvez créer des paramètres personnalisés pour le Contrôle de confidentialité, le Blocage des publicités, l'Alerte spam, le Contrôle parental et le niveau de sécurité du Firewall personnel. Les autres paramètres s'appliquent à tous les comptes.

Pour modifier les paramètres de comptes individuels

1 Ouvrez Norton Internet Security.

2 Dans Security Center, effectuez l'une des opérations suivantes :

- Cliquez deux fois sur une fonction que vous souhaitez personnaliser.
- Sélectionnez une fonction, puis dans l'angle inférieur droit de la fenêtre, cliquez sur **Personnaliser**.

3 Dans le menu Paramètres pour de la fenêtre de la fonction, sélectionnez le compte à configurer.

4 Configurez la fonction.

5 Lorsque que vous avez terminé les modifications, cliquez sur **OK**.

Utilisation de Security Monitor

Security Monitor rassemble les outils de Norton Internet Security les plus utilisés dans une fenêtre compacte. Lorsque vous êtes en ligne, placez la fenêtre de Security Monitor dans une partie inutilisée de l'écran. Ceci vous permet de surveiller votre *connexion*, d'afficher des informations sur les événements de sécurité et de personnaliser votre protection sans nécessiter beaucoup d'espace à l'écran.

A son démarrage, Norton Internet Security lance Security Center. Vous pouvez ensuite basculer dans la fenêtre de Security Monitor.

Pour afficher la fenêtre de Security Monitor

- ❖ Dans l'angle supérieur gauche de la fenêtre Security Center, cliquez sur **Security Monitor**.

Pour afficher la fenêtre Security Center

- ❖ Dans l'angle supérieur gauche de la fenêtre Security Monitor, cliquez sur **Security Center**.

Vous pouvez afficher Security Monitor par-dessus toutes les autres fenêtres. Elle sera ainsi toujours visible.

Pour garder Security Monitor au premier plan

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Général, cochez l'option **Afficher Security Monitor par-dessus tous les autres programmes**.
4. Cliquez sur **OK**.

Sélection d'une tâche avec Security Monitor

Utilisez le menu Sélectionner une tâche de Security Monitor pour exécuter rapidement les tâches courantes de Norton Internet Security. Le menu Sélectionner une tâche inclut les éléments suivants :

Tâche	Plus d'informations
Chercher les virus	Se reporter à "Analyse manuelle de disques, de dossiers et de fichiers" à la page 131.
Test de la sécurité	Se reporter à "Vérification de la vulnérabilité de l'ordinateur aux attaques" à la page 58.
Modification d'informations personnelles	Se reporter à "Protection de votre confidentialité" à la page 165.
Affichage de la visionneuse du journal	Se reporter à "Affichage des journaux de Norton Internet Security" à la page 213.
Exécution de LiveUpdate	Se reporter à "Mises à jour avec LiveUpdate" à la page 83.
Exécution de l'analyse de programme	Se reporter à "Recherche des applications utilisant Internet" à la page 115.

Tâche	Plus d'informations
Créer des comptes utilisateur	Se reporter à "Création de comptes pour utilisateurs multiples" à la page 153.
Configuration du réseau personnel	Se reporter à "Organisation des ordinateurs en zones de réseau" à la page 93.

Réponse aux alertes de Norton Internet Security

Norton Internet Security surveille les communications entrantes et sortantes et vous avertit lorsqu'une activité quelconque risque de compromettre votre sécurité.

Lorsqu'une *alerte* se produit, lisez le message avant de prendre une décision. Identifiez le type d'alerte et le niveau de menace. Quand vous avez évalué les risques, faites un choix.

Prenez le temps nécessaire avant de prendre votre décision. Tant que l'alerte est active, votre ordinateur est à l'abri des attaques.

Norton Internet Security vous permet de choisir une action appropriée en présélectionnant l'action recommandée s'il en existe une. Norton Internet Security ne peut pas suggérer d'actions recommandées pour toutes les alertes.

Informations complémentaires avec l'Assistant Alerte

Chaque alerte Norton Internet Security inclut un lien vers l'Assistant Alerte. L'Assistant Alerte comprend des informations personnalisées sur chaque alerte, notamment :

- Le type d'alerte
- Le niveau de menace
- La communication qui a déclenché cette alerte
- Ce que ces types d'alerte indiquent
- Le moyen de réduire le nombre de ces alertes

Pour utiliser l'Assistant Alerte

1. Dans une fenêtre d'alerte quelconque, cliquez sur le bouton Assistant Alerte.
2. Dans la fenêtre Assistant Alerte, examinez les informations sur cette alerte.
3. Pou répondre à l'alerte, fermez l'Assistant Alerte.

Réglage du niveau d'alerte

Le curseur du niveau d'alerte vous permet de contrôler la quantité d'informations que Norton Internet Security consigne dans des *journaux*, ainsi que le nombre d'alertes qu'il affiche.

Les utilisateurs de type Superviseur et Adulte peuvent définir le niveau d'alerte de leur choix. Les superviseurs peuvent également définir le niveau d'alerte pour les autres utilisateurs.

Les options sont les suivantes :

Niveau d'alerte	Informations fournies	Messages Alert Tracker	Alertes de sécurité	Vous informe quand...
Minimum	Evénements Internet critiques	Aucun	Consigné, non affiché	Les règles de contrôle de programme sont créées automatiquement. Des analyses de port sont exécutées. Des informations confidentielles sont bloquées. Un programme de cheval de Troie d'accès distant est rencontré.
Moyen	Evénements Internet importants	Certains	Consigné, non affiché	Mêmes notifications que pour Minimum, plus : ▪ Programmes accédant à Internet.
Haut	Evénements Internet importants et activités de programme complètes	Nombre élevé	Consigné et affiché	Mêmes notifications que pour Moyen, plus : ▪ Les ports inutilisés sont bloqués. ▪ Les cookies et les contenus sont bloqués.

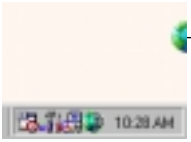
Pour régler le niveau d'alerte

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Niveau d'alerte**.
3. Déplacez le curseur pour sélectionner un niveau d'alerte.

Utilisation d'Alert Tracker

De nombreux événements Internet surveillés par Norton Internet Security ne justifient pas le déclenchement d'une alerte. Alert Tracker fournit une méthode simple pour surveiller ces événements de sécurité moins importants.

Alert Tracker affiche les mêmes informations que celles qui apparaissent dans le champ Evénement de sécurité de Security Monitor. Ceci vous permet de surveiller la sécurité de votre ordinateur sans avoir à laisser Security Monitor visible en permanence. Alert Tracker fournit également une méthode rapide pour supprimer les publicités sur des *pages Web*.



Alert Tracker est affiché en permanence sur le côté de l'écran

Si vous choisissez de l'afficher, Alert Tracker s'ancre à l'un ou l'autre des côtés de l'écran principal. Lorsqu'un événement de sécurité survient, Alert Tracker affiche un message pendant quelques secondes, puis reprend sa place sur le côté de l'écran. Si vous n'avez pas pu voir un message Alert Tracker, vous pouvez consulter la liste des messages récents.

Les messages Alert Tracker sont affichés pendant quelques secondes

Alert Tracker comporte également la Corbeille publicitaire, qui fait partie de la fonction Blocage des publicités de Norton Internet Security.

Se reporter à "Utilisation de la Corbeille publicitaire" à la page 179.

Pour afficher ou masquer Alert Tracker

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Sécurité Internet**.

3 Sur l'onglet Général, effectuez l'une des opérations suivantes :
   - Cochez l'option **Afficher Alert Tracker** pour afficher Alert Tracker.
   - Désélectionnez l'option **Afficher Alert Tracker** pour masquer Alert Tracker.

4 Cliquez sur **OK**.

Pour consulter les messages récents d'Alert Tracker

1 Sur le Bureau de Windows, cliquez deux fois sur Alert Tracker.

2 A droite du premier message, cliquez sur la flèche si elle apparaît.

3 Cliquez deux fois sur une entrée pour ouvrir la visionneuse du journal.

Se reporter à "Affichage des statistiques détaillées" à la page 210.

Pour déplacer Alert Tracker

❖ Faites glisser l'hémisphère vers le côté de l'écran sur lequel vous voulez le placer.

Pour afficher ou masquer Alert Tracker dans le menu de la barre d'état système

❖ Dans la barre d'état système de Windows, cliquez avec le bouton droit sur l'icône du Norton Internet Security, puis effectuez l'une des opérations suivantes :
   - Cliquez sur **Masquer Alert Tracker** pour masquer Alert Tracker.
   - Cliquez sur **Afficher Alert Tracker** pour afficher Alert Tracker.

Si vous masquez Alert Tracker, aucune notification ne sera affichée lorsque l'ordinateur se connectera à un *réseau*. Les informations relatives à la *connexion* seront toujours présentes dans les *journaux*.

Vérification de la vulnérabilité de l'ordinateur aux attaques

Utilisez Security Check pour vérifier la vulnérabilité de votre ordinateur face aux intrusions. Le lien Security Check dans Norton Internet Security vous connecte au *site Web* de Symantec, qui vous permet de rechercher les vulnérabilités et d'obtenir des informations détaillées sur les analyses de Security Check.

Vous devez être connecté à Internet pour vérifier la vulnérabilité de votre ordinateur.

Pour vérifier la vulnérabilité de l'ordinateur aux attaques

1. Ouvrez Norton Internet Security.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez sur **Sécurité**, puis sur **Contrôler la sécurité**.
   - Dans le menu Sélectionner une tâche Security Monitor, cliquez sur **Tester la sécurité**.
3. Dans la page Web Security Check, cliquez sur **Analyse des risques en matière de sécurité**.
4. Pour plus d'informations sur les tests de Security Check, cliquez sur **A propos de l'analyse des risques en matière de sécurité**.

Lorsque l'analyse est terminée, la page de résultats répertorie toutes les zones contrôlées, ainsi que votre niveau de vulnérabilité dans chacune. Pour chaque zone à risque, vous pouvez obtenir davantage de détails sur le problème et la manière de le résoudre.

Pour obtenir davantage d'informations sur une zone à risque

- Dans la page des résultats, cliquez sur **Afficher les détails** à côté du nom de l'analyse.

Identification de la source de communications

Visual Tracking vous aide à en savoir plus sur les ordinateurs qui tentent de se connecter à votre ordinateur. Grâce à Visual Tracking, vous pouvez identifier l'emplacement de l'*adressee IP* utilisée et des informations de contact sur le propriétaire de l'adresse. Vous pouvez utiliser ces informations pour déterminer l'origine d'une attaque et vous informer sur les tentatives d'intrusion.

Vous pouvez suivre les *tentatives de connexion* à partir de trois emplacements dans Norton Internet Security :

- Statistiques
- Visionneuse du journal
- AutoBlock

Pour suivre une tentative de connexion depuis les statistiques

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Statistiques**.
3. Cliquez sur **Détails de l'attaquant**.
   Votre navigateur ouvre la page Web Visual Tracking.

Pour suivre une tentative de connexion depuis la visionneuse du journal

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Statistiques**.
3. Cliquez sur **Afficher le journal**.
4. Dans la colonne gauche de la fenêtre de la visionneuse du journal, sous Sécurité Internet, cliquez sur **Connexion**.
5. Dans la colonne droite de la fenêtre de la visionneuse du journal, sélectionnez la connexion que vous souhaitez suivre.
6. En bas de la fenêtre de la visionneuse du journal, cliquez sur l'adresse IP ou le nom de l'ordinateur.
   Votre navigateur ouvre la page Web Visual Tracking.

Pour suivre une tentative de connexion depuis AutoBlock

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la section AutoBlock de la fenêtre Détection d'intrusion, sélectionnez une connexion que vous souhaitez suivre.
4. Cliquez sur **Détails de l'attaquant**.
   Votre navigateur ouvre la page Web Visual Tracking.

Lorsque Visual Tracking est terminé, il affiche une représentation visuelle de l'origine de cette communication et des informations de contact concernant le propriétaire de l'adresse IP.

Arrêt d'une communication Internet avec la fonction Bloquer le trafic

Les fenêtres Security Center et Security Monitor comportent un bouton Bloquer le trafic qui vous permet d'interrompre immédiatement une communication entre votre ordinateur et un autre. Ce bouton peut être pratique pour limiter les dommages éventuels sur votre ordinateur en cas d'attaque, si un *cheval de Troie* envoie des informations confidentielles à votre insu ou si vous autorisez par mégarde une personne peu fiable à accéder aux fichiers stockés sur votre ordinateur.

Lorsque cette option est active, Norton Internet Security bloque toutes les communications entrantes et sortantes. De l'extérieur, votre ordinateur semble totalement déconnecté d'Internet.

Si vous voulez bloquer tout le trafic entrant et sortant, la fonction Bloquer le trafic est plus efficace que le fait d'utiliser simplement votre logiciel Internet pour vous déconnecter. La plupart des programmes Internet étant capables de se connecter automatiquement sans aucune intervention de l'utilisateur, un programme malveillant pourrait se reconnecter en votre absence.

La fonction Bloquer le trafic est sensée servir de mesure temporaire pendant que vous résolvez un problème de sécurité. Si vous redémarrez l'ordinateur, Norton Internet Security autorise automatiquement toutes les communications entrantes et sortantes. Pour continuer à bloquer le trafic, cliquez sur le bouton Bloquer le trafic dans Security Center ou Security Monitor.

Pour éviter les attaques pendant la résolution d'un problème de sécurité

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre Security Center ou Security Monitor, cliquez sur **Bloquer le trafic**.
3. Utilisez les outils Norton Internet Security pour résoudre le problème de sécurité.
4. Une fois le problème résolu, cliquez sur **Autoriser le trafic**.

Personnalisation de Norton Internet Security

Les paramètres par défaut de Norton Internet Security offrent une protection appropriée à la majorité des utilisateurs. Si vous devez effectuer des modifications, les utilisateurs des niveaux Superviseur et Adulte peuvent utiliser le menu Options pour accéder aux options Norton Internet Security et Norton AntiVirus. Les options vous permettent de contrôler des paramètres plus avancés.

Si vous utilisez Windows 2000/XP, et que vous ne disposez pas des droits d'accès administrateur local, vous ne pouvez pas modifier les options Norton Internet Security.

Pour personnaliser Norton Internet Security

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sélectionnez l'onglet sur lequel vous souhaitez modifier des options.

A propos des options générales

Les options générales vous permettent de contrôler le moment d'exécution de Norton Internet Security, de protéger les paramètres du programme par un *mot de passe* et de sélectionner les éléments visuels à afficher. Les options sont les suivantes :

Démarrer Norton Internet Security	Vous permet d'indiquer si vous souhaitez lancer Norton Internet Security manuellement ou automatiquement au démarrage de Windows.
Protéger les outils Norton Internet Security	Définissez un mot de passe pour protéger vos paramètres de sécurité des personnes peu fiables qui accèdent physiquement à votre ordinateur. Se reporter à "Options de protection par mot de passe" à la page 70.
Alert Tracker	Activez ou désactivez Alert Tracker.
Paramètres de l'icône de la barre d'état système	Vous permet d'afficher dans la barre des tâches de Windows une icône Norton Internet Security permettant d'accéder aux paramètres du programme. Vous pouvez également choisir d'inclure des liens vers les outils Norton Internet Security suivants : ■ Options ■ Visionneuse du journal ■ Statistiques

A propos des options LiveUpdate

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Les options LiveUpdate vous permettent d'activer et de désactiver la fonction LiveUpdate automatique, qui recherche automatiquement les mises à jour de Norton Internet Security lorsque vous vous connectez à Internet. Pour une sécurité optimale, laissez cette option sélectionnée.

Vous pouvez sélectionner les composants Norton Internet Security que LiveUpdate automatique doit surveiller. Vous pouvez également indiquer à LiveUpdate automatique de mettre à jour les composants en arrière-plan ou de vous avertir lorsque des mises à jour sont disponibles. Les options sont les suivantes :

Norton Internet Security	Améliorations apportées au système d'exploitation ou à la compatibilité matérielle et solutions aux problèmes de performances
Personal Firewall	Nouvelles règles de filtrage qui augmentent et étendent les capacités de Personal Firewall à protéger votre ordinateur
Détection d'intrusion	Signatures d'attaque qui protègent votre ordinateur contre les nouvelles attaques Internet
Liste de sites Web du Contrôle parental	Liste des sites Web visités depuis l'installation de Norton Internet Security, classés par catégorie
Alerte spam	Définitions de spam actualisées, identifiant de nouveaux types de courriers non sollicités

Se reporter à "A propos des options Internet" à la page 69.

Norton AntiVirus inclut un ensemble séparé d'options LiveUpdate.

A propos des options du pare-feu

Les options du pare-feu vous permettent d'activer des fonctions de protection avancées et de personnaliser les ports utilisés par votre ordinateur pour afficher les *pages Web*. La plupart des utilisateurs n'ont pas besoin de modifier ces paramètres. Les options sont les suivantes :

Activer la surveillance des composants des programmes	Lorsqu'un programme utilise un composant logiciel externe pour se connecter à Internet, vérifiez les règles de filtrage pour chaque composant. Ainsi, les chevaux de Troie et autres programmes malveillants ne pourront pas se connecter à aux programmes fiables et échapper à la détection.
Activer le contrôle de lancement de programme	Le contrôle de lancement de programme permet de s'assurer que les chevaux de Troie et autres programmes malveillants ne peuvent pas lancer ni manipuler de programmes fiables à votre insu. Lorsque le contrôle de lancement de programme est actif, vous êtes averti chaque fois qu'un programme non reconnu lance un autre programme. Vous pouvez alors décider d'autoriser le programme non reconnu à accéder à Internet ou de le lui interdire.
Ports HTTP	Modifiez les ports que votre navigateur Web utilise pour télécharger des pages Web. Le port HTTP par défaut est 80, mais la liste des ports HTTP contient d'autres ports utilisés fréquemment.
Blocage du protocole IGMP	Activez ou désactivez la capacité de votre ordinateur à utiliser le protocole IGMP (Internet Group Membership Protocol). Ce protocole est couramment utilisé pour envoyer des fichiers multimédia à des groupes de multidiffusion.
Ports masqués	Les ports bloqués et inactifs ne répondent pas aux tentatives de connexion. Les ports actifs ne répondent pas aux tentatives de connexion dont les informations source ou de destination sont incorrectes.
Gestion des paquets IP fragmentés	Décidez si Norton Internet Security doit bloquer tous les paquets IP fragmentés ou seulement ceux qui semblent faire partie d'une attaque.

A propos des options des contenus Web

Les options des contenus Web vous permettent de contrôler comment Norton Internet Security gère les contenus interactifs en ligne, les publicités et les intrusions de confidentialité éventuelles. Ces options sont classées en trois onglets.

A propos des paramètres globaux

Les paramètres globaux vous permettent de contrôler les actions par défaut que Norton Internet Security entreprend lorsque des sites Web tentent d'obtenir des informations sur votre *navigateur* ou d'utiliser des image animées, des scripts Java et autres *contenus actifs*. Les modifications apportées à ces paramètres affectent tous les utilisateurs. Les options sont les suivantes :

Informations sur votre navigateur	Interdisez ou autorisez les sites Web à demander des informations sur votre ordinateur et votre navigateur Web.
Informations sur les sites visités	Interdisez ou autorisez les sites Web à demander des informations sur les autres sites Web que vous avez visités pendant cette session en ligne.
Images animées	Interdisez ou autorisez l'exécution d'images animées.
Scripts	Interdisez ou autorisez les scripts Java.
Publicités Flash	Interdisez ou autorisez les publicités créées avec Macromedia Flash.

A propos des paramètres utilisateur

Les paramètres utilisateurs vous permettent de personnaliser le blocage des *cookies*, des fenêtres déroulantes ainsi que les paramètres *ActiveX* et *Java* pour des sites individuels. Les modifications apportées à ces paramètres affectent uniquement l'utilisateur en cours. Les options sont les suivantes :

Cookies	Interdisez ou autorisez les sites Web à créer et à lire des fichiers de cookies sur votre ordinateur.
Applets Java	Interdisez ou autorisez l'exécution des applets Java.

Contrôles ActiveX	Interdisez ou autorisez l'exécution des contrôles ActiveX.
Publicités déroulantes	Interdisez ou autorisez les publicités déroulantes.

A propos des paramètres du blocage des publicités

Se reporter à "Utilisation des chaînes de texte pour identifier les publicités à bloquer ou à autoriser" à la page 180.

Les paramètres du blocage des publicités vous permettent de spécifier les *bannières publicitaires* individuelles ou les groupes d'images publicitaires que vous souhaitez interdire ou autoriser sur des sites spécifiques.

A propos des options de messagerie

Les options de *messagerie* vous permettent de contrôler la manière dont Norton Internet Security vous avertir quand il recherche dans les messages électroniques des informations confidentielles et des courriers spam. Les options de Les options sont les suivantes :

Icône de la barre d'état système	Vous permet de modifier l'icône de Norton Internet Security dans la barre d'état système pour indiquer que les courriers électroniques sont en cours d'analyse.
Indicateur de progression	Vous permet d'afficher le nombre de courriers électroniques analysés ainsi qu'une estimation du délai d'analyse restant.

Personnalisation de Norton AntiVirus

Les paramètres par défaut de Norton AntiVirus assurent à votre ordinateur une protection complète contre les virus. Vous pouvez toutefois les ajuster pour optimiser les performances du système ou désactiver des options sans objet.

Tous les paramètres d'options sont classés en trois catégories principales. Les options contenues sous chaque catégorie se présentent comme suit.

Catégorie	Options
Système	Auto-Protect ▪ Bloodhound ▪ Avancé ▪ Exclusions Blocage des scripts Analyse manuelle ▪ Bloodhound ▪ Exclusions
Internet	Messagerie ▪ Avancé Messagerie instantanée LiveUpdate
Autre	Inoculation (Windows 98/98SE/Me) Divers

A propos des options système

Les options système contrôlent l'analyse et la surveillance de votre ordinateur. Vous pouvez utiliser ces options pour déterminer les éléments à analyser, ce que l'analyse recherche et les opérations effectuées lorsqu'un virus ou une activité suspecte est détecté.

Avec des niveaux de protection supérieurs, il peut y avoir un léger compromis en terme de performances de l'ordinateur. Si vous remarquez une différence de performances après avoir installé Norton Internet Security, vous pouvez définir la protection sur un niveau inférieur ou désactiver les options superflues.

Option	Description
Auto-Protect	Vous permet de déterminer si l'option Auto-Protect s'exécute au démarrage de l'ordinateur, les éléments qu'elle recherche pendant la surveillance de l'ordinateur et les actions à entreprendre si un virus est détecté. Bloodhound est la technologie d'analyse qui protège contre les virus inconnus. Utilisez ces options pour définir ce niveau de sensibilité dans Auto-Protect. Les options avancées déterminent les activités à surveiller lors de la recherche d'activités suspectes et de l'analyse de disquettes. Les exclusions spécifient les fichiers qui ne doivent pas être analysés par extension de fichier ou nom de fichier spécifique. Veillez à ne pas exclure les types de fichiers susceptibles d'être infectés, comme les fichiers contenant des macros ou les exécutables.
Blocage de script	Activez le Blocage de script et spécifiez ce que doit faire Norton AntiViruss'il détecte un script dangereux. Si vous développez ou déboguez des scripts, désactivez le Blocage de script, sinon il risque de bloquer vos propres développements.
Analyse manuelle	Vous permet de déterminer les éléments à analyser et les opérations effectuées si un virus est détecté pendant une analyse que vous demandez. Les options d'analyse manuelle comprennent également les sous-catégories Bloodhound et Exclusions.

A propos des options Internet

Les options Internet définissent les opérations effectuées lorsque vous connectez votre ordinateur à Internet. Vous pouvez utiliser les options Internet pour définir comment Norton Internet Security doit analyser les courriers électroniques et les pièces jointes de la messagerie instantanée, activer la fonction Blocage des vers et déterminer le mode d'application des mises à jour LiveUpdate.

Option	Description
Messagerie	Vous permet d'activer l'analyse de la messagerie et Blocage des vers, et de définir le comportement de Norton AntiVirus pendant l'analyse des courriers électroniques. L'analyse des courriers électroniques entrants protège votre ordinateur contre les virus envoyés par d'autres ordinateurs. L'analyse des courriers électroniques sortants vous empêche de transmettre par mégarde des virus ou des vers à d'autres utilisateurs. Vous pouvez choisir d'analyser les courriers entrants ou sortants, voire les deux, et d'afficher une icône ou un indicateur de progression pendant l'analyse. Vous pouvez définir des options pour réparer, mettre en quarantaine ou supprimer automatiquement les courriers infectés avec ou sans votre intervention. Les options avancées déterminent les opérations à effectuer lors de l'analyse du courrier électronique
Messagerie instantanée	Vous permet de déterminer les messageries instantanées à prendre en charge, la configuration d'une nouvelle messagerie instantanée et les opérations à effectuer si un virus est détecté pendant une session de messagerie instantanée.
LiveUpdate	Activez LiveUpdate automatique et définissez le mode d'application des mises à jour. LiveUpdate automatique recherche les mises à jour des définitions de virus et des programmes automatiquement lorsque vous vous connectez à Internet.

A propos des autres options

Les autres options comprennent les paramètres d'inoculation pour Windows 98/98SE/Me et les paramètres divers. Vous pouvez activer l'inoculation, provoquer une alerte si un fichier système est modifié et définir de nombreuses options diverses.

Option	Description
Inoculation	Activez l'inoculation et, si un fichier système est modifié, choisissez de mettre à jour le cliché d'inoculation ou de réparer le fichier en le ramenant à ses valeurs initiales. Les options d'inoculation sont seulement disponibles sous Windows 98/98SE/Me.
Divers	Sauvegarder le fichier en quarantaine avant de tenter une réparation. (Cette option est automatiquement activée.) Activer le plug-in Office. Si vous vous mettez à niveau vers Microsoft Office 2000 ou ultérieur après avoir installé Norton Internet Security, vous devez activer cette option pour analyser automatiquement les fichiers Microsoft Office. M'avertir si ma protection antivirus est périmée. Analyser les fichiers au démarrage du système (Windows 98/98SE seulement). Activer la protection par mot de passe pour les options.

Options de protection par mot de passe

Vous pouvez protéger les options de Norton Internet Security et de Norton AntiVirus par des *mots de passe*. Ainsi, seules les personnes fiables sont à même de modifier vos options. Si vous avez installé des comptes et n'avez pas défini de mot de passe pour un compte actuel, le mot de passe que vous choisissez devient celui de votre compte.

Pour protéger les options de Norton Internet Security et de Norton AntiVirus, vous devez définir des mots de passe pour les deux produits.

Pour protéger les options de Norton Internet Security par un mot de passe

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre de Norton Internet Security, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Général, cochez **Activer la protection par mot de passe**.
   Si le compte actuellement connecté ne possède pas de mot de passe, vous devez en sélectionner un maintenant.
4. Cliquez sur **Définir mot de passe**.
5. Tapez un mot de passe dans les zones de texte Mot de passe et Confirmation du mot de passe.
   Si vous définissez également un mot de passe pour les options de Norton AntiVirus, vous pouvez utiliser le même mot de passe pour les deux.
6. Cliquez sur **OK**.

Pour protéger les options de Norton AntiVirus par un mot de passe

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre de Norton Internet Security, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la fenêtre des options de Norton AntiVirus, sou Autre, cliquez sur **Divers**.
4. Sous Contrôle d'accès aux paramètres, cochez **Activer la protection par mot de passe pour les options**.
5. Tapez un mot de passe dans les zones de texte Mot de passe et Confirmation du mot de passe.
   Si vous définissez également un mot de passe pour les options de Norton Internet Security, vous pouvez utiliser le même mot de passe pour les deux.
6. Cliquez sur **OK**.

Réinitialisation des mots de passe des options

Si vous oubliez les mots de passe des options, vous pouvez les redéfinir.

Pour redéfinir le mot de passe des options Norton Internet Security

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Internet Security** > **Désinstallation de Norton Internet Security**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Autres programmes** > **Norton Internet Security** > **Désinstallation de Norton Internet Security**.
2. Dans la fenêtre Suppression d'application, cliquez sur **Réinitialiser le mot de passe**.
3. Dans la zone de texte Réinitialiser la clé de mot de passe de la boîte de dialogue de réinitialisation du mot de passe, tapez la clé correspondante qui apparaît au-dessus de la zone de texte.
   La clé de réinitialisation du mot de passe est sensible à la casse.
4. Tapez un nouveau mot de passe dans les zones de texte Nouveau mot de passe et Confirmer le nouveau mot de passe.
5. Cliquez sur **OK**.
6. Dans la fenêtre Suppression d'application, cliquez sur **Annuler**.
7. Dans l'alerte Norton Internet Security, cliquez sur **Quitter**.
8. Dans l'alerte Installation annulée, cliquez sur **OK**.

Pour redéfinir le mot de passe des options Norton AntiVirus

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre Norton Internet Security, cliquez sur **Aide** > **A propos de Norton Internet Security**.
3. Sur l'onglet Norton AntiVirus de la fenêtre A propos de, cliquez sur **Réinitialiser le mot de passe**.
4. Dans la zone de texte Réinitialiser la clé de mot de passe de la boîte de dialogue de réinitialisation du mot de passe, tapez la clé correspondante qui apparaît au-dessus de la zone de texte.
   La clé de réinitialisation du mot de passe est sensible à la casse.
5. Tapez un nouveau mot de passe dans les zones de texte Nouveau mot de passe et Confirmer le nouveau mot de passe.
6. Cliquez sur **OK**.
7. Dans la fenêtre A propos de, cliquez sur **OK**.

Désactivation temporaire de Norton Internet Security

Il peut y avoir des cas où vous souhaiterez désactiver temporairement Norton Internet Security ou l'une de ses fonctionnalités. Par exemple, vous pouvez souhaiter afficher des publicités en ligne ou vérifier si Norton Internet Security empêche l'affichage d'une *page Web*.

Se reporter à "A propos des comptes Norton Internet Security" à la page 153.

Seuls les utilisateurs de type Adulte et Superviseur peuvent désactiver provisoirement Norton Internet Security. Les utilisateurs de type Enfant et Adolescent ne peuvent désactiver aucune partie de Norton Internet Security.

La désactivation de Norton Internet Security désactive également l'ensemble des fonctionnalités individuelles.

Pour désactiver temporairement Norton Internet Security

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Sécurité**.
3. Sur le côté droit de l'écran, cliquez sur **Désactiver**.

Norton Internet Security est automatiquement réactivé au prochain démarrage de l'ordinateur.

Vous pouvez également désactiver des fonctions de sécurité individuelles. Par exemple, vous pouvez vérifier si Personal Firewall entrave le bon fonctionnement d'un programme.

Pour désactiver une fonction de protection

1. Ouvrez Norton Internet Security.
2. Dans Security Center, sélectionnez la fonction à désactiver.
3. Sur le côté droit de l'écran, cliquez sur **Désactiver**.

Désactivation temporaire d'Auto-Protect

Se reporter à "Personnalisation de Norton AntiVirus" à la page 67.

Si vous n'avez pas modifié les paramètres par défaut, Auto-Protect se charge au démarrage de l'ordinateur pour vous protéger contre les virus. Cette protection recherche les virus dans les programmes qui s'exécutent et contrôle toute activité susceptible d'indiquer la présence d'un virus. Quand un virus ou une *activité suspecte* est détecté, Auto-Protect vous avertit.

Dans certains cas, Auto-Protect peut vous avertir d'une activité suspecte dont vous savez qu'elle n'est pas due à un virus. Si vous souhaitez éviter les alertes dans ce cas, vous pouvez désactiver temporairement Auto-Protect.

Si vous avez défini un *mot de passe* pour les options, Norton Internet Security vous le demande avant que vous ne puissiez afficher ou ajuster les paramètres.

Pour désactiver Auto-Protect

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la fenêtre Options, sous Système, cliquez sur **Auto-Protect**.
4. Dans le volet Auto-Protect, désélectionnez **Activer Auto-Protect**.

Veillez à activer Auto-Protect quand vous avez terminé, afin de garantir la protection de votre ordinateur.

Pour activer Auto-Protect

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la fenêtre Options, sous Système, cliquez sur **Auto-Protect**.
4. Dans le volet Auto-Protect, sélectionnez **Activer Auto-Protect**.

Si l'*icône* de Norton AntiVirus apparaît dans la barre d'état système de Windows, vous pouvez l'utiliser pour activer ou désactiver Auto-Protect.

Pour activer ou désactiver Auto-Protect à l'aide de l'icône de la barre d'état système

1. Dans la barre d'état système de Windows, cliquez avec le bouton droit sur l'icône de Norton AntiVirus.
2. Effectuez l'une des opérations suivantes :
   - Si Auto-Protect est désactivé, cliquez sur **Activer Auto-Protect**.
   - Si Auto-Protect est activé, cliquez sur **Désactiver Auto-Protect**.

Création de disquettes de sauvetage

Selon le *système d'exploitation* que vous utilisez, vous pouvez choisir de conserver un jeu de disquettes de sauvetage et de le maintenir à jour.

A propos des disquettes de sauvetage

Les disquettes de sauvetage enregistrent une copie des fichiers de démarrage système et des informations sur les partitions de disques, stockent les éléments de secours et un analyseur de virus sur plusieurs disquettes ou sur un lecteur *réseau*. Vous pouvez créer des disquettes de sauvetage pour les systèmes d'exploitation Windows 98/Me.

Un jeu de disquettes de sauvetage est composé d'une disquette amorçable, d'une disquette programme Norton AntiVirus et de plusieurs disquettes de définitions de virus. Si Norton Utilities est installé, le jeu de disquettes de sauvetage comprend également deux disquettes Norton Utilities. Ce jeu vous permet de démarrer l'ordinateur en mode DOS et d'utiliser Norton AntiVirus pour résoudre les problèmes de virus.

Les disquettes de sauvetage contiennent des informations propres à l'ordinateur sur lequel elles ont été créées. Si vous utilisez les disques de sauvetage pour une restauration, servez-vous de celles que vous avez créées pour votre ordinateur. Si vous les utilisez pour rechercher les virus, vous pouvez vous servir de celles que vous avez créées pour un autre ordinateur.

Les disquettes peuvent et doivent être mises à jour chaque fois que vous actualisez la protection antivirus, que vous installez de nouveaux logiciels ou que vous modifiez la configuration du matériel.

Création d'un jeu de disquettes de sauvetage

Vous pouvez créer les disquettes de sauvetage à tout moment. Vous pouvez démarrer l'assistant Rescue Disk depuis Security Center

Se reporter à "Désactivation temporaire d'Auto-Protect" à la page 73.

Vous devez désactiver temporairement Auto-Protect lorsque vous créez le jeu de disquettes de sauvetage. Si vous ne redémarrez pas l'ordinateur après avoir créé les disquettes de sauvetage, pensez à réactiver Auto-Protect.

Vous devez disposer de plusieurs disquettes formatées de 1,44 Mo.

Pour créer des disquettes de sauvetage

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Rescue**.
3. Sélectionnez le lecteur A pour créer le jeu de disquettes de sauvetage.
4. Cliquez sur **Créer**.
5. Etiquetez les disquettes en suivant les indications de la fenêtre Liste des disquettes de sauvetage de base, puis cliquez sur **OK**.
6. Insérez les disquettes comme demandé.

Test de vos disquettes de sauvetage

A la fin de la procédure de création des disquettes de sauvetage, un message vous propose de tester les disquettes. Vous devrez alors redémarrer l'ordinateur en utilisant les disques de sauvetage.

Pour tester vos disquettes de sauvetage

1. Fermez tous les programmes Windows.
2. Insérez la disquette étiquetée Disquette d'amorçage de base dans le lecteur A, puis cliquez sur **Redémarrer**.
   Si l'écran Disquette de secours s'affiche, cela signifie que la disquette de secours fonctionne correctement. Dans le cas contraire, plusieurs options peuvent vous permettre de résoudre le problème.
3. Appuyez sur **Echap** pour accéder à l'invite du DOS.
4. Retirez la disquette du lecteur A et faites coulisser en position ouverte le taquet de plastique situé au dos de la disquette pour la protéger en écriture.
5. Redémarrez l'ordinateur.

Se reporter à "Ma disquette de sauvetage ne fonctionne pas" à la page 227.

Mise à jour des disquettes de sauvetage

Vous pouvez mettre à jour les disquettes de sauvetage aussi souvent que vous le souhaitez. L'assistant Rescue Disk vous permet de mettre à jour les disquettes de sauvetage de base sans avoir à les recréer.

Si vous mettez à jour un jeu de disquettes, vérifiez qu'elles ne sont pas protégées en écriture.

Pour mettre à jour vos disquettes de sauvetage

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Rescue**.
3. Dans la zone de sélection du disque de destination, sélectionnez le lecteur A.
4. Cliquez sur **Mettre à jour**.
5. Insérez la disquette d'amorçage de base dans le lecteur A.
   Si elle est protégée en écriture, faites coulisser en position fermée le taquet de plastique pour la rendre inscriptible.
6. Cliquez sur **OK**.
7. Insérez les disquettes suivantes conformément aux instructions.

Se reporter à "Test de vos disquettes de sauvetage" à la page 76.

Testez les disquettes de sauvetage que vous venez de mettre à jour quand un message vous le demande.

Pour plus d'informations

Norton Internet Security fournit sur le *Web* des termes de glossaire, une aide en ligne, ce guide de l'utilisateur au format PDF, des didacticiels ainsi que des liens vers la base de connaissances du *site Web* de Symantec.

Recherche des termes de glossaire

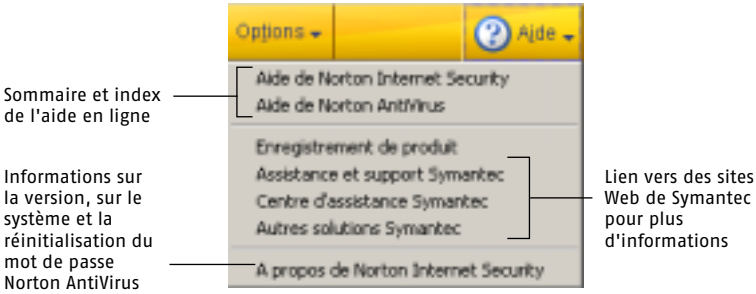
Les termes techniques indiqués en italiques dans le guide de l'utilisateur sont définis dans le glossaire disponible dans le fichier PDF du guide et dans l'aide. A ces deux emplacements, le fait de cliquer sur un terme vous donne sa définition.

Utilisation de l'aide en ligne

L'aide est en permanence disponible dans Norton Internet Security. Des boutons d'aide ou des liens vers des informations complémentaires fournissent des détails spécifiques à la tâche que vous effectuez. Le menu Aide vous offre un guide exhaustif pour toutes les fonctionnalités de produit et les tâches que vous pouvez effectuer.

Pour accéder à l'aide

1 En haut de la fenêtre Security Center, cliquez sur **Aide**.



2 Dans le menu principal de l'aide, cliquez sur **Aide Norton Internet Security**.

3 Dans le volet gauche de la fenêtre d'aide, sélectionnez l'un des onglets suivants :

- Sommaire : Affiche l'aide par rubrique.
- Index : Affiche les rubriques d'aide par mot clé et par ordre alphabétique.
- Rechercher : Ouvre un champ de recherche qui vous permet de saisir un mot ou une phrase.

Aide sur les fenêtres et les boîtes de dialogue

L'aide sur les fenêtres et les boîtes de dialogue fournit des informations sur le programme Norton Internet Security. Ce type d'aide est contextuel : l'aide affichée concerne la boîte de dialogue ou la fenêtre utilisée.

Pour accéder à l'aide sur les fenêtres et les boîtes de dialogue

❖ Effectuez l'une des opérations suivantes :

- Cliquez sur le lien **Plus d'infos** s'il est disponible.
- Dans la boîte de dialogue, cliquez sur **Aide**.

Fichier LisezMoi et notes de version

Le fichier LisezMoi contient des informations sur des questions d'installation et de compatibilité. Les notes de version contiennent des conseils techniques et des informations sur des modifications du produit intervenues après l'impression du présent manuel. Elles sont installées sur votre disque dur au même emplacement que les fichiers de Norton Internet Security.

Pour consulter le fichier LisezMoi

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Internet Security** > **Support produit**> **LisezMoi.txt**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Autres programmes** > **Norton Internet Security** > **Support produit** > **LisezMoi.txt**.

   Le fichier s'ouvre dans le Bloc-notes.
2. Une fois que vous avez fini de lire le fichier, fermez le traitement de texte.

Les notes de version sont également accessibles depuis le menu Démarrer.

Pour lire les notes de version

1. Effectuez l'une des opérations suivantes :
   - Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Programmes** > **Norton Internet Security** > **Support produit** > **Norton Internet Security Notes de version**.
   - Dans la barre des tâches de Windows XP, cliquez sur **Démarrer** > **Autres programmes** > **Norton Internet Security** > **Support produit** > **Norton Internet Security Notes de version**.

   Le fichier s'ouvre dans le Bloc-notes.
2. Une fois que vous avez fini de lire le fichier, fermez le traitement de texte.

Accès aux fichiers PDF du guide de l'utilisateur

Ce guide de l'utilisateur et le *guide de l'utilisateur de Norton AntiVirus* sont fournis sur le CD Norton Internet Security au format PDF. Pour pouvoir lire les PDF, vous devez installer Adobe Acrobat Reader sur l'ordinateur.

Pour installer Adobe Acrobat Reader

1. Insérez le CD Norton Internet Security dans le lecteur de CD-ROM.
2. Cliquez sur **Parcourir le CD**.
3. Cliquez deux fois sur le dossier **Manual**.
4. Cliquez deux fois sur le dossier **Acrobat**.
5. Cliquez deux fois sur **ar500enu.exe**.
6. Suivez les instructions affichées pour sélectionner un dossier de destination pour Adobe Acrobat Reader et terminer l'installation.

Une fois Adobe Acrobat Reader installé, vous pouvez lire les PDF depuis le CD.

Pour lire les PDF du guide de l'utilisateur depuis le CD

1. Insérez le CD Norton Internet Security dans le lecteur de CD-ROM.
2. Cliquez sur **Parcourir le CD**.
3. Cliquez deux fois sur le dossier **Manual**.
4. Cliquez deux fois sur le PDF à afficher. Les options sont les suivantes :

NIS2003.pdf	Ce guide de l'utilisateur
NAV2003.pdf	*Guide de l'utilisateur de Norton AntiVirus*

Vous pouvez également copier les guides sur le disque dur et les lire depuis ce disque. Les PDF nécessitent environ 5,5 Mo d'espace disque.

Pour lire les guides de l'utilisateur depuis le disque dur

1. Accédez à l'emplacement où vous avez copié le fichier PDF.
2. Cliquez deux fois sur le PDF à afficher. Les options sont les suivantes :

NIS2003.pdf	Ce guide de l'utilisateur
NAV2003.pdf	*Guide de l'utilisateur de Norton AntiVirus*

A propos de Norton Internet Security sur le Web

Le site Web de Symantec fournit des informations complètes sur Norton Internet Security. Il existe différents moyens d'accéder au site Web de Symantec.

Pour accéder au site Web Symantec à partir de la fenêtre principale de Norton Internet Security

1. Cliquez sur **Aide**.
2. Sélectionnez l'une des options suivantes :
   - Site Web de support technique : vous amène à la page de support technique du site Web de Symantec, où vous pouvez rechercher des solutions à des problèmes spécifiques, mettre à jour la protection antivirus et lire les dernières informations sur les technologies antivirus.
   - Visitez le site Web de Symantec : vous amène à la page d'accueil du site Web de Symantec, qui vous permet d'obtenir des informations sur tous les produits Symantec.

La page Rapports de Norton AntiVirus contient un lien vers le dictionnaire de virus en ligne de Symantec, comme le fait la barre d'outils de l'Explorateur Windows.

Pour accéder au site Web de Symantec à partir de la page Rapports

1. Dans Security Center, cliquez sur **Norton AntiVirus**.
2. Cliquez sur **Rapports**.
3. Sur la page Rapports, à côté de l'en-tête correspondant au dictionnaire de virus en ligne, cliquez sur **Afficher un rapport**.

Pour accéder au site Web de Symantec à partir de l'Explorateur Windows

1. Ouvrez l'Explorateur Windows.
2. Dans le menu Norton Internet Security de la barre d'outils, cliquez sur **Afficher le dictionnaire de virus**.
   Cette option vous connecte à la page Web de Symantec Security Response où vous pouvez rechercher des informations sur tous les types de virus.

Vous pouvez également accéder au site Web de Symantec par l'intermédiaire de votre navigateur Internet.

Pour accéder au site Web de Symantec depuis le navigateur

- Tapez l'adresse du site Web de Symantec, www.symantec.fr.

Exploration des didacticiels en ligne

Symantec fournit des didacticiels en ligne que vous pouvez utiliser pour examiner de nombreuses tâches courantes effectuées par Norton Internet Security.

Pour explorer les didacticiels en ligne

1. Accédez avec le navigateur à http://www.symantec.com/region/fr/techsupp/npf/npf_2002_info_tutorial.html
2. Sur la page Web des démos, sélectionnez le produit et la version pour lesquels vous souhaitez un didacticiel.
3. Cliquez sur **Continuer**.
4. Dans la liste des démos disponibles pour votre produit, sélectionnez celui que vous souhaitez examiner.

Inscription au bulletin d'informations de Symantec Security Response

Symantec publie chaque mois un bulletin d'informations électronique gratuit axé sur les besoins des clients de la sécurité Internet. Ce bulletin traite des dernières technologies antivirus produites par Symantec Security Response, des virus courants, des tendances en termes de travaux sur les virus, des avertissements d'épidémies de virus, et des versions de définitions de virus spécifiques.

Pour vous inscrire au bulletin d'informations de Symantec Security Response

1. Accédez avec votre navigateur à securityresponse.symantec.com
2. Sur la page Web de Security Response, défilez jusqu'à la zone de référence, puis cliquez sur **Newsletter**.
3. Sur la page Web du bulletin d'informations de Security Response, sélectionnez la langue dans laquelle vous souhaitez recevoir le bulletin.
4. Sur la page Web d'inscription, tapez les informations demandées, puis cliquez sur **S'abonner**.

Mises à jour avec LiveUpdate

5

Les produits Symantec ont besoin d'informations à jour pour protéger l'ordinateur des nouvelles menaces virales. Symantec met ces informations à votre disposition par l'intermédiaire de LiveUpdate. LiveUpdate utilise votre connexion Internet pour obtenir des mises à jour de programme et de définitions de virus pour l'ordinateur.

Lorsque vous utilisez LiveUpdate, vous ne payez que les frais d'accès à Internet habituels.

Si vous utilisez Norton Internet Security sous Windows 2000 ou Windows XP, vous devez posséder des droits d’accès administrateur pour exécuter LiveUpdate.

A propos des mises à jour de programme

Les mises à jour de programme sont des améliorations mineures apportées au produit installé. Elles diffèrent des mises à jour de produit, qui installent une nouvelle version d'un produit entier. Les mises à jour de programme dotées d'un programme d'installation intégré qui remplace le logiciel existant sont appelées « correctifs ». Les correctifs sont généralement créés pour augmenter la compatibilité du système d'exploitation ou du matériel, pour résoudre un problème de performances ou pour corriger une erreur.

La fonction LiveUpdate automatise l’obtention et l'installation des mises à jour de programme. Il recherche et obtient les fichiers sur un site Internet, les installe, puis supprime les fichiers superflus de l'ordinateur.

A propos des mises à jour de la protection antivirus

Les mises à jour de protection sont des fichiers disponibles par abonnement auprès de Symantec et destinés à actualiser vos produits Symantec sur base de la technologie antivirus la plus récente. Les mises à jour de protection reçues dépendent des produits que vous utilisez.

Norton AntiVirus, Norton SystemWorks	Les utilisateurs de Norton AntiVirus et de Norton SystemWorks reçoivent des mises à jour du service des définitions de virus, qui donnent accès aux dernières signatures de virus et autres technologies Symantec.
Norton Internet Security	En plus du service de définition des virus, les utilisateurs de Norton Internet Security reçoivent des mises à jour de protection pour le service de filtrage Web, le service de détection des intrusions et l'alerte concernant le courrier non désiré. Les mises à jour du service de filtrage Web donnent accès aux listes d'adresses et de catégories de sites les plus récentes pour identifier les contenus Web contestables. Les mises à jour du service de détection des intrusions donne accès aux règles de firewall prédéfinies les plus récentes et aux listes d'applications accédant à Internet. Ces listes permettent d'identifier les tentatives d'accès non autorisés à votre ordinateur. Les mises à jour d'alertes de courrier non désiré donnent accès aux définitions les plus récentes et aux listes actualisées de caractéristiques de courrier non désiré. Ces listes permettent d'identifier les e-mails non désirés.
Norton Personal Firewall	Les utilisateurs de Norton Personal Firewall reçoivent des mises à jour du service de détection des intrusions pour les règles de firewall prédéfinies les plus récentes et les listes d'applications accédant à Internet.

Informations sur l'abonnement

Se reporter à "Politique d'abonnement" à la page 277.

Votre produit Symantec comprend un abonnement limité sans frais vous permettant de bénéficier de mises à jour de protection correspondant aux services d'abonnement utilisés par votre produit. Lorsque cet abonnement est sur le point d'expirer, un message vous rappelle de le renouveler.

Si vous ne renouvelez pas votre abonnement, vous pouvez continuer à utiliser LiveUpdate pour obtenir des mises à jour de programme. Cependant, vous ne pourrez plus récupérer les mises à jour de la protection antivirus et vous ne serez plus protégé contre les nouvelles menaces découvertes.

Quand mettre à jour ?

Exécutez LiveUpdate aussitôt après l'installation du produit. Une fois vos fichiers actualisés, exécutez régulièrement LiveUpdate pour obtenir des mises à jour. Par exemple, pour maintenir la protection antivirus à jour, utilisez LiveUpdate une fois par semaine ou chaque fois que de nouveaux virus sont découverts. Les mises à jour des programmes sont mises à disposition suivant les besoins.

Demander une alerte de mise à jour

Pour vous assurer que les mises à jour de protection sont actualisées, vous pouvez demander à être informé par e-mail à chaque épidémie de virus ou à chaque nouvelle menace à la sécurité d'Internet. Le message d'alerte décrit la menace, fournit des instructions de détection et de suppression et vous donne des informations pour la sécurité de votre ordinateur. Vous devez toujours exécuter LiveUpdate après réception d'une de ces alertes.

Pour demander une alerte de mise à jour

1. A l'aide de votre navigateur, accédez à http://securityresponse.symantec.com/avcenter
2. Faites défiler jusqu'au bas de la page Web Security Response, puis cliquez sur **Symantec security response - Free Subscription - Click here!**.
3. Dans la page Web Abonnement aux alertes concernant la sécurité, complétez le formulaire d'abonnement.
4. Cliquez sur **Send me free Security Alerts!**

Si vous exécutez LiveUpdate sur un réseau interne

Si vous exécutez LiveUpdate sur un ordinateur connecté à un réseau protégé par un pare-feu de société, votre administrateur de réseau pourra installer un serveur LiveUpdate interne sur le réseau. LiveUpdate doit trouver automatiquement cet emplacement.

Si vous éprouvez des problèmes de connexion à un serveur LiveUpdate interne, contactez votre administrateur de réseau.

Si vous ne pouvez pas utiliser LiveUpdate

Lorsque de nouvelles mises à jour sont disponibles, Symantec les place sur son site Web. Si vous ne pouvez pas exécuter LiveUpdate, vous pouvez obtenir de nouvelles mises à jour à partir du site Web de Symantec.

Votre abonnement doit être valide pour que vous puissiez obtenir de nouvelles mises à jour de protection à partir du site Web de Symantec.

Pour obtenir des mises à jour à partir du site Web de Symantec

1. Visitez le site Symantec Security Response : http://securityresponse.symantec.com
2. Suivez les liens pour obtenir le type de mise à jour nécessaire.

Obtenir des mises à jour à l'aide de LiveUpdate

LiveUpdate vérifie les mises à jour de tous les produits Symantec installés sur votre ordinateur.

Si vous utilisez AOL, CompuServe ou Prodigy, connectez-vous à Internet avant d'exécuter LiveUpdate.

Pour obtenir des mises à jour à l'aide de LiveUpdate

1. Ouvrez le produit Symantec.
2. En haut de la fenêtre, cliquez sur **LiveUpdate**.
   Un avertissement vous signalera peut-être que votre abonnement a expiré. Suivez les instructions affichées pour le renouveler.

3 Dans la fenêtre LiveUpdate, cliquez sur **Suivant** pour détecter les mises à jour.

4 Si des mises à jour sont proposées, cliquez sur **Suivant** pour les télécharger et les installer.

5 Quand l'installation est terminée, cliquez sur **Terminer**.

Certaines mises à jour ne prendront effet qu'après le redémarrage de l'ordinateur.

Paramétrez LiveUpdate pour opérer en mode interactif ou en mode express

LiveUpdate s'exécute en mode interactif ou en mode express. En mode interactif (option par défaut), LiveUpdate télécharge une liste de mises à jour disponible pour vos produits Symantec pris en charge par la technologie LiveUpdate. Vous pouvez alors choisir les mises à jour que vous voulez installer. En mode express, LiveUpdate installe automatiquement toutes les mises à jour de vos produits Symantec.

Pour paramétrer LiveUpdate pour opérer en mode interactif ou en mode express.

1 Ouvrez le produit Symantec.

2 En haut de la fenêtre, cliquez sur **LiveUpdate**.

3 Dans l'écran de bienvenue de LiveUpdate, cliquez sur **Configure**.

4 Dans l'onglet Général de la boîte de dialogue Configuration de LiveUpdate, choisissez **Mode interactif** ou **Mode express**.

5 Si vous avez choisi le Mode express, sélectionnez la manière de vérifier les mises à jour :

- Pour avoir la possibilité d'annuler la mise à jour, sélectionnez **Je veux appuyer sur le bouton Démarrer pour exécuter LiveUpdate**.
- Pour que les mises à jour soient installées automatiquement à chaque démarrage de LiveUpdate, sélectionnez **Je veux que LiveUpdate démarre automatiquement**.

6 Cliquez sur **OK**.

Désactiver le mode express

Après avoir paramétré LiveUpdate pour s'exécuter en mode express, vous ne pouvez plus accéder à la boîte de dialogue Configuration de LiveUpdate directement à partir de LiveUpdate. Vous devez utiliser le panneau de configuration de Symantec LiveUpdate.

Pour désactiver le mode express

1. Dans la barre des tâches Windows, cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.
2. Dans la fenêtre Panneau de configuration, double-cliquez sur **Symantec LiveUpdate**.
3. Dans l'onglet Général de la boîte de dialogue Configuration de LiveUpdate, choisissez **Mode interactif**.
4. Cliquez sur **OK**.

Exécution automatique de LiveUpdate

Vous pouvez demander à LiveUpdate de contrôler automatiquement les mises à jour de programme de protection, selon le programme paramétré, en activant des sessions LiveUpdate automatiques. Vous devez poursuivre l'exécution de LiveUpdate manuellement pour recevoir des mises à jour de produit.

Les sessions LiveUpdate automatiques vérifient une connexion Internet toutes les cinq minutes, jusqu'à ce qu'elle réponde et, par la suite, toutes les quatre heures. Si votre routeur RNIS est paramétré pour se connecter automatiquement à votre fournisseur d'accès Internet, de nombreuses connexions seront effectuées et chacune pourra occasionner des frais téléphoniques. Pour éviter cela, configurez le routeur RNIS de manière à désactiver la connexion automatique au fournisseur d'accès ou désactivez les sessions automatiques LiveUpdate dans les options Norton Internet Security.

Pour activer les sessions LiveUpdate automatiques

1. Démarrez Norton Internet Security.
2. En haut de la fenêtre principale de Norton Internet Security, cliquez sur **Options** > **Internet Security**.

Si vous définissez un mot de passe pour les options, Norton Internet Security vous demande de saisir le mot de passe avant de continuer.

3 Dans le volet LiveUpdate, cochez la case **Activer une session LiveUpdate automatique**.

4 Si vous voulez être prévenu lorsque des mises à jour Norton Internet Security sont disponibles, cochez **Me prévenir lorsque des mises à jour sont disponibles**.

5 Sélectionnez les mises à jour à vérifier par la session LiveUpdate automatique.

6 Pour chaque type de mise à jour que vous voulez demander à la session LiveUpdate automatique de vérifier, définissez la façon dont ces mises à jour doivent être appliquées en sélectionnant une des options suivantes :

Mettre à jour automatiquement ma protection	LiveUpdate recherche et installe les mises à jour de la protection antivirus sans vous consulter. LiveUpdate affiche une alerte lorsqu'une mise à jour de protection a été téléchargée. Vous devez toutefois exécuter LiveUpdate de temps en temps afin de rechercher les mises à jour de programme.
Me prévenir	LiveUpdate recherche les mises à jour des définitions de virus et vous demande si vous souhaitez les installer.

7 Cliquez sur **OK**.

Pour supprimer les sessions LiveUpdate automatiques programmées, désactivez l'option de sessions LiveUpdate automatiques.

Pour désactiver les sessions LiveUpdate automatiques

1 Démarrez Norton Internet Security.

2 En haut de la fenêtre principale de Norton Internet Security, cliquez sur **Options > Internet Security**.

Si vous définissez un mot de passe pour les options, Norton Internet Security vous demande de saisir le mot de passe avant de continuer.

3 Dans la boîte de dialogue Options de Norton Internet Security, cliquez sur l'onglet **LiveUpdate**.

4 Dans le volet LiveUpdate, désactivez l'option **Activer une session LiveUpdate automatique**.

5 Cliquez sur **OK**.

Contrôle de l'accès aux ordinateurs protégés

6

Norton Internet Security peut être configuré pour répondre à vos besoins dans de nombreuses situations. Vous pouvez utiliser le programme pour contrôler l'accès de votre ordinateur à la fois aux ordinateurs locaux et par l'intermédiaire d'Internet. Vous pouvez également contrôler les modalités d'accès des utilisateurs extérieurs à votre ordinateur.

Contrôle de l'utilisation de votre ordinateur

Norton Internet Security contrôle toutes les *connexions*, y compris celles entre les ordinateurs de votre domicile. Après l'installation, il peut être nécessaire d'ajuster quelques paramètres afin de partager des fichiers, des imprimantes et d'autres ressources avec d'autres ordinateurs.

Connexion à un réseau

Chaque fois que vous utilisez le partage de fichiers de Windows pour échanger des fichiers, que vous imprimez sur une imprimante partagée ou que vous vous connectez à Internet avec un *modem* ou une connexion à haut débit, votre ordinateur se connecte à un *réseau* composé d'autres ordinateurs. En tant que membre d'un réseau, votre ordinateur est vulnérable aux attaques. Norton Internet Security surveille automatiquement l'ensemble des connexions réseau afin de garantir la sécurité de l'ordinateur.

En temps normal, votre ordinateur se connecte à un réseau à la suite d'une action de votre part. Une connexion inattendue peut indiquer qu'un programme nuisible tente d'envoyer des informations sur Internet. Certaines cartes réseau sans fil analysent automatiquement tout réseau à leur portée et s'y connectent. Si vous vous déplacez avec un ordinateur portable équipé d'une telle carte, vous constaterez peut-être qu'il se connecte à des réseaux sans fil dans les aéroports et autres lieux publics.

Se reporter à "Contrôle de Norton Internet Security" à la page 207.

Dès qu'une connexion réseau est établie, Norton Internet Security en commence automatiquement la surveillance. Il n'est pas nécessaire d'effectuer des modifications pour être protégé. Norton Internet Security vous avertit de la nouvelle connexion et l'enregistre dans le *journal des connexions*.

Activation du partage de fichiers et d'imprimantes

Le réseau Microsoft permet de partager des fichiers et des imprimantes. Par défaut, Norton Internet Security empêche tout ordinateur d'accéder à ces *services* sur un ordinateur protégé.

Pour partager des fichiers et donner accès à des imprimantes sur votre *réseau* local, vous devez activer le partage de fichiers et d'imprimantes. Si vous activez ces fonctionnalités sur votre réseau local, elles restent protégées des internautes malintentionnés.

Avant d'activer le partage de fichiers et d'imprimantes sur votre réseau local, assurez-vous que chaque ressource partagée est protégée par un *mot de passe* sécurisé. Pour plus d'informations sur la sécurisation des ressources partagées, consultez le fichier Aide de Windows dans le menu Démarrer.

Pour activer le partage de fichiers et d'imprimantes

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Firewall personnel, cliquez sur **Règles générales** sur l'onglet Avancé.
4. Dans la fenêtre Règles générales, sélectionnez l'entrée pour le partage de fichiers ou d'imprimantes Windows.
5. Cliquez sur **Modifier**.
6. Sur l'onglet Action de la boîte de dialogue Modifier une règle, cliquez sur **Autoriser l'accès à Internet**.

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Règles générales, cliquez sur **OK**.

9 Dans la fenêtre Firewall avancé, cliquez sur **OK**.

Organisation des ordinateurs en zones de réseau

Norton Internet Security vous permet d'organiser les ordinateurs de votre réseau personnel et sur Internet en deux zones : Approuvés et Restreints.

Les ordinateurs placés dans la zone Approuvés ne sont pas surveillés par Norton Internet Security. Ils bénéficient du même accès à votre ordinateur que si Norton Internet Security n'était pas installé. Réservez cette zone aux ordinateurs de votre réseau personnel avec lesquels vous avez besoin de partager des fichiers et des imprimantes. Si un ordinateur de la zone Approuvés est attaqué et si un intrus en prend le contrôle, tous les ordinateurs de la zone Approuvés sont menacés.

Les ordinateurs placés dans la zone Restreints ne peuvent pas du tout accéder à votre ordinateur. Si un ordinateur se trouve dans la zone Restreints, toute communication qui en provient est automatiquement bloquée.

Si vous avez plusieurs ordinateurs chez vous, vous les ajouterez probablement à votre zone Approuvés. N'ajoutez d'ordinateurs externes à cette zone que s'il s'agit d'utilisateurs de confiance qui disposent d'un logiciel de pare-feu installé.

L'assistant de contrôle de zone permet d'organiser rapidement les ordinateurs dans les zones. Vous pouvez aussi répartir les ordinateurs manuellement.

Pour ouvrir l'assistant de contrôle de zone depuis Security Center

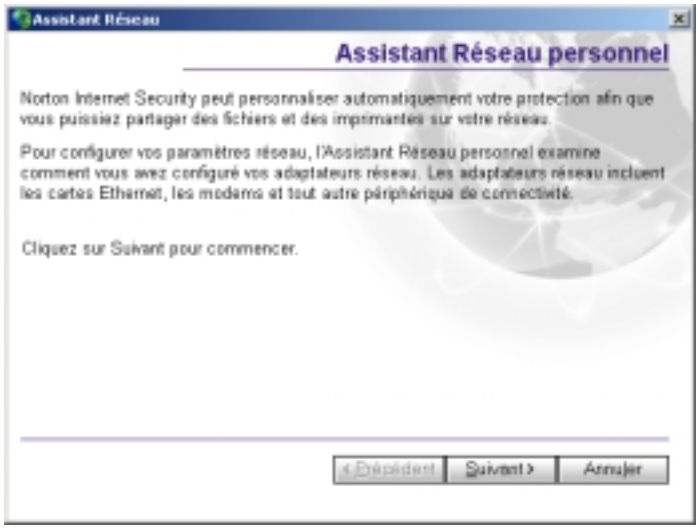
1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Firewall personnel**.

3 Dans la fenêtre Firewall personnel, cliquez sur l'onglet **Réseau personnel**.

Pour ouvrir l'Assistant de contrôle de zone depuis Security Monitor

1. Ouvrez Norton Internet Security.
2. Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Configurer un réseau personnel**.



Pour organiser des ordinateurs en zones ave l'Assistant de contrôle de zone

1. Dans l'Assistant de contrôle de zone, cliquez sur **Suivant**.
2. Dans la liste obtenue, cochez les adaptateurs réseau que vous souhaitez que Norton Internet Security configure automatiquement et ajoute à la zone Approuvés.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Terminer** pour fermer l'assistant.

Pour ajouter manuellement des ordinateurs aux zones

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Firewall personnel**.
3. Dans la fenêtre Firewall personnel, sur l'onglet Réseau personnel, sélectionnez la zone à laquelle vous voulez ajouter un ordinateur.
4. Cliquez sur **Ajouter**.

5 Utilisez la fenêtre Indiquer les ordinateurs pour identifier l'ordinateur.

6 Quand vous avez fini d'ajouter des ordinateurs, cliquez sur **OK**.

Se reporter à "Identification des ordinateurs dans Norton Internet Security" à la page 95.

Pour supprimer des ordinateurs des zones

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Firewall personnel**.

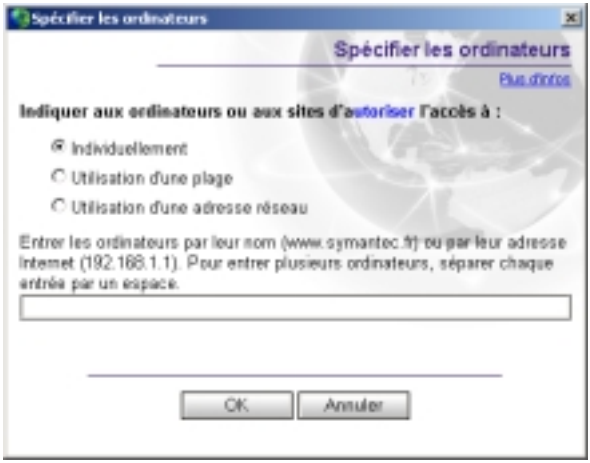
3 Sélectionnez l'ordinateur que vous souhaitez supprimer.

4 Cliquez sur **Supprimer**.

5 Quand vous avez fini de supprimer des ordinateurs, cliquez sur **OK**.

Identification des ordinateurs dans Norton Internet Security

Vous devez identifier les ordinateurs dans Norton Internet Security pour configurer manuellement les zones du réseau, les règles de filtrage et d'autres fonctions de protection. Dans ce cas, la boîte de dialogue Indiquer les ordinateurs apparaît.



Se reporter à "A propos d'Internet" à la page 235.

Cette boîte de dialogue permet d'identifier des ordinateurs de trois façons. Dans tous les cas, vous pouvez indiquer des *adresses IP*.

Recherche de l'adresse IP d'un ordinateur

Deux méthodes permettent de trouver l'adresse IP d'un ordinateur : Sur les ordinateurs Windows 98/Me, vous pouvez utiliser Winipcfg pour trouver l'adresse IP d'un ordinateur. Sur les ordinateurs Windows 2000/XP, vous pouvez utiliser Ipconfig pour trouver l'adresse IP d'un ordinateur.

Pour rechercher une adresse IP avec Winipcfg

1. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Exécuter**.
2. Dans la boîte de dialogue Exécuter, tapez **winipcfg**
3. Cliquez sur **OK**.
4. Sélectionnez un adaptateur réseau.
5. Notez l'adresse IP.

Pour rechercher une adresse IP avec Ipconfig

1. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Exécuter**.
2. Dans la boîte de dialogue Exécuter, tapez **cmd**.
3. Cliquez sur **OK**.
4. A l'invite de commande, tapez **ipconfig**.
5. Cliquez sur **OK**.
6. Notez l'adresse IP.

Spécification d'un ordinateur individuel

Le nom de l'ordinateur peut être une adresse IP, une *URL* comme service.symantec.com ou un nom de réseau Microsoft comme Mojave. Vous pouvez trouver le nom des ordinateurs du réseau local dans le Voisinage réseau ou dans les Favoris réseau Windows.

Si le protocole TCP/IP n'est pas associé au Client pour les réseaux Microsoft dans les propriétés réseau Windows, vous devez utiliser des adresses IP au lieu de noms pour désigner les ordinateurs du réseau local.

Pour spécifier un ordinateur individuel

1. Dans la boîte de dialogue Indiquer les ordinateurs, cliquez sur **Individuellement**.
2. Tapez le nom ou l'adresse IP de l'ordinateur.
3. Cliquez sur **OK**.

Spécification d'une série d'ordinateurs

Vous pouvez identifier une plage d'ordinateurs en indiquant l'adresse IP de départ (plus petit nombre) et celle de fin (plus grand nombre). Tous les ordinateurs compris dans la plage d'adresses IP sont inclus.

Dans la plupart des cas, les trois premiers nombres sur les quatre qui composent une adresse IP sont identiques.

Pour spécifier une plage d'ordinateurs

1. Dans la boîte de dialogue Indiquer les ordinateurs, cliquez sur **A l'aide d'une plage**.
2. Dans le champ Adresse Internet de départ, tapez l'adresse IP de départ (plus petit nombre).
3. Dans le champ Adresse Internet de fin, tapez l'adresse IP de fin (plus grand nombre).
4. Cliquez sur **OK**.

Spécification d'ordinateurs avec une adresse réseau

Se reporter à "Identification des ordinateurs sur Internet" à la page 242.

Vous pouvez identifier tous les ordinateurs d'un même *sous-réseau* en spécifiant une adresse IP et un masque de sous-réseau. L'adresse IP spécifiée peut être n'importe quelle adresse du sous-réseau identifié.

Pour spécifier des ordinateurs avec une adresse réseau

1. Dans la fenêtre Indiquer les ordinateurs, cliquez sur **A l'aide d'une adresse réseau**.
2. Dans le champ Adresse réseau, tapez l'adresse IP de l'un des ordinateurs du sous-réseau.
3. Dans le champ Masque de sous-réseau, tapez le masque de sous-réseau.
   Le masque de sous-réseau est presque toujours 255.255.255.0.
4. Cliquez sur **OK**.

Si vous utilisez le protocole DHCP

Si votre *FAI* utilise un serveur *DHCP* (dynamic host control protocol) pour fournir des adresses IP aux ordinateurs des utilisateurs, soyez prudent lorsque vous tapez les adresses IP.

Au lieu d'identifier un ordinateur avec une seule adresse IP, qui peut changer à tout moment, indiquez une adresse réseau en utilisant une adresse IP de base et un masque de sous-réseau. Fournissez des valeurs couvrant la plage d'adresses qui peuvent être attribuées à l'ordinateur.

Contrôle de l'accès des utilisateurs à Internet

Norton Internet Security prend en charge la plupart des méthodes de *connexion* à Internet sans nécessiter de configuration supplémentaire.

Si vous accédez à Internet via un routeur câble ou DSL

Norton Internet Security fonctionne derrière un *routeur* câble ou DSL et renforce la protection assurée par le routeur. Dans certains cas, il peut être utile de réduire la protection fournie par le routeur pour pouvoir utiliser des applications telles que NetMeeting ou Microsoft Messenger. Norton Internet Security propose également des fonctions qui peuvent ne pas être disponibles avec les routeurs câble et DSL, comme le Contrôle de confidentialité.

Si des ordinateurs multiples partagent une même connexion à Internet

Norton Internet Security fonctionne avec la plupart des programmes de partage de connexion à Internet. Pour protéger votre réseau des nombreuses attaques extérieures, installez Norton Internet Security sur l'ordinateur passerelle. Pour une protection optimale contre les *chevaux de Troie* ou autres applications qui initient des *connexions sortantes*, installez Norton Internet Security sur tous les ordinateurs qui partagent la connexion.

Si votre FAI utilise un serveur proxy

Norton Internet Security fonctionne avec la plupart des serveurs *proxy*. Vous pouvez toutefois être amené à modifier certains paramètres afin de bénéficier d'une protection totale.

Pour savoir si Norton Internet Security est compatible avec votre serveur proxy

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la catégorie Web, consultez le compteur Octets traités.
5. Utilisez votre navigateur pour vous connecter à un site Web.
   Le compteur Octets traités de la fenêtre Statistiques détaillées doit augmenter quand vous accédez à des pages Web. Cela indique que Norton Internet Security est correctement configuré pour fonctionner avec votre serveur proxy.
6. Pour fermer la fenêtre Statistiques détaillées, cliquez sur **Quitter** dans le menu Fichier.

Si le compteur Octets traités reste à 0, Norton Internet Security ne contrôle probablement pas le port utilisé par le serveur proxy. Vous devrez déterminer quels ports votre serveur proxy utilise pour les communications HTTP, puis configurer Norton Internet Security pour surveiller ces ports.

Pour déterminer le port à surveiller pour les communications HTTP

1. Ouvrez Norton Internet Security.
2. Utilisez votre navigateur pour vous connecter à un site Web.
3. Dans Security Center, cliquez sur **Statistiques**.
4. Dans la fenêtre Statistiques, cliquez sur **Journaux**.
5. Sur l'onglet Connexions de la colonne Distant, consultez les informations.
   Un numéro de port figure à la suite de l'adresse IP du site chargé. Il s'agit du port utilisé pour accéder au serveur proxy et établir la connexion au site Web.
6. Notez le numéro du port.

Pour spécifier les ports à surveiller pour les communications HTTP

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Pare-feu, sous Liste de ports HTTP, effectuez l'une des opérations suivantes :
   - Pour ajouter un port à la liste des ports HTTP, cliquez sur **Ajouter** puis indiquez le numéro du port à surveiller pour les communications HTTP.
   - Pour supprimer un port de la liste des ports HTTP, cliquez sur le numéro du port dans la liste puis cliquez sur **Supprimer**.
4. Cliquez sur **OK**.

Contrôle de l'accès des utilisateurs extérieurs à votre réseau

Norton Internet Security peut protéger les ordinateurs tout en autorisant des utilisateurs externes à accéder aux serveurs de votre *réseau*. Pour exécuter des *serveurs* sur des ordinateurs protégés, vous devrez probablement créer des règles de filtrage permettant aux utilisateurs extérieurs de se connecter à certains ports. Pour une sécurité optimale, ne créez ces règles que sur les ordinateurs qui exécutent vos serveurs.

Si vous exécutez un serveur Web

Pour qu'un serveur Web puisse s'exécuter derrière Norton Internet Security, vous devez créer une règle de filtrage autorisant les *connexions* TCP entrantes sur le port 80. La manière la plus simple de procéder consiste à créer ces règles via une *alerte* de Norton Internet Security.

Pour créer des règles pour un serveur Web avec une alerte de Norton Internet Security

1. Sur le serveur Web, affichez votre site Web en indiquant l'adresse IP dans la barre d'adresse du navigateur.
   Norton Internet Security affiche une alerte.
2. Dans le menu déroulant de l'alerte, cliquez sur **Configurer l'accès à Internet automatiquement**.
3. Cliquez sur **OK**.

Si vous exécutez un serveur FTP

Pour permettre à un serveur FTP de s'exécuter derrière Norton Internet Security, vous devez créer les règles suivantes :

- Autoriser les connexions TCP entrantes sur le port 21.
- Autoriser les connexions TCP sortantes sur le port 22.
- Autoriser les connexions TCP entrantes sur les ports 1024 à 5000.

La manière la plus simple de procéder consiste à créer ces règles via une alerte de Norton Internet Security.

Pour créer des règles pour un serveur FTP avec une alerte de Norton Internet Security

1. Dans la barre d'adresses de votre navigateur, tapez **FTP://** suivi de l'adresse IP de votre serveur FTP.
   Norton Internet Security affiche une alerte.
2. Dans le menu déroulant de l'alerte, cliquez sur **Configurer l'accès à Internet automatiquement**.
3. Cliquez sur **OK**.

Si vous exécutez Symantec pcAnywhere

Se reporter à "Modification d'une règle de filtrage existante" à la page 123.

Vous ne devriez pas rencontrer de problèmes avec Symantec pcAnywhere utilisé comme client ou Elève avec Norton Internet Security. Pour bénéficier d'une protection maximale si vous utilisez un Elève pcAnywhere, modifiez la règle pour limiter son utilisation aux seuls ordinateurs que vous utilisez avec l'Elève. Cette précaution, combinée aux *mots de passe* de Symantec pcAnywhere, offre un niveau de protection optimal.

Si vous exécutez un réseau privé virtuel

Norton Internet Security fonctionne avec les réseaux privés virtuels (VPN) suivants :

- Nortel
- VPNRemote
- PGP
- SecureRemote

Avec la plupart des VPN, vous ne pouvez pas voir Internet ou d'autres ordinateurs du réseau local quand le client VPN est actif. Vous ne pouvez voir que ce qui est disponible par l'intermédiaire du serveur VPN auquel vous êtes connecté.

Protection contre les tentatives d'intrusion

7

Les attaques issues d'Internet exploitent la manière dont les ordinateurs transfèrent les données. Norton Internet Security protège votre ordinateur en surveillant les informations entrantes et sortantes, et en bloquant toute tentative d'attaque.

Sur Internet, les informations circulent sous la forme de *paquets*. En plus des données, chaque paquet comprend un en-tête contenant des informations sur l'ordinateur à l'origine de l'envoi, le destinataire, le mode de traitement des données du paquet et le port de réception du paquet.

Les *ports* sont des canaux qui divisent le flux de données issu d'Internet en itinéraires distincts traités par des applications individuelles. Les applications Internet exécutées sur un ordinateur sont à l'écoute d'un ou de plusieurs ports et acceptent les informations qui y sont envoyées.

Les attaques de réseau sont conçues pour exploiter les faiblesses de certaines applications Internet. Les pirates utilisent des outils qui envoient à un port particulier des paquets contenant du code de programmation malveillant. Si une application vulnérable à cette attaque est à l'écoute de ce port, le code permet au pirate d'accéder à l'ordinateur, de le désactiver, voire même de le contrôler. Le code de programmation servant à générer les attaques peut être inclus dans un seul paquet ou se répartir sur plusieurs paquets.

Protection offerte par Norton Internet Security contre les attaques de réseau

Norton Internet Security est doté de trois outils de protection contre les tentatives d'intrusion, les contenus Web malveillants et les *chevaux de Troie* :

- Norton Personal Firewall
  Contrôle toutes les communications Internet et crée un bouclier qui bloque ou limite les tentatives pour accéder aux informations de votre ordinateur.
- Détection d'intrusion
  Analyse toutes les informations entrantes et sortantes pour rechercher des modèles de données caractéristiques d'une attaque.
- Visual Tracking
  Identifie l'ordinateur à l'origine de l'attaque.

Surveillance des communications par Norton Personal Firewall

Lorsque Norton Personal Firewall est actif, il surveille les communications entre votre ordinateur et d'autres ordinateurs sur Internet. Il protège également votre ordinateur contre les problèmes de sécurité courants :

Tentatives de connexion anormales	Vous avertit de toute tentative de connexion provenant d'autres ordinateurs et des tentatives d'applications de votre ordinateur de se connecter à d'autres ordinateurs.
Chevaux de Troie	Vous avertit quand votre ordinateur rencontre des programmes malveillants qui prennent l'apparence d'applications utiles.
Infractions à la sécurité et à la confidentialité issues de contenus Web malveillants	Surveille l'ensemble des applets Java et contrôles ActiveX, et permet de choisir de les exécuter ou de les bloquer.
Analyses de port	Masque les ports inactifs de votre ordinateur et détecte les analyses de port.
Intrusions	Détecte et bloque les transmissions malveillantes et les tentatives d'attaque émanant d'utilisateurs externes.

Se reporter à "Personnalisation de la protection du pare-feu" à la page 107.

Vous pouvez contrôler le niveau de protection offert par Norton Personal Firewall à l'aide du curseur de niveau de sécurité. Vous pouvez également configurer la réaction de Norton Personal Firewall à des tentatives de connexions incorrectes, des chevaux de Troie et des contenus Web malveillants.

Détection d'intrusion et analyse des communications

La Détection d'intrusion analyse chaque *paquet* entrant ou sortant de votre ordinateur pour vérifier la présence de signatures d'attaque. Une signature d'attaque est un groupe de données qui identifie une tentative de piratage visant à exploiter une faille connue d'un système d'exploitation ou d'une application.

Norton Internet Security protège votre ordinateur contre les attaques les plus fréquente, notamment celles-ci :

Bonk	Attaque de la pile TCP/IP Microsoft capable de bloquer l'ordinateur cible.
RDS_Shell	Utilisation du composant RDS (Remote Data Services, services de données distants) de Microsoft Data Access Components permettant à un pirate d'exécuter des commandes à distance avec les privilèges système.
WinNuke	Utilisation de NetBIOS pour bloquer les ordinateurs exécutant l'un des anciens systèmes d'exploitation Windows.

Comme les attaques peuvent se répartir sur plusieurs paquets, la détection d'intrusion examine les paquets de deux manières différentes. D'une part, elle analyse chaque paquet individuellement pour rechercher les modèles de données caractéristiques d'une attaque. D'autre part, elle surveille les paquets sous forme de flux de données afin d'identifier les attaques réparties sur plusieurs paquets.

Si les informations correspondent à une attaque connue, la Détection d'intrusion rejette automatiquement le paquet et interrompt la *connexion* avec l'ordinateur à l'origine de l'envoi des données. L'ordinateur est ainsi protégé contre toutes les attaques possibles.

Vous pouvez modifier la façon dont la Détection d'intrusion répond aux attaques en excluant de la surveillance certaines signatures d'attaque et en activant/désactivant la fonction AutoBlock, qui bloque automatiquement toute communication issue de l'ordinateur à l'origine d'une attaque. L'exclusion du blocage de certains comportements de réseau vous permet de continuer à travailler, même lorsque votre ordinateur subit une attaque.

Parallèlement à la protection qu'il vous offre contre les attaques, Norton Internet Security surveille toutes les informations que votre ordinateur envoie à d'autres ordinateurs. Cela permet de s'assurer que votre ordinateur ne peut pas servir à attaquer d'autres utilisateurs ni être exploité par des programmes *zombies*. Si Norton Internet Security détecte que votre ordinateur envoie des informations caractéristiques d'une attaque, il bloque immédiatement la connexion et vous avertit du problème potentiel.

Pour réduire le nombre d'avertissements, Norton Internet Security surveille uniquement les attaques visant les ports que votre ordinateur utilise. Si un pirate tente de se connecter à votre ordinateur par l'intermédiaire d'un port inactif ou d'un port bloqué par le pare-feu, Norton Internet Security ne vous en avertit pas car il n'y a aucun risque d'intrusion.

Norton Internet Security ne surveille pas les intrusions des ordinateurs figurant dans la zone Approuvés. La Détection d'intrusion analyse néanmoins les informations que vous leur envoyez pour vérifier l'existence de zombies ou d'autres attaques de contrôle à distance.

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Pour détecter et bloquer les activités de réseau douteuses, la Détection d'intrusion s'appuie sur une vaste liste de signatures d'attaque. Veillez à ce que la liste des signatures d'attaque reste à jour en exécutant régulièrement LiveUpdate.

Visual Tracking et le repérage d'attaquants

Se reporter à "Identification de la source de communications" à la page 59.

Norton Internet Security inclut à présent Visual Tracking, qui vous permet d'obtenir des informations sur l'adresse IP à l'origine d'une connexion particulière. Il peut ainsi vous aider à identifier un attaquant.

Activation de Norton Personal Firewall et de la Détection d'intrusion

Le Firewall personnel et la Détection d'intrusion sont automatiquement activés lors de l'installation de Norton Internet Security. Vous n'aurez sans doute pas besoin de modifier de paramètres. Vous pouvez toutefois vous assurer que le pare-feu et la détection d'intrusion sont actifs en procédant comme suit.

Pour vérifier que le Firewall personnel est activé

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Firewall personnel**.
3. Cochez la case **Activer le Firewall personnel** pour activer le Firewall personnel.

Pour vérifier que la Détection d'intrusion est activée

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Cochez l'option **Activer la Détection d'intrusion** pour activer la détection d'intrusion.

Personnalisation de la protection du pare-feu

Les paramètres par défaut du Firewall personnel offrent une protection appropriée à la majorité des utilisateurs. Si la protection par défaut ne convient pas, vous pouvez la personnaliser avec le curseur du niveau de sécurité pour sélectionner des niveaux de sécurité prédéfinis ou modifier des paramètres individuels.

Modification du niveau de sécurité

Le curseur du niveau de sécurité permet de sélectionner un niveau de sécurité Bas, Moyen ou Elevé. Le niveau de protection varie en fonction de la position du curseur. Le curseur n'affecte pas la protection assurée par la Détection d'intrusion.

Se reporter à "A propos des comptes Norton Internet Security" à la page 153.

Vous pouvez définir des paramètres de sécurité individuels pour chaque utilisateur de Norton Internet Security.

Pour modifier le niveau de sécurité

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Personal Firewall**.

3 Dans la fenêtre Personal Firewall, sélectionnez le compte à modifier dans la liste déroulante Choisissez un niveau de sécurité pour.

4 Placez le curseur sur un niveau de sécurité. Les options sont les suivantes :

Elevé	Le pare-feu bloque toute transmission jusqu'à votre autorisation. Si vous avez effectué une Analyse des applications, vous ne devriez pas être interrompu souvent par des alertes du Contrôle des programmes. Se reporter à "Activation du Contrôle des programmes automatique" à la page 114. Un avertissement s'affiche lors de la détection d'un contrôle ActiveX ou d'une applet Java. Les ports inutilisés ne répondent pas aux demandes de connexion. Les ordinateurs externes ne les voient plus.
Moyen (recommandé)	Le pare-feu bloque toute transmission jusqu'à votre autorisation. Si vous avez effectué une Analyse des applications, vous ne devriez pas être interrompu souvent par des alertes du Contrôle des programmes. Les contrôles ActiveX et les applets Java s'exécutent sans avertissement. Les ports inutilisés ne répondent pas aux demandes de connexion. Les ordinateurs externes ne les voient plus.
Bas	Le pare-feu bloque les tentatives de connexion émanant des chevaux de Troie. Les contrôles ActiveX et les applets Java s'exécutent sans avertissement.

Modification de paramètres de sécurité individuels

Si le paramétrage offert par l'option Niveau de sécurité ne vous convient pas, vous pouvez modifier le niveau de protection de Norton Personal Firewall, des *applets Java* et des *contrôles ActiveX*. La modification d'un paramètre individuel remplace le Niveau de sécurité, mais n'a aucun impact sur les autres paramètres de sécurité.

Pour modifier des paramètres de sécurité individuels

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Personal Firewall**.

3 Dans la fenêtre Personal Firewall, sélectionnez le compte à modifier dans la liste déroulante Choisissez un niveau de sécurité pour.

4 Cliquez sur **Niveau personnalisé**.

5 Effectuez une ou plusieurs des opérations suivantes :

- Dans le menu Personal Firewall, sélectionnez un niveau. Les options sont les suivantes :

Maximum	Bloque toutes les communications que vous n'autorisez pas expressément. Vous devez définir des règles de filtrage pour toutes les applications qui nécessitent un accès à Internet.
Moyen	Bloque de nombreux ports utilisés par des applications dangereuses. Cependant, ce réglage peut également bloquer les programmes utiles qui utilisent les mêmes ports.
Aucun	Désactive Norton Personal Firewall et autorise toutes les communications Internet.

- Sélectionnez le niveau de sécurité souhaité pour les applets Java et les contrôles ActiveX. Les options sont les suivantes :

Maximum	Empêche le navigateur d'exécuter des applets Java ou des contrôles ActiveX sur Internet. Cette option est la plus sûre, mais aussi la moins pratique. Certains sites Web risquent de ne pas fonctionner correctement lorsqu'elle est active.
Moyen	Vous interroge en cas de présence d'une applet Java ou d'un contrôle ActiveX. Vous pouvez ainsi, selon les cas, accepter ou bloquer les applets et les contrôles. Il peut être fastidieux d'intervenir chaque fois que vous rencontrez une applet Java ou un contrôle ActiveX, mais cette méthode permet de choisir d'en exécuter certains.
Aucun	Autorise l'exécution de toutes les applets Java et de tous les contrôles ActiveX.

- Pour être averti chaque fois que des programmes inconnus accèdent à Internet, cochez l'option **Activer les alertes de contrôle d'accès**.
- Pour être averti quand un ordinateur distant tente de se connecter à un port inutilisé de votre ordinateur, cochez l'option **Alerter en cas d'accès à des ports inutilisés**.

6 Cliquez sur **OK**.

Réinitialisation des options de sécurité sur les valeurs par défaut

La configuration d'un niveau de sécurité personnalisé désactive le curseur Sécurité. Le curseur indique le niveau de sécurité sur lequel le vôtre est basé, mais vous ne pouvez pas utiliser le curseur pour modifier vos paramètres. Pour utiliser le curseur Sécurité pour choisir l'un des niveaux prédéfinis, vous devez réinitialiser le niveau de sécurité.

Pour réinitialiser les paramètres de sécurité sur les valeurs par défaut

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Personal Firewall**.

3 Dans la fenêtre Personal Firewall, sélectionnez le compte à modifier dans la liste déroulante Choisissez un niveau de sécurité pour.

4 Cliquez sur **Niveau personnalisé**.

Se reporter à "Modification du niveau de sécurité" à la page 107.

Votre niveau de sécurité est réinitialisé sur le niveau moyen. Utilisez le curseur Sécurité pour choisir l'un des autres niveaux de sécurité prédéfinis.

Personnalisation des règles de filtrage

Les règles de filtrage déterminent la façon dont Norton Personal Firewall protège votre ordinateur contre les transmissions entrantes, les applications et les *chevaux de Troie* malveillants. Le pare-feu utilise ces règles pour vérifier automatiquement toutes les données entrantes ou sortantes de votre ordinateur.

Traitement des règles de filtrage

Lorsqu'un ordinateur tente de se connecter à votre ordinateur ou vice versa, Norton Personal Firewall compare le type de *connexion* à la liste des règles de filtrage.

Les règles de filtrage sont traitées dans un ordre défini en fonction de leur type. Les règles système sont traitées d'abord, suivies des règles d'application puis de celles applicables aux chevaux de Troie.

Lorsqu'une règle de blocage ou d'autorisation s'applique, les autres règles ne sont pas prises en compte. Autrement dit, les autres règles pertinentes pour ce type de communication sont ignorées si elles apparaissent à la suite de la première règle applicable.

Imaginons qu'une règle interdise l'utilisation de Symantec pcAnywhere sur l'ordinateur. Si vous ajoutez plus haut dans la liste une règle autorisant l'utilisation de Symantec pcAnywhere avec un ordinateur particulier, la première règle autorise l'emploi de Symantec pcAnywhere avec cet ordinateur et la deuxième bloque son utilisation avec les autres ordinateurs.

Si aucune règle ne correspond, la communication est bloquée. Selon le niveau de rapport demandé, une alerte peut apparaître.

A propos des règles de filtrage par défaut

Diverses règles de filtrage sont prédéfinies et activées à l'installation de Norton Internet Security. Elles assurent les principales fonctionnalités réseau et vous protègent des risques connus sur Internet. Les règles de filtrage par défaut figurent dans les paramètres système et dans ceux concernant les chevaux de Troie. Exemples de règles de filtrage par défaut :

DNS entrant par défaut DNS sortant par défaut	Autorise l'utilisation du système de noms de domaine (DNS).
Bootp entrant par défaut Bootp sortant par défaut	Autorise l'utilisation du service Bootp. Bootp est l'appellation abrégée du protocole bootstrap qui permet à un ordinateur de connaître sa propre adresse IP.
Nom NetBIOS entrant par défaut NetBIOS entrant par défaut NetBIOS sortant par défaut	Contrôle l'utilisation du service de noms NetBIOS et du service de datagrammes NetBIOS servant au partage de fichiers sur les réseaux Microsoft.
Loopback entrant par défaut Boucle sortante par défaut	Autorise les connexions en boucle (loopback) entrantes et sortantes à l'adresse d'hôte local 127.0.0.1. Il est généralement sans danger d'autoriser les connexions locales ou de bouclage dans la mesure où l'origine de la connexion est normalement une application approuvée située sur votre ordinateur. Même si cette règle de filtrage est activée, les ordinateurs distants se voient toujours interdire l'accès à l'adresse de l'hôte local par le réseau sous-jacent.
ICMP entrant par défaut ICMP sortant par défaut	Autorise tous les types de messages ICMP sortants et les types de messages ICMP entrants sans danger. Les messages ICMP fournissent des informations d'état et de contrôle.
Blocage par défaut du cheval de Troie Back Orifice 2000 Blocage par défaut du cheval de Troie NetBus	Vous protège contre les chevaux de Troie connus.

Création de règles de filtrage

Norton Internet Security inclut le Contrôle des programmes, qui crée automatiquement les règles de filtrage au fur et à mesure que vous utilisez Internet.

Se reporter à "A propos des comptes Norton Internet Security" à la page 153.

Les utilisateurs de type Superviseur et Adulte peuvent créer et modifier des règles de filtrage. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier les règles de filtrage.

Vous pouvez créer des règles de filtrage avec le Contrôle des programmes de quatre manières différentes :

Activer le Contrôle automatique des programmes	Configure automatiquement l'accès à Internet des applications connues à leur premier lancement. Il s'agit de la méthode de configuration de règles la plus rapide.
Utiliser l'Analyse des applications	Détecte et configure simultanément toutes les applications Internet d'un ordinateur.
Ajouter manuellement des programmes	Gère avec précision la liste des applications pouvant accéder à Internet.
Répondre aux alertes	Norton Internet Security avertit les utilisateurs lorsqu'une application tente d'accéder à Internet pour la première fois. Les utilisateurs peuvent alors décider d'autoriser l'application à accéder à Internet ou de le lui interdire.

Activation du Contrôle des programmes automatique

Lorsque le Contrôle automatique des programmes est activé, Norton Internet Security crée automatiquement des règles de filtrage la première fois qu'une application connue est exécutée. Le Contrôle automatique des programmes ne configure l'accès à Internet que pour les versions des applications que Symantec a identifiées comme sans danger.

Si une application inconnue ou une version inconnue d'une application connue tente d'accéder à Internet, Norton Internet Security en avertit l'utilisateur. L'utilisateur peut alors décider d'autoriser l'application à accéder à Internet ou de le lui interdire.

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Symantec actualise en permanence la liste des applications reconnues. Exécutez régulièrement LiveUpdate pour tenir à jour votre liste.

Pour activer le Contrôle automatique des programmes

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Personal Firewall**.

3 Dans la fenêtre de Personal Firewall, cliquez sur **Activer le Contrôle automatique des programmes** sur l'onglet Contrôle des programmes.

4 Cliquez sur **OK**.

Recherche des applications utilisant Internet

L'Analyse des applications est la méthode la plus rapide pour configurer le Firewall personnel. Norton Internet Security recherche les applications de l'ordinateur qu'il reconnaît et propose des paramètres appropriés pour chaque application.

Vous pouvez rechercher les programmes accédant à Internet depuis Security Center ou Security Monitor.

Pour rechercher les applications utilisant Internet depuis Security Center

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur **Analyse programme** sur l'onglet Contrôle des programmes.
4. Sélectionnez le ou les disques de l'ordinateur à analyser.
5. Cliquez sur **OK**.
6. Dans la fenêtre Analyse des applications, effectuez l'une des opérations suivantes :
   - Cochez les applications à ajouter à la liste du Contrôle des programmes.
   - Pour ajouter simultanément toutes les applications Internet, cliquez sur **Tout sélect.**.
7. Cliquez sur **Terminer**.
8. Cliquez sur **OK**.

Pour rechercher les applications utilisant Internet depuis Security Monitor

1. Ouvrez Norton Internet Security.
2. Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Exécuter l'analyse des programmes**.
3. Sélectionnez le ou les disques de l'ordinateur à analyser.
4. Cliquez sur **OK**.
5. Dans la fenêtre Analyse des applications, effectuez l'une des opérations suivantes :
   - Cochez les applications à ajouter à la liste du Contrôle des programmes.
   - Pour ajouter simultanément toutes les applications Internet, cliquez sur **Tout sélect.**.
6. Cliquez sur **Terminer**.

Ajout manuel d'un programme au Contrôle des programmes

Se reporter à "Personnalisation de la protection du pare-feu" à la page 107.

Les utilisateurs peuvent ajouter des applications au Contrôle des programmes pour contrôler étroitement leur accès à Internet. Cette opération remplace tout paramétrage effectué par le Contrôle automatique des programmes.

Pour ajouter manuellement un programme au Contrôle des programmes

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur **Ajouter** sur l'onglet Contrôle des programmes.
4. Sélectionnez le fichier exécutable de l'application.
   Le nom des fichiers exécutables se termine généralement par .exe.
5. Cliquez sur **Ouvrir**.
6. Dans l'alerte du Contrôle d'accès à Internet, sélectionnez le niveau d'accès à accorder au programme. Les options sont les suivantes :

Configurer l'accès à Internet automatiquement (recommandé)	Utilise les paramètres de Norton Internet Security par défaut pour l'application.
Autoriser	Autorise toutes les tentatives d'accès de ce programme.
Bloquer	Refuse toutes les tentatives d'accès de ce programme.
Configurer automatiquement l'accès à Internet	Permet de créer des règles contrôlant l'accès à Internet de cette application.

7. Pour évaluer les risques qu'une application peut poser à votre ordinateur, cliquez sur **Détails**.
8. Cliquez sur **OK**.

Modification des paramètres du Contrôle des programmes

Après vous être familiarisé avec Norton Internet Security, vous souhaiterez peut-être modifier les paramètres d'accès des applications. Cette opération remplace tout paramétrage effectué par le Contrôle automatique des programmes.

Pour modifier les paramètres du Contrôle des programmes

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur le programme à modifier sur l'onglet Contrôle des programmes.
4. Cliquez sur **Modifier**.
5. Dans l'alerte du Contrôle d'accès à Internet, sélectionnez le niveau d'accès à accorder au programme. Les options sont les suivantes :

Configurer automatiquement l'accès à Internet	Utilise les paramètres de Norton Internet Security par défaut pour l'application.
Autoriser cette application à accéder à Internet	Autorise toutes les tentatives d'accès de ce programme.
Empêcher cette application d'accéder à Internet	Refuse toutes les tentatives d'accès de ce programme.
Personnaliser l'accès à Internet pour cette application	Permet de créer des règles contrôlant l'accès à Internet de cette application.

6. Cliquez sur **OK**.

Ajout manuel d'une règle de pare-feu

Norton Internet Security crée automatiquement la plupart des règles de filtrage nécessaires, mais vous pouvez être amené à en ajouter en fonction de vos besoins. Ne créez des règles de filtrage que si vous êtes un utilisateur expérimenté d'Internet.

Vous pouvez personnaliser trois ensembles de règles de filtrage :

- Règles générales
- Règles de cheval de Troie
- Règles d'application

Pour ajouter une règle générale

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur **Règles générales** sur l'onglet Avancé.
4. Suivez les instructions affichées à l'écran.
   Se reporter à "Ecriture d'une règle de filtrage" à la page 120.

Pour ajouter une règle de cheval de Troie

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur **Règles cheval de Troie** sur l'onglet Avancé.
4. Suivez les instructions affichées à l'écran.
   Se reporter à "Ecriture d'une règle de filtrage" à la page 120.

Pour ajouter une règle d'application

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal Firewall**.
3. Dans la fenêtre Personal Firewall, cliquez sur **Ajouter** sur l'onglet Contrôle des programmes.

4 Dans la fenêtre Sélection de programme, choisissez le fichier exécutable d'une application.
Le nom des fichiers exécutables se termine généralement par .exe.

5 Dans l'alerte du contrôle d'accès à Internet, sélectionnez **Créer une règle de filtrage** dans le menu Que dois-je faire ?

6 Suivez les instructions affichées à l'écran.
Se reporter à "Ecriture d'une règle de filtrage" à la page 120.

Ecriture d'une règle de filtrage

Norton Internet Security vous guide pour créer vos propres règles de filtrage.

Pour écrire une règle de filtrage

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.

2 Dans la fenêtre Ajouter une règle, sélectionnez l'action souhaitée pour cette règle. Les options sont les suivantes :

Autoriser l'accès à Internet	Autorise les communications du type indiqué.
Bloquer l'accès à Internet	Interdit les communications du type indiqué.
Contrôler à l'accès à Internet	Actualise l'onglet Pare-feu du journal des événements ou affiche un message à chaque communication du type indiqué. Cette opération permet de constater la fréquence d'utilisation de cette règle de filtrage. Pour surveiller une connexion autorisée, vous devez créer à la fois une règle de surveillance et une règle d'autorisation. La règle de surveillance doit précéder la règle d'autorisation.

3 Cliquez sur **Suivant**.

4 Sélectionnez le type de connexion que la règle doit surveiller. Les options sont les suivantes :

Connexions à d'autres ordinateurs	La règle s'applique aux connexions sortantes (de votre ordinateur vers un autre ordinateur).
Connexions en provenance d'autres ordinateurs	La règle s'applique aux connexions entrantes (d'un ordinateur distant vers votre ordinateur).
Connexions à destination et en provenance d'autres ordinateurs	La règle s'applique aux connexions entrantes et sortantes.

5 Cliquez sur **Suivant**.

6 Sélectionnez les ordinateurs que la règle doit surveiller. Les options sont les suivantes :

Ordinateur quelconque	La règle s'applique à tous les ordinateurs.
Uniquement les ordinateurs identifiés ci-dessous	La règle ne s'applique qu'aux ordinateurs, sites et domaines répertoriés.
Adaptateurs	La règle s'applique à un adaptateur réseau particulier de votre ordinateur. Ce paramètre permet de personnaliser des règles de filtrage pour chaque adresse IP de votre ordinateur. Si, par exemple, l'ordinateur est connecté à un réseau personnel et à Internet, vous pouvez définir une règle qui autorise le partage de fichiers au sein du réseau personnel et une autre qui l'interdise sur Internet.

7 Cliquez sur **Suivant**.

8 Sélectionnez les protocoles que la règle doit surveiller. Les options sont les suivantes :

TCP	La règle s'applique aux communications TCP (Transport Control Protocol).
UDP	La règle s'applique aux communications UDP (User Datagram Protocol).

TCP et UDP	La règle s'applique à la fois aux communications TCP et UDP.
ICMP	La règle s'applique aux communications ICMP (Internet Control Message Protocol). Cette option n'est disponible que pour ajouter ou modifier une règle générale.

9 Sélectionnez les ports que la règle doit surveiller. Les options sont les suivantes :

Tous les types de communications (tous les ports)	La règle s'applique aux communications utilisant n'importe quel port.
Uniquement les types de communications ou les ports mentionnés ci-dessous	La règle s'applique aux ports répertoriés. Vous pouvez ajouter des ports à la liste ou en supprimer.

10 Cliquez sur **Suivant**.

11 Choisissez si et comment Norton Internet Security doit suivre cette règle. Les options sont les suivantes :

Pas de suivi de la règle	Aucune trace des actions de la règle n'est conservée.
Créer une entrée de fichier journal	Une entrée est ajoutée au journal des événements du pare-feu lorsqu'un événement de communication réseau correspond à la règle.
Envoyer un message Alert Tracker	Un message Alert Tracker apparaît lorsqu'une communication réseau correspond à la règle.
Afficher une alerte de sécurité	Une boîte de dialogue d'alerte de sécurité apparaît lorsqu'une communication réseau correspond à la règle.

12 Cliquez sur **Suivant**.

13 Dans la zone de texte **Comment voulez-vous appeler cette règle ?** , tapez un nom pour la règle.

14 Dans la zone de texte **A quelle catégorie appartient cette règle ?** , sélectionnez une catégorie.

15 Cliquez sur **Suivant**.

16 Vérifiez les paramètres de la nouvelle règle et cliquez sur **Terminer**.

17 Quand vous avez fini d'ajouter des règles, cliquez sur **OK**.

Modification d'une règle de filtrage existante

Vous pouvez modifier les règles de filtrage qui ne fonctionnent pas comme vous le souhaitez.

Pour modifier une règle de filtrage existante

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.

2 Sélectionnez la règle à modifier.

3 Cliquez sur **Modifier**.

Se reporter à "Ecriture d'une règle de filtrage" à la page 120.

4 Suivez les instructions affichées à l'écran pour modifier la règle.

5 Quand vous avez fini de modifier des règles, cliquez sur **OK**.

Modification de l'ordre des règles de filtrage

Se reporter à "Traitement des règles de filtrage" à la page 112.

Norton Internet Security traite chaque liste de règles de filtrage du début à la fin. Vous pouvez déterminer comment Norton Internet Security traite les règles de filtrage en modifiant l'ordre de celles-ci.

Pour modifier l'ordre d'une règle de filtrage

1 Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, sélectionnez la règle que vous souhaitez déplacer.

2 Effectuez l'une des opérations suivantes :

- Pour que Norton Internet Security traite cette règle avant la règle située au-dessus, cliquez sur **Vers le haut**.
- Pour que Norton Internet Security traite cette règle après la règle située au-dessous, cliquez sur **Vers le bas**.

3 Quand vous avez fini de déplacer des règles, cliquez sur **OK**.

Désactivation temporaire d'une règle de filtrage

Vous pouvez désactiver temporairement une règle de filtrage si vous devez accorder un accès spécifique à un ordinateur ou un programme.

Pour désactiver temporairement une règle de filtrage

- Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, sélectionnez la règle que vous souhaitez désactiver.

Pensez à réactiver la règle quand vous avez fini de travailler avec le programme ou l'ordinateur qui nécessitait la modification.

Suppression d'une règle de filtrage

Supprimez les règles de filtrage dont vous n'avez plus besoin.

Pour supprimer une règle de filtrage

1. Dans la fenêtre Règles générales, Règles de cheval de Troie ou Règles d'application, cliquez sur **Ajouter**.
2. Sélectionnez la règle à supprimer.
3. Cliquez sur **Supprimer**.
4. Quand vous avez fini de supprimer des règles, cliquez sur **OK**.

Réinitialisation des paramètres par défaut des règles de filtrage

La réinitialisation des règles de filtrage ramène la protection par pare-feu de tous les utilisateurs aux paramètres par défaut et supprime toute modification apportée aux règles.

N'utilisez cette procédure qu'en cas d'urgence. Avant de réinitialiser vos règles de filtrage, essayez de supprimer les règles modifiées récemment.

Pour réinitialiser les paramètres par défaut des règles de filtrage

1. Fermez toutes les fenêtres de Norton Internet Security.
2. Dans l'Explorateur Windows, cliquez deux fois sur **Poste de travail**.
3. Cliquez deux fois sur le disque dur sur lequel vous avez installé Norton Internet Security.
   Dans la plupart des cas, il s'agit du disque C.

4 Ouvrez **Program Files** > **Fichiers communs** > **Symantec Shared**.

5 Faites glisser **firewall.rul** sur la Corbeille.

Le pare-feu reviendra à ses paramètres par défaut la prochaine fois que vous exécuterez Norton Internet Security.

Personnalisation de la Détection d'intrusion

Les paramètres par défaut de la Détection d'intrusion offrent une protection appropriée à la majorité des utilisateurs. Vous pouvez personnaliser la Détection d'intrusion, en excluant certaines activités de réseau de la surveillance, en activant ou en désactivant AutoBlock et en limitant les ordinateurs bloqués.

Exclusion d'activités de réseau de la surveillance

Certaines activités de réseau inoffensives peuvent ressembler à des signatures d'attaque Norton Internet Security. Si vous recevez de nombreux avertissements relatifs à des attaques potentielles déclenchés par des comportements inoffensifs, vous pouvez créer une exclusion pour la signature d'attaque correspondante.

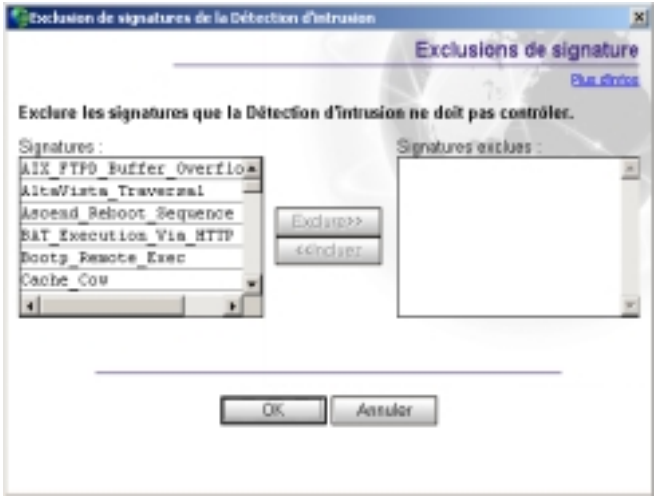
Chaque exclusion rend l'ordinateur un peu plus vulnérable aux attaques. Soyez très sélectif dans votre choix des attaques à exclure. N'excluez que les activités qui sont toujours inoffensives.

Pour exclure des signatures d'attaque de la surveillance

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Signatures**.



4 Dans la liste Signatures, sélectionnez la signature d'attaque à exclure.

5 Cliquez sur **Exclure**.

6 Quand vous avez fini d'exclure des signatures, cliquez sur **OK**.

Si vous avez exclu des signatures d'attaque que vous voulez surveiller de nouveau, vous pouvez les inclure dans la liste de signatures actives.

Pour inclure des signatures d'attaque

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Signatures**.

4 Dans la liste Signatures exclues, sélectionnez la signature d'attaque à surveiller.

5 Cliquez sur **Inclure**.

6 Quand vous avez fini d'inclure des signatures, cliquez sur **OK**.

Activation ou désactivation d'AutoBlock

Lorsque Norton Internet Security détecte une attaque, il bloque automatiquement la *connexion* pour garantir la sécurité de l'ordinateur. Le programme peut également activer la fonction AutoBlock, qui bloque automatiquement toutes les communications entrantes issues de l'ordinateur attaquant pendant une période de temps donnée, même lorsqu'elles ne correspondent pas à une signature d'attaque.

Par défaut, la fonction AutoBlock interrompt toutes les communications émanant de l'ordinateur malveillant pendant 30 minutes.

Pour activer ou désactiver AutoBlock

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, cochez ou décochez la case **Activer AutoBlock**.

Déblocage d'ordinateurs

Dans certains cas, Norton Internet Security peut considérer une activité normale comme une attaque. Si vous ne parvenez pas à communiquer avec un ordinateur avec lequel vous devriez pouvoir le faire, ce dernier figure peut-être sur la liste des ordinateurs actuellement bloqués par AutoBlock.

Si un ordinateur auquel vous voulez accéder apparaît dans la liste des ordinateurs actuellement bloqués par AutoBlock, débloquez-le. Si, à la suite d'une modification des paramètres de protection, vous souhaitez réinitialiser la liste AutoBlock, vous pouvez simultanément lever l'interdiction de tous les ordinateurs de la liste AutoBlock.

Pour débloquer les ordinateurs actuellement bloqués par AutoBlock

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, effectuez l'une des opérations suivantes :
   - Pour débloquer un ordinateur, sélectionnez son adresse IP, puis cliquez sur **Débloquer**.
   - Pour débloquer tous les ordinateurs figurant dans la liste AutoBlock, cliquez sur **Tout débloquer**.

Exclusion d'ordinateurs d'AutoBlock

Si un ordinateur auquel vous voulez accéder est systématiquement placé dans la liste d'AutoBlock, vous pouvez l'exclure du blocage AutoBlock.

Pour exclure certains ordinateurs d'AutoBlock

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la fenêtre Détection d'intrusion, cliquez sur **Adresse IP**.
4. Effectuez l'une des opérations suivantes :
   - Dans la liste Actuellement bloqués, sélectionnez une adresse IP bloquée et cliquez sur **Exclure**.
   - Cliquez sur **Ajouter**, puis tapez le nom de l'ordinateur, son adresse IP, son identification réseau ou une plage d'adresses IP incluant l'ordinateur à exclure.
5. Quand vous avez fini d'exclure des adresses IP, cliquez sur **OK**.

Ajout d'un ordinateur bloqué à la zone Restreints

Vous pouvez ajouter un ordinateur bloqué à la zone Restreints pour l'empêcher en permanence d'accéder à votre ordinateur. Les ordinateurs ajoutés à la zone Restreints ne figurent pas dans la liste des ordinateurs bloqués car Norton Internet Security rejette automatiquement toutes les *tentatives de connexion* qu'ils effectuent.

Pour ajouter un ordinateur bloqué à la zone Restreints

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.
3. Dans la liste des ordinateurs actuellement bloqués par AutoBlock, sélectionnez celui à ajouter à la liste Restreints.
4. Cliquez sur **Restreindre**.
5. Quand vous avez fini de restreindre des ordinateurs, cliquez sur **OK**.

Protection antivirus des disques, des fichiers et des données

8

La protection de votre ordinateur requiert la surveillance régulière par Auto-Protect, le blocage de script et le blocage de vers, l'analyse des pièces jointes aux *e-mails* et des fichiers transférés par la messagerie instantanée, ainsi que des analyses de système fréquentes. Vous pouvez configurer toutes ces tâches pour qu'elles soient effectuées automatiquement.

Pour bénéficier d'une protection Norton AntiVirus supplémentaire sous Windows 98/98SE/Me, activez l'inoculation pour qu'elle vous *alerte* si un fichier système est modifié.

Assurez-vous que les paramètres de protection sont activés

Norton Internet Security est configuré pour assurer une protection antivirus complète. Vous n'aurez sans doute pas besoin de modifier de paramètres. Cependant, pour bénéficier d'un maximum de protection, vous devez vous assurer que les fonctionnalités de protection sont activées.

Fonction	Comment régler	Réglage de protection maximale
Protection automatique	**Fenêtre principale de Norton AntiVirus > Activer** Se reporter à "A propos des options système" à la page 67.	Auto-Protect est mis sur **Activé**.
Analyse des e-mails	**Options > E-mail** Se reporter à "A propos des options Internet" à la page 69.	Cocher les options **Analyser les e-mails entrants** et **Analyser les e-mails sortants**. Si le programme d'e-mail utilise l'un des protocoles de communication pris en charge, les deux options sont sélectionnées par défaut.
Protection contre l'expiration du délai	**Options> E-mail** Se reporter à "A propos des options Internet" à la page 69.	Activer l'option **Protéger contre les délais dépassés pendant l'analyse des messages**. Pour éviter l'expiration du délai de connexion lors de la réception de pièces jointes de grande taille, activez l'option de protection contre l'expiration du délai.
Analyse de la messagerie instantanée	**Options>Messagerie instantanée** Se reporter à "A propos des options Internet" à la page 69.	Les MI que vous voulez protéger sont cochés.

Blocage des vers	**Options > E-mail** Se reporter à "A propos des options Internet" à la page 69.	Les options **Activer le blocage des vers** et **M'alerter lors de l'analyse des pièces jointes aux e-mails** sont activées.
Blocage de scripts	**Options > Blocage des scripts** Se reporter à "A propos des options système" à la page 67.	L'option **Activer le blocage des scripts** est activée.
Inoculation	**Options > Inoculation** Se reporter à "A propos des autres options" à la page 70.	L'option **Inoculer les zones amorce** est cochée.

Ce tableau résume les paramètres de protection maximale et leur emplacement. Pour plus d'informations sur une option particulière, reportez-vous à l'aide en ligne.

Analyse manuelle de disques, de dossiers et de fichiers

Si Auto-Protect est activé et les options de Norton AntiVirus à leurs niveaux par défaut, vous ne devez pas normalement procéder à une analyse manuelle. Cependant, si vous avez désactivé temporairement Auto-Protect (par exemple, pour charger ou utiliser un autre programme qui crée un conflit avec Norton AntiVirus) et si vous avez oublié de le réactiver, il est possible qu'un virus se soit logé sur votre disque dur sans être détecté. Vous pouvez analyser tout votre ordinateur, ou des disquettes individuelles, des lecteurs, des dossiers ou des fichiers.

Bien que les paramètres par défaut pour analyse manuelle soient habituellement appropriés, vous pouvez élever le niveau des heuristiques de Bloodhound ou ajuster les options d'analyse manuelle dans la fenêtre Options. Vérifiez l'aide en ligne pour y trouver des informations supplémentaires sur les options d'analyse manuelle.

Exécution d'une analyse complète du système

Une analyse complète du système comprend l'analyse de toutes les *zones amorce* et de tous les fichiers de l'ordinateur.

Pour effectuer une analyse complète du système

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse antivirus**.
3. Dans le volet Analyse antivirus, cliquez sur **Analyser mon ordinateur**.
4. Dans la zone Actions, cliquez sur **Analyser**.
   Lorsque l'analyse est terminée, un résumé apparaît.
5. Quand vous avez passé ce résumé en revue, cliquez sur **Terminé**.

Analyse d'éléments distincts

Occasionnellement, vous pouvez choisir d'analyser un fichier particulier, tous les supports amovibles, une disquette, tous les disques, tous les dossiers ou tous les fichiers de l'ordinateur. Il se peut que vous ayez travaillé avec des disquettes ou reçu un fichier comprimé dans un e-mail et que vous redoutiez la présence d'un virus. Vous pouvez analyser un disque particulier ou un élément individuel que vous voulez vérifier.

Pour analyser des éléments distincts

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.
3. Dans le volet Analyse antivirus, cliquez sur l'analyse à exécuter.
4. Dans la zone Actions, cliquez sur **Analyser**.
   Si vous choisissez d'analyser tous les supports amovibles ou une disquette, l'analyse démarre automatiquement. Si vous choisissez d'analyser des disques, des dossiers ou des fichiers, une boîte de dialogue apparaît et vous permet de sélectionnez les disques, les dossiers ou les fichiers à analyser.
5. Dans la boîte de dialogue, cliquez sur **Analyser** après avoir choisi les options voulues.
   Lorsque l'analyse est terminée, un résumé apparaît.
6. Quand vous avez passé ce résumé en revue, cliquez sur **Terminé**.

En cas de problèmes lors d'une analyse

Se reporter à "Si un virus est détecté lors d'une analyse" à la page 140.

En fin d'analyse, un rapport récapitulatif répertorie les éléments détectés par Norton Internet Security en cours d'analyse. Si un virus a été trouvé et si vous avez demandé que Norton Internet Security répare automatiquement le fichier, ce dernier est répertorié dans la liste des fichiers réparés. Si le fichier ne peut pas être réparé, il peut être mis en quarantaine ou supprimé.

Création et utilisation d'analyses personnalisées

Se reporter à "Programmation d'une analyse personnalisée" à la page 135.

Vous pouvez créer une analyse personnalisée si vous analysez régulièrement une section particulière de l'ordinateur et si vous souhaitez éviter d'indiquer chaque fois la section à analyser. Vous pouvez également programmer l'analyse personnalisée pour qu'elle soit exécutée automatiquement.

Vous pouvez supprimer l'analyse lorsqu'elle n'est plus nécessaire. Par exemple, si vous travaillez sur un projet pour lequel vous avez besoin de fréquemment échanger des fichiers avec d'autres utilisateurs, vous pouvez être amené à créer un dossier où vous copiez et analysez ces fichiers avant de les utiliser. Lorsque le projet est terminé, vous pouvez supprimer l'analyse personnalisée correspondant à ce dossier.

Pour créer une analyse personnalisée

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.
3. Dans le volet Analyse antivirus, dans la zone Actions, cliquez sur **Nouveau**.
4. Dans la fenêtre d'accueil de l'Assistant d'analyse Norton AntiVirus, cliquez sur **Suivant**.
5. Effectuez une ou plusieurs des opérations suivantes :
   - Pour sélectionner des fichiers particuliers à analyser, cliquez sur **Ajouter fichiers**.
   - Pour sélectionner les dossiers ou les lecteurs à analyser, cliquez sur **Ajouter dossiers**.

   Vous pouvez combiner ces deux options pour sélectionner les éléments voulus.

6 Choisissez les éléments à analyser dans la boîte de dialogue qui apparaît.
Si vous sélectionnez un dossier, tous les fichiers qu'il contient sont pris en compte. Si vous sélectionnez un disque, tous les dossiers qu'il contient sont pris en compte.

7 Ajoutez les éléments sélectionnés à la liste des éléments à analyser, en effectuant l'une des opérations suivantes :
- Dans la boîte de dialogue Analyser fichiers, cliquez sur **Ouvrir**.
- Dans la boîte de dialogue Analyse de dossiers, cliquez sur **Ajouter**.

8 Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur **Supprimer**.

9 Lorsque la liste des éléments à analyser est créée, cliquez sur **Suivant**.

10 Entrez un nom permettant d'identifier cette analyse dans la liste.

11 Cliquez sur **Terminer**.

Exécution d'une analyse personnalisée

Lors de l'exécution d'une analyse personnalisée, vous n'avez pas besoin de redéfinir les éléments à analyser.

Pour exécuter une analyse personnalisée

1 Démarrez Norton Internet Security.

2 Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.

3 Dans le volet Analyse antivirus, cliquez sur l'analyse personnalisée.

4 Dans la zone Actions, cliquez sur **Analyser**.
Lorsque l'analyse est terminée, un résumé apparaît.

5 Quand vous avez passé ce résumé en revue, cliquez sur **Terminé**.

Suppression d'une analyse personnalisée

Les analyses personnalisées peuvent être supprimées dès qu'elles ne sont plus nécessaires.

Pour supprimer une analyse personnalisée

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.
3. Dans le volet Analyse antivirus, cliquez sur l'analyse à supprimer.

Si vous cliquez sur le bouton à côté du nom de l'analyse, cette dernière est exécutée.

4. Dans la zone Actions, cliquez sur **Supprimer**.
5. Cliquez sur **Oui** pour confirmer la suppression de l'analyse.

Planification d'analyses antivirus

Après l'installation, Norton AntiVirus exécute automatiquement une analyse système complète hebdomadaire. Vous pouvez également programmer des analyses antivirus personnalisées.

Vous pouvez programmer des analyses antivirus personnalisées qui s'exécuteront automatiquement à des dates et heures précises ou à intervalles réguliers. Si vous utilisez l'ordinateur quand l'analyse programmée commence, celle-ci s'exécute en arrière-plan pour ne pas interférer avec votre travail.

Vous ne pouvez pas programmer les analyses prédéfinies dans la liste d'analyse, mais vous pouvez programmer toutes les analyses personnalisées que vous avez créées.

Programmation d'une analyse personnalisée

Vous êtes entièrement libre de votre choix dans la programmation d'analyses personnalisées. Lorsque vous sélectionnez la fréquence d'exécution d'une analyse (par exemple, journalière, hebdomadaire ou mensuelle), des zones de texte sont à votre disposition pour affiner votre requête. Vous pouvez, par exemple, demander une analyse journalière, puis programmer cette analyse pour qu'elle soit exécutée plutôt tous les deux ou trois jours.

Pour programmer une analyse

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.
3. Dans le volet Analyse antivirus, cliquez sur l'analyse à programmer.

Si vous cliquez sur le bouton à côté du nom de l'analyse, cette dernière est exécutée.

4. Sous Programmation des tâches, cliquez sur **Programmer**.
5. Dans la boîte de dialogue de programmation, si l'option Afficher les différents horaires est activée, cliquez sur **Nouveau** pour activer les champs de programmation.
   Si l'option n'est pas cochée, les champs sont déjà activés.
6. Configurez la fréquence et l'heure auxquelles l'analyse doit être exécutée.
   La plupart des options de fréquence comprennent elles-mêmes des options permettant de préciser la programmation. Configurez des options supplémentaires selon les besoins.
7. Une fois que vous avez terminé, cliquez sur **OK**.

Vous pouvez également créer des programmations multiples pour une même analyse. Par exemple, vous pouvez exécuter la même analyse au début et à la fin de votre journée de travail.

Pour créer plusieurs programmations pour une même analyse

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.
3. Dans le volet Analyse antivirus, cliquez sur l'analyse à programmer.

Si vous cliquez sur le bouton à côté du nom de l'analyse, cette dernière est exécutée.

4. Sous Programmation des tâches, cliquez sur **Programmer**.
5. Dans la boîte de dialogue de planification, cochez la case **Afficher les différents horaires**.

6 Pour définir une autre programmation, cliquez sur **Nouveau**.

7 Configurez la fréquence et l'heure auxquelles l'analyse doit être exécutée.
La plupart des options de fréquence comprennent elles-mêmes des options permettant de préciser la programmation. Configurez des options supplémentaires selon les besoins.

8 Une fois que vous avez terminé, cliquez sur **OK**.

Modification d'analyses programmées

Vous pouvez modifier la programmation d'une analyse programmée, y compris l'analyse hebdomadaire complète du système.

Pour modifier une analyse programmée

1 Démarrez Norton Internet Security.

2 Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.

3 Dans le volet Analyse antivirus, cliquez sur l'analyse à programmer.

Si vous cliquez sur le bouton à côté du nom de l'analyse, cette dernière est exécutée.

4 Sous Programmation des tâches, cliquez sur **Programmer**.

5 Modifiez la programmation selon vos besoins.

6 Cliquez sur **OK**.

Suppression d'une programmation d'analyse

Vous pouvez supprimer la programmation d'analyse de votre choix. La suppression de la programmation ne supprime pas l'analyse.

Pour supprimer une programmation d'analyse

1 Démarrez Norton Internet Security.

2 Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus** > **Analyse AntiVirus**.

3 Dans le volet Analyse antivirus, cliquez sur l'analyse à programmer.

Si vous cliquez sur le bouton à côté du nom de l'analyse, cette dernière est exécutée.

4 Sous Programmation des tâches, cliquez sur **Programmer**.

5 Dans la boîte de dialogue de planification, cochez la case **Afficher les différents horaires**.

6 Sélectionnez la programmation à supprimer (s'il en existe plusieurs).

7 Cliquez sur **Supprimer**.

8 Cliquez sur **OK**.

Comment procéder en cas d'infection

9

Si Norton AntiVirus trouve un virus sur l'ordinateur, vous disposez de trois solutions pour résoudre le problème :

- Réparer le fichier
  Elimine le *virus* du fichier ou, si la *menace* est un ver ou un cheval de Troie, supprime le fichier.
- Mettre le fichier en quarantaine
  Rend le fichier inaccessible à tout programme autre que Norton AntiVirus. Vous ne pouvez pas ouvrir ce fichier accidentellement et propager le virus, mais vous pouvez toujours l'analyser et voir s'il doit être soumis à Symantec.
- Supprimer le fichier
  Elimine le virus, le ver ou le cheval de Troie de l'ordinateur en supprimant le fichier qui le contient. Cette option ne doit être utilisée que si le fichier est irréparable ou impossible à mettre en quarantaine.

Se reporter à "Si des fichiers sont en quarantaine" à la page 145.

Des *menaces* peuvent être trouvées au cours d'une analyse manuelle ou d'une analyse programmée, ou encore effectuée par Auto-Protect lorsque vous manipulez un *fichier infecté*. Des menaces peuvent également apparaître au cours d'une session de messagerie instantanée ou lors de l'envoi d'un e-mail. La façon de réagir à une menace dépend de la méthode employée pour la détecter.

Si un virus est détecté lors d'une analyse

Si Norton Internet Security détecte un virus, un cheval de Troie ou un ver au cours d'une analyse ou à l'occasion d'une session de messagerie instantanée, vous recevrez un résumé des résultats de réparation ou de la suppression automatique, ou vous devrez utiliser l'Assistant de réparation pour résoudre le problème.

Consultation des détails de réparation

Si vous avez configuré les options d'analyse manuelle afin que Norton AntiVirus répare automatiquement les fichiers et si tous les fichiers infectés ont pu être réparés, le résumé de l'analyse répertorie le nombre de fichiers infectés et réparés. Ces informations ne sont fournies qu'à titre indicatif ; vous n'avez pas besoin de prendre d'autres mesures pour protéger l'ordinateur. Pour en savoir plus, vous pouvez consulter les détails de réparation pour connaître les fichiers infectés et le nom du virus.

Pour consulter les détails de réparation

1. Dans le volet Résumé de la fenêtre de l'analyseur, cliquez sur **Autres détails**.
2. Quand vous avez fini de consulter les résultats, cliquez sur **Terminé**.

Utilisation de l'Assistant de réparation

Si certains fichiers sont irréparables ou si vous avez configuré les options d'analyse manuelle afin que Norton AntiVirus vous demande ce qu'il doit faire lorsqu'il détecte un virus, l'Assistant de réparation apparaît. Si Norton AntiVirus n'a tenté aucune réparation, l'Assistant de réparation apparaît en présentant son volet Réparer. Sinon, il est ouvert sur le volet Quarantaine.

Pour utiliser l'Assistant de réparation

1. Si l'Assistant de réparation apparaît sur le volet Réparer, désélectionnez tous les fichiers que Norton AntiVirus ne doit pas réparer.
   Par défaut, tous les fichiers sont sélectionnés. Il s'agit de l'action recommandée.

2 Cliquez sur **Fichiers**.
Si certains fichiers ne peuvent pas être réparés ou supprimés, le volet Quarantaine apparaît.
Par défaut, tous les fichiers sont sélectionnés afin d'être mis en quarantaine. Il s'agit de l'action recommandée.

3 Dans le volet Quarantaine, désélectionnez tous les fichiers à ne pas mettre en quarantaine.

4 Cliquez sur **Quarantaine**.
Si certains fichiers ne peuvent pas être mis en quarantaine, le volet Supprimer apparaît.
Si vous ne supprimez pas les fichiers infectés, le virus reste sur l'ordinateur, et peut occasionner des dégâts ou être transmis à d'autres utilisateurs.

5 Désélectionnez tous les fichiers à supprimer.

6 Cliquez sur **Supprimer**.
Une fois tous les fichiers réparés, mis en quarantaine ou supprimés, le volet Résumé de la fenêtre de l'analyseur apparaît.

7 Quand vous avez passé ce résumé en revue, cliquez sur **Terminé**.

Après la réparation d'un virus sur le secteur d'amorçage du disque dur, redémarrez l'ordinateur.

Si le virus a été détecté par Auto-Protect

Auto-Protect analyse les fichiers pour détecter des virus et d'autres *codes* malveillants lorsque vous exécutez certaines opérations, comme le déplacement, la copie ou l'ouverture de ces fichiers. Si Auto-Protect détecte un virus ou une activité suspecte, dans la plupart des cas, une *alerte* vous signale qu'un virus a été détecté et que le fichier a été réparé. La façon de procéder ensuite dépend du système d'*exploitation* que vous utilisez.

Si vous utilisez Windows 98/98SE/Me

Si un virus ou une menace est détecté et réparé par Auto-Protect sous Windows 98/98SE/Me, une alerte vous indique le nom du fichier réparé ou supprimé.

Pour fermer le message d'alerte

❖ Cliquez sur **Terminer**.

Si vous avez configuré les options de telle sorte qu'Auto-Protect vous demande ce qu'il doit faire lorsqu'il a détecté un virus, le message d'alerte vous demande de choisir une action. L'action recommandée est toujours présélectionnée.

Bouton	Résultat
Réparer le fichier infecté	Elimine automatiquement le virus, le cheval de Troie ou le ver et répare ou supprime le fichier infecté. Quand un virus est détecté, l'option de réparation est toujours le meilleur choix.
Mettre en quarantaine le fichier infecté	Isole le fichier infecté mais ne supprime pas la menace. Sélectionnez Mettre en quarantaine si vous pensez que l'infection est due à une menace inconnue et que vous vouliez la transmettre à Symantec pour analyse.
Supprimer le fichier infecté	Supprime à la fois la menace et le fichier infecté. Sélectionnez Supprimer si la réparation échoue. Remplacez le fichier supprimé par le fichier programme d'origine ou par la copie de sauvegarde. Si le virus, le cheval de Troie ou le ver est à nouveau détecté, la copie d'origine est infectée.
Ne pas ouvrir le fichier mais ne pas traiter le problème	Interrompt l'opération en cours pour vous éviter d'utiliser un fichier infecté. Cette action ne résout pas le problème. Un message d'alerte apparaîtra lors de la prochaine exécution de la même activité.
Ignorer le problème et ne plus analyser ce fichier à l'avenir	Ajoute le fichier suspect à la liste d'exclusions. Lorsque vous ajoutez un fichier à la liste d'exclusions, ce fichier est exclu de toutes les analyses antivirus suivantes, jusqu'à ce que vous le supprimiez de la liste. Sélectionnez cette option uniquement si vous savez que le fichier est sain.
Ignorer le problème et continuer avec le fichier infecté	Poursuit l'opération en cours. Sélectionnez cette option uniquement si vous êtes sûr qu'aucun virus, cheval de Troie ni ver n'est actif. Vous recevrez à nouveau une alerte. Si vous n'êtes pas sûr de l'action à effectuer, sélectionnez Ne pas ouvrir le fichier mais ne pas traiter le problème.

Si le fichier ne peut pas être réparé, un message d'alerte vous signale que la réparation n'a pas été effectuée et vous recommande de mettre le fichier en quarantaine. Vous disposez alors des mêmes options que celles répertoriées dans le tableau, à l'exception de Réparer le fichier infecté.

Si vous utilisez Windows 2000/XP

Si une *menace* est détectée et réparée par Auto-Protect sous Windows 2000 ou Windows XP, une alerte vous indique le nom du fichier réparé et celui du virus, du cheval de Troie ou du ver qui infectait le fichier. Si vous disposez d'une connexion Internet active, cliquez sur le nom du virus pour accéder à la page Web Symantec contenant la description de ce virus.

Pour fermer le message d'alerte

❖ Cliquez sur **OK**.

Si le fichier ne peut pas être réparé, deux alertes sont générées, l'une indiquant qu'Auto-Protect n'a pas pu réparer le fichier et l'autre signalant que l'accès au fichier a été refusé.

Se reporter à "Si des fichiers sont en quarantaine" à la page 145.

Vous pouvez configurer les options d'Auto-Protect pour tenter de mettre en quarantaine tous les fichiers infectés qu'il ne peut pas réparer. Ainsi, vous serez informé de toute mise en quarantaine de fichiers.

Pour résoudre les problèmes des fichiers non réparés

Se reporter à "Exécution d'une analyse complète du système" à la page 132.

1 Exécutez une analyse système complète de l'ordinateur pour vous assurer qu'aucun autre fichier n'est infecté.

Se reporter à "Si un virus est détecté lors d'une analyse" à la page 140.

2 Effectuez les opérations recommandées par l'Assistant de réparation pour protéger l'ordinateur des fichiers infectés.

Si le virus a été détecté par le blocage de script

Se reporter à "Assurez-vous que les paramètres de protection sont activés" à la page 130.

Le blocage de script analyse les scripts Visual Basic et JavaScript pour y détecter des virus. S'il détecte un virus ou une activité suspecte, dans la plupart des cas, une alerte vous signale qu'une *menace* menace a été détectée.

Vous devez choisir une des options pour supprimer la menace. L'action recommandée est d'arrêter l'exécution du script. Vous pouvez cliquer sur Aide ou sur Alerte pour obtenir plus d'informations sur la réponse à apporter.

Si une menace a été détectée par le blocage de vers

Se reporter à "Assurez-vous que les paramètres de protection sont activés" à la page 130.

Si le programme essaie de se propager par e-mail ou d'expédier par e-mail une copie de son code, il pourrait s'agir d'un ver cherchant à se répandre par la messagerie électronique. Un ver est en mesure de s'envoyer lui-même dans un e-mail sans aucune intervention de votre part.

Le blocage de vers analyse en permanence les pièces jointes aux e-mails sortants pour y détecter des *vers*. S'il détecte un ver, une alerte vous signale sa présence.

L'alerte vous propose un choix d'options et vous demande ce qu'il faut faire. Si vous n'étiez pas occupé à envoyer un e-mail à ce moment, il s'agit probablement d'un ver et vous devez mettre le fichier en quarantaine. Vous pouvez cliquer sur Aide ou sur Alerte pour obtenir plus d'informations sur la réponse à apporter.

Après que vous ayez répondu à la *menace* et supprimé le fichier, votre système risque encore d'être infecté. Exécutez LiveUpdate, analysez votre système et, si nécessaire, consultez la page Web Symantec security response (securityresponse.symantec.com) pour télécharger les derniers outils de définitions de virus.

Si l'inoculation signale une modification des fichiers système

L'inoculation est uniquement disponible sous Windows98/98SE/Me.

Se reporter à "Assurez-vous que les paramètres de protection sont activés" à la page 130.

Les fichiers systèmes peuvent changer pour plusieurs raisons. Il est possible que vous ayez mis à jour votre *système d'exploitation*, que vous ayez repartitionné votre disque dur, ou que votre ordinateur ait été contaminé par un virus. Norton AntiVirus vous avertit lorsqu'une modification des fichiers système se produit.

Si vous recevez une *alerte* au sujet d'une modification des fichiers système, vous avez deux options. Vous pouvez soit mettre à jour votre cliché d'inoculation, soit réparer le fichier. Avant de réparer le fichier, assurez-vous que vos définitions de virus soient à jour et lancez une analyse.

Réponse aux modifications d'inoculation

❖ Dans la fenêtre Alerte, cliquez sur le bouton de l'action à exécuter. Les options disponibles sont les suivantes :

Mettre à jour la copie sauvegardée de mon enregistrement principal d'amorce	Choisissez cette option si l'alerte se produit après une modification légitime de vos fichiers système.
Restaurer mon enregistrement principal d'amorce	Choisissez cette option si vous êtes certain que le système n'a pas été modifié pour des raisons légitimes.

Si des fichiers sont en quarantaine

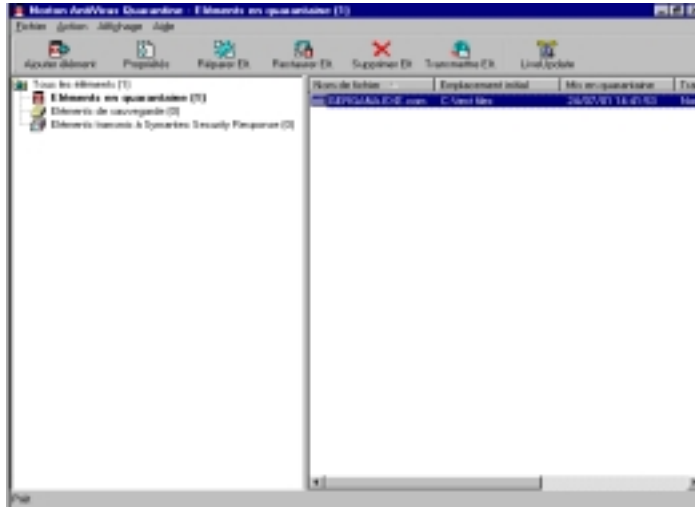
Une fois un fichier mis en quarantaine, vous disposez de plusieurs solutions. Toutes les actions effectuées sur les fichiers en quarantaine doivent être exécutées à partir de la fenêtre Quarantaine.

Pour ouvrir la fenêtre Quarantaine

1 Démarrez Norton Internet Security.

2 Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus > Rapports**.

3 Dans le volet Rapports, sur la ligne Eléments en quarantaine, cliquez sur **Afficher un rapport**.



La barre d'outils en haut de la fenêtre Quarantaine contient toutes les commandes qui peuvent être appliquées aux fichiers en quarantaine.

Ajouter élément	Ajoute des fichiers à la zone de quarantaine. Utilisez cette action pour mettre en quarantaine un fichier suspect. Elle n'a aucun effet sur les fichiers déjà en quarantaine.
Propriétés	Fournit des informations détaillées sur le fichier sélectionné et sur le virus qui l'infecte.
Réparer élément	Tente de réparer le fichier sélectionné. Utilisez cette action si vous avez reçu de nouvelles définitions de virus depuis la mise en quarantaine du fichier.
Restaurer élément	Restaure le fichier sélectionné à son emplacement d'origine, sans le réparer.
Supprimer élément	Supprime le fichier sélectionné de l'ordinateur.
Transmettre élément	Envoie le fichier sélectionné à Symantec. Choisissez cette option si vous pensez qu'un fichier a été infecté même si Norton Antivirus ne l'a pas détecté.
LiveUpdate	Exécute LiveUpdate pour rechercher les nouvelles mises à jour de la protection antivirus et des programmes. Utilisez cette action si vous n'avez pas mis à jour vos définitions de virus récemment et si vous souhaitez tenter de réparer les fichiers en quarantaine.

Pour exécuter une opération sur un fichier en quarantaine

1. Sélectionnez le fichier à traiter.
2. Dans la barre d'outils, cliquez sur le bouton de l'action à exécuter.
3. Quand vous avez terminé, accédez au menu Fichier et cliquez sur **Quitter**.

Si Norton AntiVirus ne peut pas réparer un fichier

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

L'une des raisons les plus courantes pour lesquelles Norton AntiVirus ne peut pas réparer ou supprimer un fichier automatiquement est que vous ne disposez pas de la dernière protection antivirus. Mettez à jour la protection antivirus avec LiveUpdate, puis lancez une nouvelle analyse.

Si cela ne fonctionne pas, consultez les informations de la fenêtre de rapport pour savoir quels types d'éléments ne peuvent pas être réparés, puis effectuez l'action suivante.

Type de fichier	Bouton
Les fichiers infectés ayant une extension .exe, .doc ou .xls (n'importe quel fichier peut être infecté).	Utilisez l'Assistant de réparation pour résoudre le problème. Se reporter à "Utilisation de l'Assistant de réparation" à la page 140.
Enregistrement de zone amorce sur le disque dur maître ou sur un autre disque, fichiers système (comme IO.SYS ou MSDOS.SYS) et enregistrements de zone amorce et fichiers système sur disquette.	Remplacez-les à l'aide des disques de sauvetage ou des disques d'installation du système d'exploitation. Se reporter à "A propos des disquettes de sauvetage" à la page 75.

Si l'ordinateur ne démarre pas correctement

Se reporter à "A propos des disquettes de sauvetage" à la page 75. Se reporter à "Création de disquettes d'urgence" à la page 30.

Si un virus infecte l'ordinateur et si vous avez besoin de démarrer à partir d'un disque sain pour supprimer ce virus, ou si vous avez besoin de restaurer une zone amorce, utilisez vos disques de sauvetage. Si vous n'avez pas de disques de sauvetage, vous pouvez utiliser vos disquettes d'urgence pour démarrer l'ordinateur et supprimer le virus. Si vous avez besoin de restaurer des zones amorce et que vous n'ayez pas de disques de sauvetage, ou si vous avez besoin de restaurer des fichiers système, vous devez réinstaller Windows.

Si vous devez utiliser les disques de sauvetage (Windows 98/98SE/Me)

Parfois, l'infection empêche l'ordinateur de démarrer normalement. Certains virus ne peuvent être supprimés que si l'ordinateur démarre à partir d'une disquette nettoyée, et non depuis le disque dur infecté. La plupart du temps, une alerte Norton AntiVirus vous indique le moment où vous devez utiliser les disquettes de secours.

Vous devez d'abord déterminer si vos disques de sauvetage sont à jour. Vous devez avoir créé ou mis à jour les disquettes de secours après avoir effectué l'une des opérations suivantes :

- Ajout, modification ou retrait d'un composant matériel interne
- ajout, modification ou suppression de partitions de disque dur
- mise à niveau du système d'exploitation
- mise à jour des définitions de virus

Si vos disques de sauvetage ne sont pas à jour, vous pouvez quand même les utiliser pour supprimer les virus de votre ordinateur. Lorsque la fenêtre Rescue Disk s'affiche, n'utilisez que la tâche Norton AntiVirus.

Pour utiliser les disques de sauvetage

1. Insérez la disquette d'amorçage de base dans le lecteur A et redémarrez l'ordinateur.
   Le programme Rescue fonctionne sous DOS.
2. Utilisez les touches fléchées pour sélectionner le programme à exécuter.
   Une description du programme sélectionné apparaît dans le volet de droite du programme Rescue. Les options disponibles sont les suivantes :

Norton AntiVirus	recherche les virus sur l'ordinateur et répare tout fichier infecté.
Récupération Rescue	vérifie et restaure les informations d'amorce et de partition.

3. Appuyez sur **Entrée** pour exécuter le programme sélectionné.
4. Suivez les invites affichées pour insérer les disques de sauvetage dans le lecteur et les en retirer.
5. Lorsque la procédure est terminée, retirez le disque de sauvetage du lecteur A et redémarrez l'ordinateur.

Si vous avez besoin d'utiliser des disquettes d'urgence

Se reporter à "Création de disquettes d'urgence" à la page 30.

Si vous n'avez pas créé de disques de sauvetage, vous pouvez utiliser les disquettes d'urgence pour démarrer l'ordinateur et rechercher les virus.

Pour utiliser des disquettes d'urgence

1. Insérez la disquette d'urgence 1 dans le lecteur A et redémarrez l'ordinateur.
   Le programme Emergency fonctionne sous DOS.
2. Vérifiez que l'option Antivirus est sélectionnée et appuyez sur **Entrée** pour lancer le programme d'urgence Norton AntiVirus.
3. Suivez les invites affichées pour insérer les disquettes d'urgence dans le lecteur et les en retirer.
   Le programme Emergency recherche automatiquement les virus sur l'ordinateur.
4. Lorsque la procédure est terminée, retirez la disquette d'urgence du lecteur A et redémarrez l'ordinateur.

Si vous utilisez le CD comme disquette d'urgence

Se reporter à "Impossible de démarrer depuis le lecteur A" à la page 228.

Si vous utilisez le CD-ROM Norton Internet Security au lieu d'une disquette d'urgence, ne tenez pas compte des instructions sur le changement de disquette. Toutes les informations nécessaires sont disponibles sur le CD-ROM.

Vous devrez peut-être modifier les données de configuration du BIOS de l'ordinateur pour qu'il démarre depuis le lecteur de CD-ROM.

Pour utiliser le CD-ROM comme disque d'urgence

1. Insérez le CD-ROM Norton Internet Security dans le lecteur.
2. Redémarrez votre ordinateur.
   Le programme Emergency recherche automatiquement les virus sur l'ordinateur.

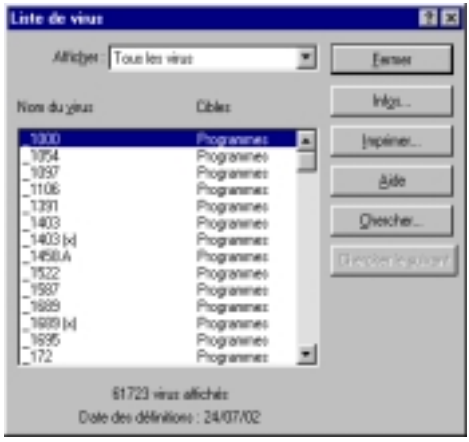
Recherche de virus sur le site Web de Symantec

Le site Web de Symantec comprend la liste exhaustive de tous les virus et codes malveillants connus, avec leur description. Pour la consulter, vous devez vous connecter à Internet.

Pour rechercher des virus

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale, cliquez sur **Norton AntiVirus**.
3. Dans le volet Rapports, sur la ligne correspondant au dictionnaire de virus en ligne, cliquez sur **Afficher un rapport**.
   Votre navigateur Internet démarre et accède au site Web de Symantec.
4. Utilisez les liens de la page Web pour accéder aux informations sur le virus recherché.

Rechercher des virus dans Norton AntiVirus



Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Pour obtenir les dernières définitions de virus, exécutez LiveUpdate.

Pour rechercher des noms et des définitions de virus

1. Démarrez Norton Internet Security.
2. Dans la fenêtre principale de Norton AntiVirus, cliquez sur **Norton AntiVirus > Rapports**.
3. Dans le volet Rapports, sur la ligne Liste des virus, cliquez sur **Afficher un rapport**.

Pour obtenir des informations supplémentaires sur un virus

1. Dans la boîte de dialogue Liste des virus, sélectionnez le virus sur lequel vous souhaitez obtenir des informations.
2. Cliquez sur **Infos**.
3. Quand vous avez fini de lire la liste, cliquez sur **Fermer** dans la boîte de dialogue Liste des virus.

Création de comptes pour utilisateurs multiples

10

Si vous avez choisi d'installer la fonction Comptes de Norton Internet Security, vous pouvez créer des paramètres de sécurité personnalisés pour des utilisateurs individuels. Cela vous permet de personnaliser le Contrôle parental, l'Alerte spam, le Blocage des publicités et la Confidentialité pour chaque utilisateur de l'ordinateur.

A propos des comptes Norton Internet Security

Votre ordinateur peut héberger plusieurs comptes, qui se classent en quatre niveaux d'accès :

Enfant	Ne peut pas modifier les paramètres de protection de Norton Internet Security. Dispose d'un accès limité aux programmes Internet et aux catégories de sites Web.
Adolescent	Ne peut pas modifier les paramètres de protection de Norton Internet Security. Peut accéder à davantage de programmes Internet et catégories de sites Web que les utilisateurs du niveau Enfant.
Adulte	Peut personnaliser l'ensemble des paramètres de Norton Internet Security pour son propre compte.
Superviseur	Peut personnaliser l'ensemble des paramètres de Norton Internet Security pour tous les utilisateurs.

Il existe également un compte par défaut, appelé Non connecté, qui bloque tout accès à Internet. Lorsqu'un utilisateur ferme une session, les paramètres du compte Non connecté restent actifs jusqu'à l'ouverture de session d'un autre utilisateur.

Se reporter à "Définition ou modification du mot de passe d'un compte" à la page 159.

Lorsque vous installez Norton Internet Security, le programme crée un compte par défaut possédant des privilèges Superviseur. Ce compte n'est pas protégé par un *mot de passe*. Pour une sécurité optimale, créez un mot de passe pour ce compte.

Si plusieurs personnes utilisent l'ordinateur, vous pouvez créer des comptes distincts pour chacun d'entre elles ou établir des comptes de groupe utilisables par tous les utilisateurs requérant un même niveau d'accès ou de restriction.

Création de comptes Norton Internet Security

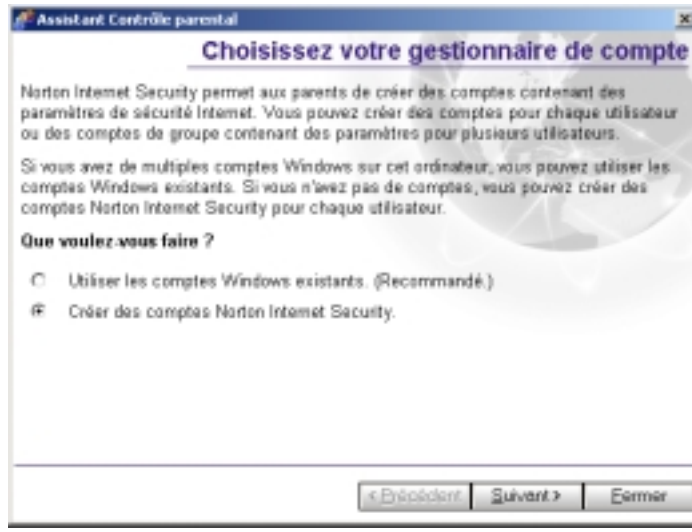
Les utilisateurs de niveau Superviseur et Adulte peuvent créer de nouveaux comptes et personnaliser les paramètres des autres utilisateurs. Ils peuvent également créer de nouveaux comptes utilisateur avec l'assistant Sécurité. Les utilisateurs de niveau Adulte peuvent personnaliser leur propre compte, mais pas celui des autres utilisateurs. Les utilisateurs de niveau Adolescent et Enfant peuvent uniquement modifier leur *mot de passe*.

Vous pouvez créer plusieurs comptes simultanément avec l'assistant Contrôle parental ou les créer l'un après l'autre avec l'écran Comptes utilisateur.

Pour créer des comptes Norton Internet Security avec l'assistant Contrôle parental

1. Ouvrez Norton Internet Security.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez sur **Comptes utilisateur**, puis sur **Assistant Contrôle parental**.

- Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Créer des comptes utilisateur**.



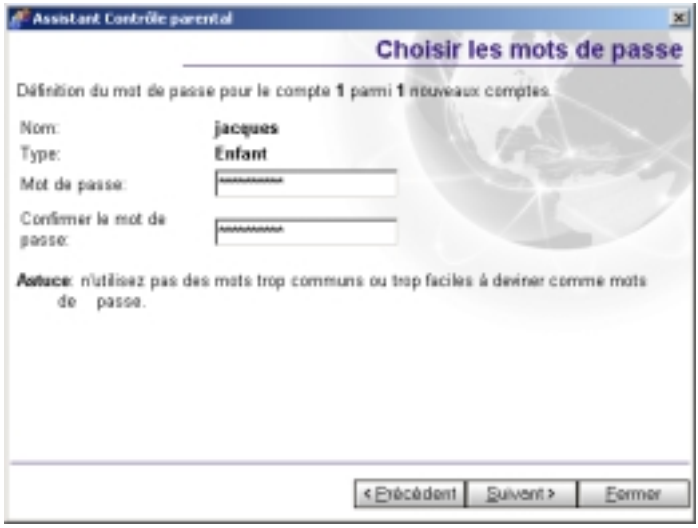
3 Sur l'écran Sélection d'un gestionnaire de compte, cliquez sur **Créer des comptes Norton Internet Security**.

4 Cliquez sur **Suivant**.

5 Sur l'écran Création de comptes, saisissez un ou plusieurs noms de compte.

6 Dans les menus de niveau de compte, sélectionnez le niveau approprié pour chaque compte.

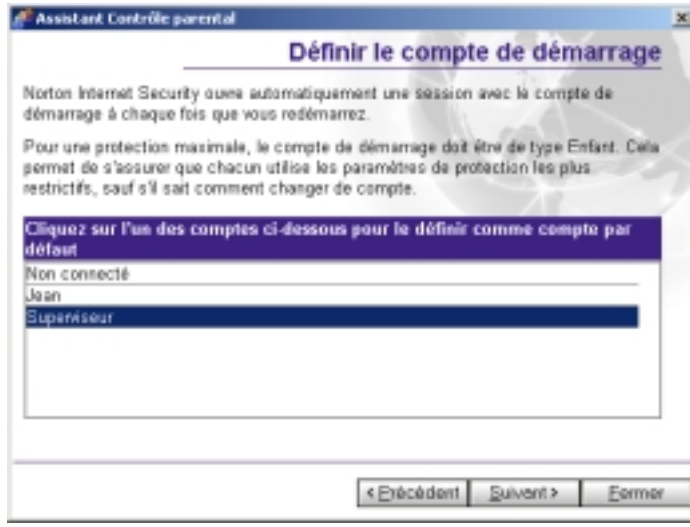
7 Cliquez sur **Suivant**.



8 Sur l'écran Sélection de mot de passe tapez un mot de passe pour cet utilisateur dans les zones de texte Mot de passe et Confirmer le mot de passe.

Se reporter à "Définition ou modification du mot de passe d'un compte" à la page 159.

9 Cliquez sur **Suivant**.
Si vous avez créé plusieurs comptes, répétez les deux étapes précédentes pour chaque compte.



Se reporter à "Définition du compte de démarrage" à la page 159.

10 Sur l'écran Définition du compte de démarrage, sélectionnez le compte auquel Norton Internet Security se connectera automatiquement au redémarrage de l'ordinateur.

11 Cliquez sur **Suivant**.

12 Cliquez sur **Terminer**.

Pour créer des comptes Norton Internet Security avec l'écran Comptes utilisateur

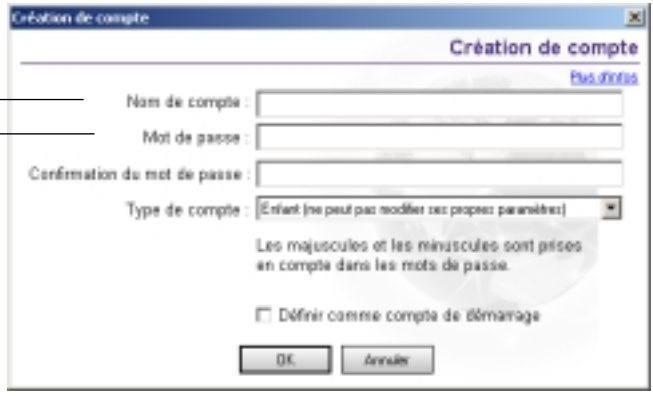
1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Comptes utilisateur**.

Indique le compte qui est connecté

Indique les comptes qui ont été définis

3 Sur l'écran Comptes utilisateur, cliquez sur **Créer un compte**.



Attribuez au compte un nom descriptif de son utilisation

Protège le compte avec un mot de qui empêche d'autres utilisateurs de s'en servir

4 Dans le champ Nom de compte de la boîte de dialogue Créer un compte, saisissez le nom du compte.

5 Dans les champs Mot de passe et Confirmation du mot de passe, saisissez le mot de passe du compte.
Les mots de passe sont sensibles à la casse (majuscules/minuscules).

6 Dans le menu Type de compte, sélectionnez un type de compte.

7 Cliquez sur **OK**.

Définition du compte de démarrage

A chaque redémarrage de l'ordinateur, Norton Internet Security se connecte automatiquement au compte défini comme compte de démarrage. Le compte de démarrage doit être le compte qui impose le plus de restrictions. Ainsi, à moins de savoir comment changer de compte, tous les utilisateurs utiliseront les paramètres les plus protégés.

Lors de l'installation de Norton Internet Security, un compte superviseur est créé. Il est désigné en tant que compte de démarrage. Pour garantir que les utilisateurs n'apportent aucune modification indésirable aux paramètres de Norton Internet Security, il est recommandé de créer un compte restreint et de le définir comme compte de démarrage par défaut.

Pour définir un compte comme compte de démarrage

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Comptes utilisateur**.

3 Sélectionnez le compte utilisateur à adopter comme compte de démarrage.

4 Cliquez sur **Propriétés**.

5 Dans la boîte de dialogue Propriétés du compte, cochez l'option **Définir comme compte de démarrage**.

6 Cliquez sur **OK**.

Définition ou modification du mot de passe d'un compte

Pour une sécurité optimale, il est recommandé de protéger chaque compte par un *mot de passe*. Ainsi, seuls les utilisateurs autorisés peuvent accéder à Internet et à votre *réseau*.

Pour définir ou modifier votre propre mot de passe

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Comptes**.

3 Sur l'écran Comptes utilisateur, sélectionnez votre compte.

4 Cliquez sur **Modifier le mot de passe**.

5 Dans la boîte de dialogue Modification du mot de passe, saisissez votre ancien mot de passe, puis le nouveau.
Si aucun mot de passe n'était précédemment affecté au compte, le champ Ancien mot de passe n'est pas disponible.

6 Cliquez sur **OK**.

Les utilisateurs du niveau Adulte peuvent modifier les mots de passe des comptes Adolescent et Enfant. Les superviseurs peuvent modifier les mots de passe de tous les autres comptes. Si vous modifiez le mot de passe d'un compte, prévenez tous les utilisateurs de ce compte.

Pour définir ou modifier le mot de passe d'autres utilisateurs

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Comptes**.

3 Sur l'écran Comptes utilisateur, sélectionnez le compte à modifier.

4 Cliquez sur **Propriétés**.

5 Sur l'écran propriétés du compte, tapez un nouveau mot de passe dans les zones de texte Mot de passe et Confirmer le mot de passe.

6 Cliquez sur **OK**.

Affectation des types de comptes Norton Internet Security aux comptes Windows

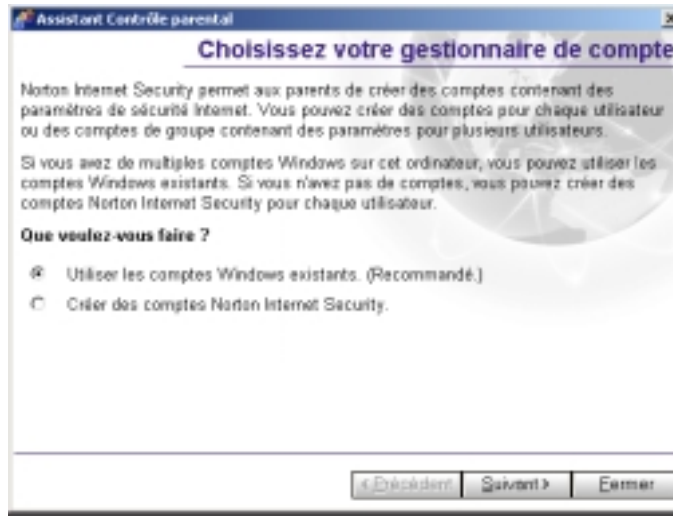
Si vous avez créé des comptes Windows pour plusieurs utilisateurs, vous pouvez utiliser ces comptes au lieu de créer de nouveaux comptes Norton Internet Security. Si vous utilisez des comptes Windows, votre compte Norton Internet Security utilisera le même nom que votre compte Windows.

Pour affecter les types de comptes Norton Internet Security à des comptes Windows

1 Ouvrez Norton Internet Security.

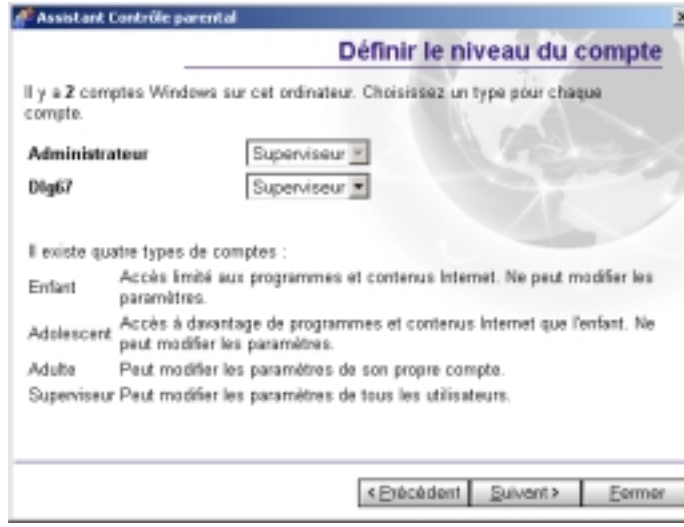
2 Dans Security Center, cliquez sur **Comptes**.

3 Dans la fenêtre Comptes, cliquez sur **Assistant Contrôle parental**.



4 Sur l'écran Sélection d'un gestionnaire de compte, cliquez sur **Utiliser les comptes Windows existants (recommandé)**.

5 Cliquez sur **Suivant**.
L'écran Sélection d'un niveau de compte affiche tous les comptes Windows actuellement définis.



6 Pour chaque compte, sélectionnez un type de compte.

7 Cliquez sur **Suivant**.

8 Cliquez sur **Terminer** pour fermer l'assistant Contrôle parental.

Ouverture d'une session Norton Internet Security

Si vous avez choisi d'installer la fonction Comptes, les utilisateurs doivent se connecter à un compte Norton Internet Security pour accéder à Internet. Vous pouvez configurer des comptes pour contrôler l'utilisation d'Internet de chaque personne.

Se reporter à "A propos des comptes Norton Internet Security" à la page 153.

Lorsqu'il est lancé, Norton Internet Security utilise les paramètres du compte défini comme compte de démarrage.

Pour changer de compte, vous devez fermer la session ouverte sous le compte courant et ouvrir une nouvelle session sous un autre compte. Vous pouvez vérifier quel est le compte actif.

Pour déterminer le compte actif

❖ Ouvrez Norton Internet Security.
Le compte actif apparaît au centre de Security Center.

Si vous souhaitez changer de compte, déconnectez-vous du compte actuel, puis ouvrez une session avec le compte souhaité.

Pour ouvrir une session sous un autre compte

1 Dans la barre d'état système de Windows, cliquez sur l'icône de Norton Internet Security.

2 Dans le menu, cliquez sur **Fermeture de session**.

3 Cliquez sur **Oui** pour confirmer la fermeture de session.

4 Dans la barre d'état système de Windows, cliquez sur l'icône de Norton Internet Security.

5 Dans le menu, cliquez sur **Ouverture de session d'un compte**.

6 Dans la fenêtre Ouverture d'une session, sélectionnez le compte à utiliser.

7 Tapez le mot de passe si nécessaire.

8 Cliquez sur **OK**.

Dès que vous changez de compte, Norton Internet Security utilise les paramètres qui lui sont associés. La fenêtre Comptes affiche le compte actuellement actif.

Personnalisation des comptes Norton Internet Security

Chaque compte Norton Internet Security peut avoir des paramètres personnalisés pour les éléments suivants :

- Contrôle parental
  Se reporter à "Protection des enfants avec le Contrôle parental" à la page 193.
- Confidentialité
  Se reporter à "Protection de votre confidentialité" à la page 165.
- Blocage des publicités
  Se reporter à "Blocage des publicités sur Internet" à la page 175.
- Alerte spam
  Se reporter à "Suppression des courriers indésirables" à la page 185.

Protection de votre confidentialité

11

Chaque fois que vous naviguez sur Internet, les ordinateurs et les *sites Web* collectent des informations à votre sujet. Certaines de ces informations proviennent de formulaires que vous remplissez et des choix que vous effectuez sur des pages. D'autres renseignements sont issus de votre *navigateur*, qui fournit automatiquement des informations sur la dernière page Web visitée et le type d'ordinateur utilisé.

Des utilisateurs malintentionnés peuvent également recueillir des informations confidentielles à votre insu Chaque fois que vous envoyez des informations par l'intermédiaire d'Internet, les données passent par un certain nombre d'ordinateurs avant d'atteindre leur destination. Lors de la transmission, des tiers peuvent intercepter ces informations.

Les ordinateurs comportent des fonctions de sécurité de base, mais celles-ci risquent de ne pas être suffisantes pour protéger vos informations confidentielles. Le Contrôle de confidentialité vous aide à protéger vos données personnelles en assurant différents niveaux de contrôle sur les *cookies* et les informations que votre navigateur envoie aux sites Web.

Le Contrôle de confidentialité permet également de vous assurer que les utilisateurs n'envoient pas par inadvertance des informations confidentielles non codées sur Internet, comme des numéros de carte de crédit.

Identification des informations confidentielles à protéger

Sur de nombreux *sites Web*, vous êtes invité à indiquer votre nom, votre *adresse électronique* et d'autres informations confidentielles. Bien que vous puissiez généralement fournir ces informations en toute confiance aux sites renommés, des sites malveillants peuvent utiliser ces informations pour porter atteinte à votre vie privée. Des personnes peuvent également intercepter des informations envoyées par l'intermédiaire du Web, de la messagerie électronique ou des programmes de messagerie instantanée.

Le Contrôle de confidentialité permet d'établir la liste des informations qui doivent rester confidentielles. Si des utilisateurs tentent d'envoyer des informations confidentielles sur Internet, Norton Internet Security les avertit du risque encouru par rapport à la sécurité ou bloque la *connexion*. Tous les utilisateurs d'un ordinateur sécurisé partagent une même liste d'informations confidentielles.

Conseils de saisie des informations confidentielles

Norton Internet Security bloque les informations confidentielles telles que vous les avez saisies. Il est donc préférable de taper une partie seulement des numéros à protéger. Par exemple, un numéro de téléphone peut être saisi sous la forme 01-02-03-04-05, 0102030405 ou 01 02 03 04 05, voire dans plusieurs champs. Quel que soit le format, les deux derniers chiffres sont toujours groupés. Vous serez donc mieux protégé si vous saisissez uniquement les derniers chiffres au lieu du numéro entier.

La saisie d'informations partielles présente deux avantages. En ne saisissant pas l'intégralité du numéro, vous évitez que quelqu'un n'en prenne connaissance. Deuxièmement, Norton Internet Security pourra bloquer vos informations confidentielles sur les sites sur lesquels les numéros de carte de crédit sont découpés en plusieurs champs.

Confidentialité et SSL

Certains sites Web et serveurs de messagerie utilisent des connexions SSL (Secure Socket Layer) pour chiffre les connexions entre votre ordinateur et le serveur. Le Contrôle de confidentialité ne peut pas bloquer les informations confidentielles transmises sur des connexions SSL. Toutefois comme les informations sont chiffrées, le destinataire du courrier électronique sera seul à pouvoir le lire.

Ajout d'informations confidentielles

Vous devez ajouter les informations à protéger à la liste Informations confidentielles de Norton Internet Security. Tous les utilisateurs d'un ordinateur partagent une même liste d'informations confidentielles.

Pour ajouter des informations confidentielles

1. Démarrez Norton Internet Security.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez deux fois sur **Confidentialité**, puis sur **Informations confidentielles**.
   - Dans le menu Sélectionner une tâche de Security Monitor, sélectionnez **Modifier les informations confidentielles**.
3. Dans la boîte de dialogue Informations confidentielles, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue Ajout d'informations confidentielles, sélectionnez une catégorie dans la liste Type d'informations à protéger.
5. Dans le champ Nom descriptif, indiquez pour mémoire la raison pour laquelle vous souhaitez protéger ces données.
6. Dans le champ Informations à protéger, tapez les informations dont vous souhaitez empêcher la transmission sur des connexions Internet non sécurisées.
7. Dans le champ Protéger ces informations confidentielles pour, sélectionnez les programmes Internet dans lesquels le Contrôle de la confidentialité doit bloquer ces informations :
   - Web
   - Messagerie instantanée
   - Courrier électronique
8. Cliquez sur **OK**.

Modification ou suppression d'informations confidentielles

Vous pouvez modifier ou supprimer des informations confidentielles à tout moment.

Pour modifier ou supprimer des informations confidentielles

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre e volet Confidentialité, cliquez sur **Informations confidentielles**.
4. Sélectionnez les informations confidentielles à modifier ou à supprimer.
5. Sélectionnez l'une des options suivantes :
   - Modifier
   - Supprimer
6. Cliquez sur **OK**.

Personnalisation de la confidentialité

Le Contrôle de confidentialité protège quatre zones :

Informations confidentielles	Bloque des chaînes de texte spécifiques à ne pas envoyer sur Internet.
Blocage des cookies	Empêche les sites Web de récupérer des informations personnelles stockées dans des fichiers de cookies.
Confidentialité de navigation	Protège les informations relatives à vos habitudes de navigation.
Connexions sécurisées	Empêche les utilisateurs d'établir des connexions sécurisées vers des sites marchands et d'autres sites Web.

Les utilisateurs de type Superviseur et Adulte peuvent modifier les paramètres du programme. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier le Contrôle de confidentialité.

Il existe deux façons de définir les paramètres de confidentialité :

- Définir le niveau de confidentialité
  Utilisez le curseur du volet principal Confidentialité pour sélectionner des niveaux de sécurité prédéfinis.
- Régler des paramètres de confidentialité individuels
  Personnalisez votre protection en réglant des paramètres manuellement.

Vous pouvez définir des paramètres de confidentialité individuels pour chaque utilisateur de Norton Internet Security.

Définition du niveau de confidentialité

Norton Internet Security propose des niveaux de sécurité prédéfinis permettant de paramétrer plusieurs options de confidentialité à la fois. Le curseur de niveau de confidentialité permet de sélectionner une protection minimale, moyenne ou maximale.

Pour définir le niveau de confidentialité

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre Contrôle de confidentialité, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle de confidentialité pour.
4. Placez le curseur sur le niveau de confidentialité souhaité. Les options sont les suivantes :

Haut	Toutes les informations confidentielles sont bloquées et une alerte s'affiche à chaque cookie rencontré.
Moyen (recommandé)	Une alerte apparaît si des informations confidentielles sont saisies dans un formulaire Web ou une messagerie instantanée. Dissimule votre navigation aux sites Web. Les cookies ne sont pas bloqués.
Bas	Les informations confidentielles ne sont pas bloquées. Les cookies ne sont pas bloqués. Dissimule votre navigation aux sites Web.

5. Cliquez sur **OK**.

Réglage de paramètres de confidentialité individuels

Vous pouvez modifier les paramètres pour les options Informations confidentielles, Blocage des cookies, Confidentialité de navigation et Connexions sécurisées si le niveau de confidentialité ne vous convient pas. Par exemple, vous pouvez bloquer toute tentative d'envoi d'informations confidentielles, tout en autorisant des sites Web à personnaliser leurs pages en utilisant les informations de votre navigateur.

Modification du paramètre Informations confidentielles

Modifiez le paramètre Informations confidentielles pour contrôler la façon dont Norton Internet Security traite les tentatives d'envoi sur Internet d'informations figurant dans la liste Informations confidentielles.

Pour modifier le paramètre Informations confidentielles

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre Contrôle de confidentialité, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle de confidentialité pour.
4. Cliquez sur **Niveau personnalisé**.
5. Sélectionnez un paramètre pour Informations confidentielles. Les options sont les suivantes :

Maximum	Bloque toutes les informations confidentielles.
Moyen	Vous avertit quand vous tentez de transmettre des informations confidentielles à un site Web non sécurisé ou par l'intermédiaire d'un programme de messagerie instantanée.
Aucun	Ne bloque pas les informations confidentielles.

6. Cliquez sur **OK**.

Modification du paramètre Blocage des cookies

De nombreux sites Web stockent les informations collectées dans des *cookies* placés sur votre disque dur. Lorsque vous retournez sur un site qui a installé un cookie sur votre ordinateur, le serveur Web ouvre le cookie et le lit.

La plupart des cookies sont inoffensifs. Les sites les utilisent pour personnaliser les pages Web, mémoriser vos choix sur le site et proposer des pages optimisées pour votre ordinateur. Cependant, les sites peuvent également utiliser des cookies pour effectuer le suivi de l'usage que vous faites d'Internet et de vos habitudes de navigation.

Modifiez le paramètre Blocage des cookies pour contrôler la façon dont Norton Internet Security gère les sites qui tentent de placer des cookies sur votre ordinateur.

Pour modifier le paramètre Blocage des cookies

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre Contrôle de confidentialité, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle de confidentialité pour.
4. Cliquez sur **Niveau personnalisé**.
5. Sélectionnez un paramètre pour Blocage des cookies. Trois options sont disponibles :

Maximum	Bloque tous les cookies.
Moyen	Vous prévient chaque fois qu'un cookie est rencontré.
Aucun	Autorise les cookies.

6. Cliquez sur **OK**.

Activation ou désactivation de la Confidentialité de navigation

La Confidentialité de navigation empêche les sites Web d'identifier le type de *navigateur* que vous utilisez, le dernier site Web visité en dernier et d'autres informations concernant vos habitudes de navigation. Certains sites Web basés sur JavaScript risquent de ne pas fonctionner correctement s'ils ne peuvent pas identifier le type de navigateur utilisé.

Pour activer ou désactiver la Confidentialité de navigation

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre Contrôle de confidentialité, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle de confidentialité pour.
4. Cliquez sur **Niveau personnalisé**.
5. Dans la boîte de dialogue Personnalisation de la confidentialité, cochez ou décochez la case **Activer la confidentialité de navigation**.
6. Cliquez sur **OK**.

Activation ou désactivation des connexions Web sécurisées

Lorsque vous visitez un site Web sécurisé, le navigateur établit automatiquement une *connexion* chiffrée avec ce site. Par défaut, Norton Internet Security permet à tous les comptes d'utiliser des connexions sécurisées. Si vous souhaitez éviter que les utilisateurs n'envoient pas d'informations confidentielles vers des sites Web sécurisés, désactivez les connexions Web sécurisées.

Si vous désactivez les connexions Web sécurisées, votre navigateur ne chiffrera plus aucune information envoyée. Désactivez les connexions Web sécurisées uniquement si vous protégez vos informations confidentielles.

Pour activer ou désactiver les connexions Web sécurisées

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Confidentialité**.
3. Dans la fenêtre Contrôle de confidentialité, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle de confidentialité pour.
4. Cliquez sur **Niveau personnalisé**.
5. Dans la boîte de dialogue Personnalisation de la confidentialité, cochez ou décochez la case **Activer les connexions sécurisées (https)**.
6. Cliquez sur **OK**.

Blocage des publicités sur Internet

12

De nombreux sites Web utilisent des techniques agressives pour attirer l'attention sur les publicités présentes sur leurs pages. Certains utilisent des publicités de grande taille et voyantes, tandis que d'autres font appel à des fenêtres qui apparaissent lorsque vous visitez ou quittez le site. Outre l'augmentation du délai d'affichage des pages Web, certaines publicités contiennent des contenus inconvenants, provoquent des conflits logiciels ou utilisent des astuces *HTML* pour ouvrir des fenêtres de *navigateur* supplémentaires.

Le Blocage des publicités permet d'éviter ces problèmes. Lorsque le Blocage des publicités est actif, Norton Internet Security supprime de manière transparente les éléments suivants :

- Bannières publicitaires
- Publicités déroulantes
- Publicités "Flash" Macromedia

Fonctionnement du Blocage des publicités

Norton Internet Security détecte et bloque les publicités selon deux critères : leurs dimensions et leur emplacement.

Blocage d'après les dimensions

La plupart des publicistes en ligne utilisent une ou plusieurs dimension standard pour leurs publicités. Norton Internet Security est désormais capable de bloquer les images, les animations Flash et d'autres éléments *HTML* dont les dimensions sont celles des publicités courantes.

Blocage d'après l'emplacement

Chaque fichier sur Internet possède une adresse ou *URL* unique. Lorsqu'une page Web s'affiche, l'ordinateur se connecte à une URL et affiche le fichier stocké à cet emplacement. Si la page pointe vers des images, des fichiers audio ou d'autres contenus multimédia, votre *navigateur* affiche les fichiers en tant qu'éléments de la page.

Lorsque vous consultez une page Web contenant une *bannière publicitaire*, les instructions d'affichage de la page peuvent inclure les options suivantes :

<p>Bienvenue chez Ajax<img src="http://www.ajax.com/nifty_images/image7.gif">

Le navigateur affiche le texte "Bienvenue chez Ajax". Il se connecte ensuite à www.ajax.com et demande un fichier appelé /belles_images/image7.gif. (Le suffixe .gif indique qu'il s'agit d'un fichier de format GIF (Graphics Interchange Format), c'est à dire un format commun de fichier image.) L'ordinateur à l'adresse www.ajax.com envoie le fichier au navigateur qui affiche l'image.

Si le Blocage des publicités est activé lorsque vous vous connectez à un site Web, Norton Internet Security analyse les pages Web et compare leur contenu à deux listes :

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

- Une liste par défaut de publicités bloquées automatiquement par Norton Internet Security. Utilisez LiveUpdate pour actualiser régulièrement la liste des publicités bloquées.
- Une liste que vous créez en interceptant des publicités spécifiques. Vous pouvez enrichir et modifier cette liste.

Si la page contient des fichiers issus d'un *domaine* bloqué, Norton Internet Security supprime le lien et télécharge le reste de la page.

Vous pouvez définir des paramètres individuels du Blocage des publicités pour chaque utilisateur de Norton Internet Security. Les utilisateurs de type Superviseur et Adulte peuvent modifier les paramètres du programme. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier la fonction Blocage des publicités.

Activation et désactivation du Blocage des publicités

Norton Internet Security recherche les adresses des publicités à bloquer pendant le téléchargement de la page Web par le *navigateur*. S'il détecte des adresses figurant dans la liste des publicités à intercepter, les informations correspondantes sont bloquées pour qu'elles ne s'affichent pas dans le navigateur. Le reste de la page Web demeure inchangé et vous pouvez le consulter sans publicités.

Pour activer ou désactiver le Blocage des publicités

1 Ouvrez Norton Internet Security.

2 Cliquez deux fois sur **Blocage des publicités**.

3 Dans la fenêtre du Blocage des publicités, sélectionnez le compte à modifier dans la liste Paramètres du Blocage des publicités pour.

4 Cochez ou décochez la case **Activer le blocage des publicités**.

5 Cliquez sur **OK**.

Activation/désactivation du Blocage des fenêtres déroulantes

Les publicités déroulantes sont des fenêtres secondaires que les sites Web ouvrent lorsque vous visitez ou quittez le site. Ces fenêtres apparaissent devant ("pop-up") ou derrière ("pop-under") la fenêtre en cours.

Lorsque le Blocage des fenêtres déroulantes est actif, Norton Internet Security bloque automatiquement le code de programmation que les sites Web utilisent pour ouvrir des fenêtres secondaires à votre insu. Les sites qui ouvrent des fenêtres secondaires lorsque vous cliquez sur un lien ou effectuez d'autres actions ne sont pas affectés.

Pour activer ou désactiver le Blocage des fenêtres déroulantes

1. Ouvrez Norton Internet Security.
2. Cliquez deux fois sur **Blocage des publicités**.
3. Dans la fenêtre du Blocage des publicités, sélectionnez le compte à modifier dans la liste Paramètres du Blocage des publicités pour.
4. Cochez ou décochez la case **Activer le blocage des fenêtres déroulantes**.
5. Cliquez sur **OK**.

Activation ou désactivation du Blocage Flash

Lorsque le Blocage des publicités est actif, Norton Internet Security bloque automatiquement toutes les animations Flash qui ont les dimensions des publicités courantes. Norton Internet Security peut également bloquer tous les contenus Flash. Cette option est utile si votre connexion est lente ou si vous n'êtes pas intéressé par l'affichage d'animations Flash.

Vous pouvez demander à Norton Internet Security de bloquer toutes les animations Flash ou de ne les bloquer que sur certains sites Web. Le fait de modifier les paramètres du Blocage Flash affecte tous les utilisateurs de cet ordinateur.

Pour activer ou désactiver le Blocage Flash

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Contenu Web, cliquez sur l'onglet **Paramètres globaux**.

4 Dans la liste des sites Web, effectuez l'une des opérations suivantes :
   - Pour modifier les paramètres Flash de tous les sites, cliquez sur **(Par défaut)**.
   - Pour modifier les paramètres Flash d'un site de la liste, cliquez sur le nom du site.
   - Pour modifier les paramètres Flash d'un site absent de la liste, cliquez sur **Ajouter** et tapez l'adresse du site dans la boîte de dialogue Nouveau site/domaine.
5 Dans la section Animation Flash, sélectionnez l'une des options suivantes :
   - Bloquer
   - Autoriser
6 Cliquez sur **OK**.

Certains sites Web utilisent Flash pour créer des barres d'outils de navigation. Le Blocage Flash peut rendre ces sites inexploitables.

Utilisation de la Corbeille publicitaire

En utilisant Internet, vous vous rendrez compte que certaines publicités ne font pas partie de la liste de Blocage des publicités par défaut de Norton Internet Security. Vous pouvez utiliser la Corbeille publicitaire pour les ajouter à votre liste personnelle de publicités bloquées.

Pour utiliser la Corbeille publicitaire

1 Lancez votre navigateur Web et affichez la page qui contient la publicité à bloquer.
2 Ouvrez Norton Internet Security.
3 Dans Security Center, cliquez deux fois sur **Blocage des publicités**.
4 Blocage des publicités, vérifiez que Activer le blocage des publicités est coché.
5 Cliquez sur **Ouvrir la Corbeille publicitaire**.
La fenêtre Corbeille publicitaire apparaît.

6 Disposez les fenêtres de manière à voir à la fois la publicité et la fenêtre de la Corbeille, puis effectuez l'une des opérations suivantes :

- Si vous utilisez Microsoft Internet Explorer, faites glisser la publicité importune du site Web vers la boîte de dialogue Blocage des publicités.
- Si vous utilisez Netscape, cliquez sur la publicité avec le bouton droit de la souris puis cliquez sur **Copier l'adresse de l'image**. Dans la Corbeille publicitaire, cliquez sur **Coller**.
  L'adresse de la publicité apparaît dans la zone Informations sur la publicité de la boîte de dialogue Corbeille publicitaire.

7 Sélectionnez l'une des options suivantes :

- Ajouter : Bloquer cette adresse.
- Modifier : Modifier l'entrée avant de l'ajouter à la liste de Blocage des publicités.
  Par exemple, si l'adresse de la publicité est http://www.publicites.org/irritantes/pubs/numeroun.gif, vous pouvez la changer pour l'adresse http://www.publicites.org/irritantes/pubs pour bloquer tout le contenu du répertoire "pubs".

8 Cliquez sur **OK**.

Utilisation des chaînes de texte pour identifier les publicités à bloquer ou à autoriser

Vous pouvez spécifier que Norton Internet Security affiche des publicités spécifiques en créant une liste de chaînes de texte identifiant des bannières publicitaires individuelles. Les chaînes de Blocage des publicités sont des sections d'adresses *HTML*. Si une partie de l'adresse d'un fichier correspond à la chaîne de texte, Norton Internet Security bloque automatiquement le fichier.

Norton Internet Security propose une liste prédéfinie (Par défaut) de Blocage des publicités utilisée pour déterminer les images à bloquer lors de l'affichage de pages Web.

Lorsque le Blocage des publicités est activé, toutes les pages Web sont analysées pour repérer les chaînes HTML définies dans la liste (Par défaut). Norton Internet Security recherche les chaînes bloquées dans les balises HTML utilisées pour représenter les images et les publicités. Les structures HTML qui contiennent des chaînes en correspondance sont supprimées par Norton Internet Security avant que la page ne soit affichée dans le navigateur Web.

Veillez à ne pas insérer de chaînes trop génériques dans la liste de blocage (Par défaut). Par exemple, il ne serait pas judicieux de bloquer la chaîne www car presque toutes les *URL* contiennent www. Une chaîne telle que www.slowads est plus efficace car elle bloque uniquement les graphiques du *domaine* slowads sans affecter les autres sites.

Tous les utilisateurs partagent une liste commune de Blocage des publicités. Les utilisateurs de type Superviseur et Adulte peuvent modifier la liste. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier les paramètres de Blocage des publicités.

Identification des chaînes de Blocage des publicités

La manière dont vous définissez les chaînes de Blocage des publicités détermine la rigueur avec laquelle Norton Internet Security filtre les données.

Si vous ajoutez par exemple la chaîne ajax.com à la liste de blocage (Par défaut), toutes les pages du domaine ajax.com sont bloquées. En vous montrant plus précis, par exemple en ajoutant la chaîne "belles_images/image7.gif" à la liste de blocage spécifique au site www.ajax.com, seule cette image est bloquée.

Un site peut devenir inutilisable si toutes ses images sont bloquées. Un bon compromis consiste à bloquer seulement les répertoires contenant des publicités. Par exemple, si www.ajax.com stocke ses publicités sous /nifty_images/ et ses images de navigation sous /useful_images/, il est possible de bloquer www.ajax.com/nifty_images/ sans limiter l'utilisation du site.

Vous pouvez également créer des chaînes d'autorisation qui permettent aux sites Web d'afficher les images correspondant à la chaîne. Ceci vous permet de neutraliser l'effet de blocage d'une chaîne dans la liste de blocage (Par défaut) pour des sites individuels. Les règles d'autorisation sont prioritaires par rapport aux règles de blocage sur tous les sites.

Ajout d'une chaîne de Blocage des publicités

Vous pouvez ajouter des chaînes à la liste de Blocage des publicités pour tous les sites ou des sites spécifiques.

Pour ajouter une chaîne de Blocage des publicités

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Contenu Web, sur l'onglet Blocage des publicités, faites l'une des opérations suivantes :
   - Pour bloquer une chaîne sur tous les sites Web, cliquez sur **(Par défaut)**.
   - Pour bloquer une chaîne sur un site Web de la liste, sélectionnez le nom du site.
   - Pour bloquer une chaîne sur un site Web absent de la liste, cliquez sur **Ajouter un site** et tapez l'adresse du site dans la boîte de dialogue Nouveau site/domaine.
4. Sur l'onglet Blocage des publicités, cliquez sur **Ajouter**.
5. Dans la boîte de dialogue Ajouter une nouvelle chaîne HTML, sélectionnez l'action à effectuer. Les options sont les suivantes :

Bloquer	Bloque les publicités correspondant à la chaîne.
Autoriser	Accepte les publicités correspondant à la chaîne.

6. Saisissez une chaîne HTML à bloquer ou à autoriser.
7. Cliquez sur **OK**.

Modification ou suppression d'une chaîne de Blocage des publicités

S'il apparaît qu'une chaîne de Blocage des publicités devient trop restrictive, pas assez vaste ou inadaptée, vous pouvez la modifier ou la supprimer.

Pour modifier ou supprimer une chaîne de Blocage des publicités

1. Ouvrez Norton Internet Security.
2. En haut de la fenêtre Security Center, cliquez sur **Options** > **Sécurité Internet**.
3. Sur l'onglet Blocage des publicités de l'onglet Contenu Web, effectuez l'une des opérations suivantes :
   - Pour modifier ou supprimer une chaîne de la liste (Par défaut), cliquez sur **(Par défaut)**.
   - Pour modifier ou supprimer une chaîne d'un site spécifique, sélectionnez le nom du site.
4. Dans la liste des chaînes HTML, sélectionnez celle à modifier.
5. Effectuez l'une des opérations suivantes :
   - Pour modifier une chaîne, cliquez sur **Modifier** et saisissez vos modifications.
   - Pour supprimer une chaîne, cliquez sur **Supprimer**.
6. Cliquez sur **OK**.

Suppression des courriers indésirables

13

Le *courrier électronique* est devenu populaire et de nombreux utilisateurs reçoivent des volumes croissants de courriers publicitaires non sollicités, baptisés "spam". Le spam ne rend pas seulement difficile d'identifier le courrier utile. Dans certains cas, il contient des textes ou des images choquants.

L'Alerte spam permet de diminuer le nombre de courriers non sollicités que vous recevez en filtrant intelligemment les messages entrants et en marquant distinctement les courriers spam éventuels.

Fonctionnement de l'Alerte spam

L'Alerte spam utilise un moteur de correspondance de modèle, qui compare automatiquement le contenu de tous les *courriers électroniques entrants* à une liste de caractéristiques connues des spam. Plus un courrier comporte de caractéristiques des spam, plus il est susceptible d'en être. Sur la base de cette analyse, l'Alerte spam évalue la probabilité que le courrier soit du spam.

Après cette analyse initiale, Norton Internet Security utilise les paramètres que vous avez spécifiés dans la page Alerte spam pour identifier les messages marqués comme spam. Si l'Alerte spam est définie sur un niveau de sensibilité Bas, un courrier doit comporter de nombreuses caractéristiques de spam avant d'être bloqué. Si l'Alerte spam est définie sur un niveau de sensibilité Elevé, un courrier ne comportant que quelques caractéristiques de spam sera bloqué.

Quand un courrier est identifié comme du spam, Norton Internet Security indique "Alerte Spam :" au début de l'objet du courrier. Vous pouvez alors utiliser le programme de messagerie pour créer des filtres bloquant touts les courriers contenant ce texte.

Si vous avez choisi d'installer la fonction Comptes, vous pouvez créer des paramètres d'Alerte spam personnalisés pour chaque utilisateur. Les utilisateurs de type Superviseur et Adulte peuvent modifier les paramètres d'Alerte spam. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier ces paramètres.

Alerte spam et SSL

Certains serveurs de messagerie utilisent des *connexions* SSL (Secure Socket Layer) pour chiffrer les connexions entre votre ordinateur et le serveur. L'Alerte spam ne peut analyser les courriers reçus sur des connexions SSL.

Activation et désactivation de l'Alerte spam

Activation et désactivation de l'Alerte spam depuis Security Center

Pour activer ou désactiver l'Alerte spam

1. Ouvrez Norton Internet Security.
2. Cliquez deux fois sur **Alerte spam**.
3. Dans la fenêtre Alerte spam, dans la liste déroulante Paramètres de l'Alerte spam pour, sélectionnez le compte à modifier.
4. Cochez ou décochez la case **Activer l'Alerte spam**.

5 Utilisez le curseur de l'Alerte spam pour déterminer la rigueur du filtrage de spam de Norton Internet Security. Les options sont les suivantes :

Maximum	Filtrage maximum du contenu. La plupart des courriers de spam sont identifiés correctement. Probabilité plus élevée d'identifier des courriers personnels comme du spam.
Moyen (recommandé)	Filtrage modéré. De nombreux courriers de spam sont identifiés correctement. Probabilité moyenne d'identifier des courriers personnels comme du spam.
Minimum	Filtrage léger du contenu. Une partie du spam est identifiée correctement. Courriers personnels rarement identifiés comme du spam.

6 Cliquez sur **OK**.

Création de filtres de spam

Quand l'Alerte de spam est active, Norton Internet Security ajoute l'avertissement "Alerte Spam :" au début de l'objet des courriers identifiés comme spam. Cela vous permet de filtrer facilement ces courriers avec votre programme de *messagerie*.

Symantec fournit des instructions de configuration pour Microsoft Outlook Express, Microsoft Outlook, Netscape Communicator et Eudora, mais l'Alerte spam fonctionnera avec la plupart des programmes de messagerie utilisant POP3.

Pour créer des filtres de spam pour Microsoft Outlook Express

1 Ouvrez Microsoft Outlook Express.

2 Dans le menu Outils, cliquez sur **Règles de message > Courrier**.

3 Dans la fenêtre Nouvelle règle de courrier, sous sélectionnez les conditions pour votre règle, cochez **Lorsque la ligne Objet contient des mots spécifiques**.

4 Sous Sélectionnez les actions pour votre règle, cochez **Le déplacer vers le dossier spécifié**.

5 Sous Description de la règle, cliquez sur **contient des mots spécifiques**.

6 Dans la boîte de dialogue Entrer des mots spécifiques, tapez **Alerte spam :** et cliquez sur **Ajouter**.

7 Cliquez sur **OK**.

8 Sous Description de la règle, cliquez sur **spécifié**.

9 Dans la boîte de dialogue Déplacer, cliquez sur le signe plus (+) en regard de Dossiers locaux pour afficher vos dossiers de courrier.

10 Dans la liste de boîtes postales, choisissez la boîte de spam et cliquez sur **OK**.

11 Dans la boîte de dialogue Nouvelle règle de courrier, tapez un nom pour la règle dans la zone Nom de la règle.

12 Cliquez sur **OK**.

13 Dans la fenêtre Règles de courrier, cliquez sur **OK**.

Pour créer des filtres de spam pour Microsoft Outlook

1 Ouvrez Microsoft Outlook Express.

2 Dans le menu Outils, cliquez sur **Règles de message** > **Courrier**.

3 Cliquez sur **Nouveau**.

4 Sous Quel type de règles voulez-vous créer, cliquez sur **Vérifiez les messages quand ils arrivent**.

5 Cliquez sur **Suivant**.

6 Sous Quelles conditions voulez-vous vérifier, cliquez sur **avec des mots spécifiques dans l'objet**.

7 Sous Description de règle, cliquez sur **mots spécifiques**.

8 Dans la boîte de dialogue Chercher le texte, tapez **Alerte spam :** et cliquez sur **OK**.

9 Cliquez sur **Suivant**.

10 Sous Que voulez-vous faire avec le message, cochez **le déplacer vers le dossier spécifié**.

11 Sous Description de la règle, cliquez sur **spécifié**.

12 Dans la boîte de dialogue Déplacer, cliquez sur le signe plus (+) en regard de Dossiers locaux pour afficher vos dossiers de courrier.

13 Dans la liste de boîtes postales, choisissez la boîte de spam et cliquez sur **OK**.

14 Cliquez sur **Suivant**.

15 Sous Spécifiez un nom pour la règle, tapez un nom pour cette règle.

16 Vérifiez que Activer cette règle est coché.
Si votre Boîte de réception contient déjà des courriers comportant Alerte spam, cochez **Exécuter cette règle sur les messages déjà dans la Boîte de réception** pour les filtrer.

17 Cliquez sur **Terminer**.

Pour créer des filtres de spam pour Netscape Messenger

1 Ouvrez Netscape Messenger.

2 Dans le menu Edition, cliquez sur **Filtres de message**.

3 Cliquez sur **Nouveau**.

4 Tapez un nom pour le filtre.

5 Dans la boîte de texte Contient, tapez **Alerte spam :**.

6 Dans le menu alors, effectuez l'une des opérations suivantes :

- Pour supprimer immédiatement les messages spam, cliquez sur **Supprimer**.
- Pour transférer les courriers identifiés comme spam dans un dossier spécial, cliquez sur **Boîte de réception** et sélectionnez le nom du dossier.

7 Cliquez sur **OK**.

Pour créer des filtres de spam pour Eudora

1 Ouvrez Eudora.

2 Dans le menu Outils, cliquez sur **Filtres**.

3 Cliquez sur **Nouveau**.

4 Sous Correspondance, cochez ce qui suit :

- Entrant
- Manuel

5 Dans le menu En-tête, cliquez sur **Objet**.

6 Dans la zone de texte contient, tapez **Alerte spam :**.

7 Dans le menu Action, cliquez sur le premier élément, puis sélectionnez **Transférer vers**.

8 Cliquez sur le bouton **Dans**.

9 Dans le menu Transfert, cliquez sur **Poubelle**.

10 Dans le menu Fichier, cliquez sur **Enregistrer**.

Personnalisation de l'Alerte spam

Vous pouvez personnaliser votre protection en identifiant les adresses de *courrier électronique* et les chaînes de texte qui doivent ou non être filtrées. Lorsque l'Alerte spam rencontre un message contenant l'une de ces adresses ou de ces chaînes de texte, elle ignore la correspondance de motif et classe immédiatement le message selon les paramètres que vous avez définis. C'est une manière facile de garantir que les groupes de discussion et autres messages issus d'expéditeurs de confiance ne sont pas considérés comme du spam.

Tous les utilisateurs de cet ordinateur partagent une même liste d'Alerte spam. Les utilisateurs de type Superviseur et Adulte peuvent modifier la liste. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier les paramètres de l'Alerte spam.

Ajout d'une entrée d'Alerte spam

1. Ouvrez Norton Internet Security.
2. Cliquez deux fois sur **Alerte spam**.
3. Dans la fenêtre Alerte spam, dans la liste déroulante Paramètres de l'Alerte spam pour, sélectionnez le compte à modifier.
4. Dans la fenêtre Alerte spam, cliquez sur **Avancé**.
5. Dans la fenêtre Alerte spam avancée, cliquez sur **Nouveau**.
6. Dans la fenêtre Nouvelle entrée de spam, tapez une adresse ou une chaîne de texte dans la zone de texte Chercher.
7. Dans le menu Chercher dans, sélectionnez où Norton Internet Security doit rechercher le texte. Il y a cinq options :
   - De : (nom de l'expéditeur)
   - A : (nom du detinataire)
   - Objet du message
   - Corps du message
   - N'importe où dans le message
8. Sous Classer le message en, choisissez si les messages qui contiennent ce texte sont du spam ou n'en sont pas.
9. Cliquez sur **OK**.
10. Cliquez sur **OK**.

Vous pouvez modifier ou supprimer une entrée d'alerte spam si elle provoque un classement incorrect des messages.

Pour modifier ou supprimer un entrée d'Alerte spam

1. Ouvrez Norton Internet Security.
2. Cliquez deux fois sur **Alerte spam**.
3. Dans la fenêtre Alerte spam, dans la liste déroulante Paramètres de l'Alerte spam pour, sélectionnez le compte à modifier.
4. Dans la fenêtre Alerte spam, cliquez sur **Avancé**.
5. Dans la fenêtre Alerte spam avancée, sélectionnez l'entrée d'Alerte spam que vous voulez modifier.
6. Sélectionnez l'action à effectuer. Les options sont les suivantes :

Modifier	Change l'entrée.
Supprimer	Supprime l'entrée.

7. Cliquez sur **OK**.
8. Cliquez sur **OK**.

Conseils pour l'Alerte spam

Quand vous utilisez l'Alerte spam, rappelez-vous que :

- Vous devez périodiquement vérifier les *courriers électroniques* entrants pour vous assurer que l'Alerte spam n'identifie pas par erreur des courriers valides comme du spam.
- Pour éviter de perdre des courriers légitimes, utilisez votre programme de messagerie pour créer un dossier de spam. Vous pouvez ainsi conserver tous les courriers marqués "Alerte spam" dans ce dossier et les vérifier périodiquement avant de les supprimer.
- Les expéditeurs de spam incluent souvent des adresses fictives dans le champ De :. L'ajout d'adresses individuelles à la liste de l'Alerte spam est peu susceptible de réduire la quantité de spam que vous recevez.

Protection des enfants avec le Contrôle parental

14

Norton Internet Security inclut le Contrôle parental, grâce auquel les parents peuvent contrôler l'accès de leurs enfants à Internet. Contrôle parental vous permet de contrôler :

Sites Web	Bloquez l'accès aux pages Web à caractère pornographique, violent ou inadapté.
Programmes	Interdisez l'accès à des catégories d'applications Internet présentant des risques de sécurité ou susceptibles d'entraîner des abus.
Groupes de discussion	Limitez l'accès aux groupes de discussion traitant de sujets extrémistes, illégaux ou inadaptés.

Les utilisateurs de type Enfant ne peuvent modifier les paramètres du Contrôle parental.

A propos du Contrôle parental

Le Contrôle parental classe les *sites Web* par sujet, les groupes de discussion par chaîne de texte et les applications Internet par type.

Lorsque le Contrôle parental est activé, Norton Internet Security bloque toutes les informations entrantes provenant des sites Web et des groupes de discussion interdits. Il bloque également toutes les informations sortantes provenant d'applications Internet interdites.

Les paramètres du Contrôle parental sont liés aux comptes utilisateur. Lorsqu'un utilisateur se connecte à son compte, Norton Internet Security applique les paramètres associés au compte jusqu'à ce que l'utilisateur se déconnecte.

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Symantec met régulièrement à jour la liste des sites Web interdits. Exécutez fréquemment LiveUpdate pour vérifier que vous disposez de la liste la plus récente.

Activation et désactivation du Contrôle parental

Les utilisateurs de type Superviseur et Adulte peuvent activer et désactiver le Contrôle parental. Les utilisateurs de type Adulte peuvent modifier les paramètres du Contrôle parental pour leur compte. Les utilisateurs de type Superviseur peuvent aussi modifier les paramètres du Contrôle parental de tous les utilisateurs. Les utilisateurs de type Enfant et Adolescent ne peuvent pas modifier le Contrôle parental.

Pour activer ou désactiver le Contrôle parental

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cochez ou décochez la case **Activer le Contrôle parental**.

Se reporter à "Affichage des journaux" à la page 214.

Norton Internet Security surveille les activités du Contrôle parental sur l'onglet Restrictions du journal des événements. Consultez régulièrement cet onglet pour surveiller l'efficacité des paramètres Contrôle parental.

Personnalisation du Contrôle parental

Les paramètres par défaut du Contrôle parental offrent une protection complète à la majorité des utilisateurs. S'il vous faut ajuster les paramètres du Contrôle parental, vous pouvez ajouter ou supprimer des catégories dans la liste des applications Internet, des groupes de discussion et des sites Web interdits de Norton Internet Security. Vous pouvez aussi exclure du blocage certains sites et groupes de discussion en créant une liste de sites Web et de groupes de discussion autorisés.

Des procédures distinctes permettent de bloquer les sites Web, les groupes de discussion et les programmes.

Restriction de l'accès aux sites Web

Vous pouvez restreindre l'accès aux sites Web de deux manières :

- Bloquer les sites Web par catégorie
  Spécifiez les catégories de sites autorisées et interdites. Vous pouvez également ajouter des sites particuliers à la liste des sites bloqués d'une catégorie ou en supprimer. Cette option permet d'autoriser les utilisateurs à accéder à tous les sites Web, à l'exception de certains types de sites.
- Créer une liste des sites Web auxquels l'accès est autorisé.
  Spécifiez les sites Web que tous les utilisateurs peuvent visiter. Cette option vous permet de contrôler étroitement les activités des utilisateurs sur Internet, puisque tous les sites Web qui ne figurent pas dans la liste sont interdits, quel que soit le type de compte des utilisateurs.

Blocage des sites Web par catégorie

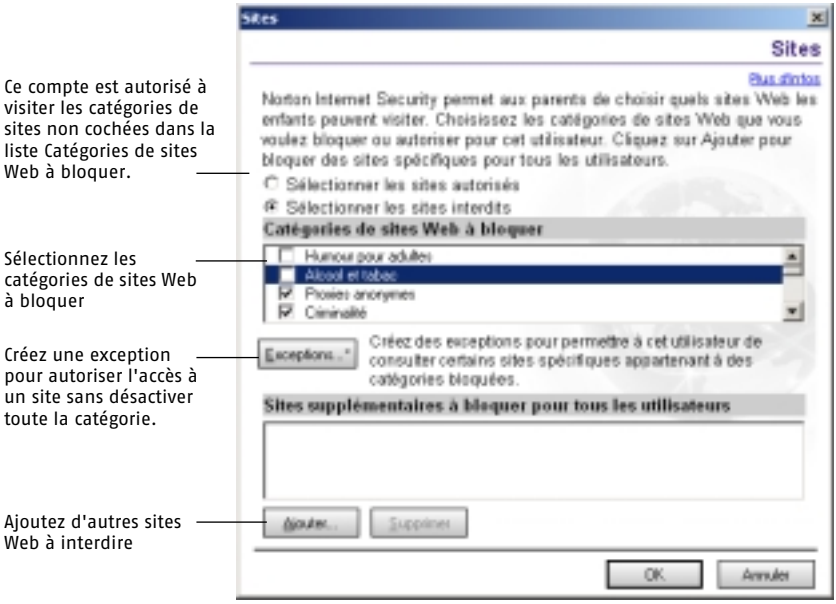
Norton Internet Security comporte une vaste liste de sites Web classés par catégorie. Vous pouvez sélectionner les catégories de sites qui conviennent à chaque compte de votre ordinateur.

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

Avant de bloquer les sites, exécutez LiveUpdate pour vérifier que la liste des sites Web est à jour.

Pour interdire l'accès aux sites Web par catégorie

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Sites**.
5. Dans la fenêtre Choix de sites, cliquez sur **Sélectionner les sites interdits**.



6. Sous Catégories de sites Web à bloquer, cochez les catégories dont vous souhaitez interdire l'accès pour ce compte.
7. Cliquez sur **OK**.
8. Quand vous avez terminé, cliquez sur **OK**.

Blocage de sites supplémentaires

Le Contrôle parental permet d'interdire l'accès à certains sites Web ou domaines qui ne figurent dans aucune des catégories interdites. Si vous bloquez un domaine, tous les sites Web du domaine sont inclus. Par exemple, si vous bloquez le domaine msn.com, le Contrôle parental bloquera tous les sites Web de ce domaine, y compris www.msn.com et messenger.msn.com. Si vous bloquez messenger.msn.com, seul ce site Web sera bloqué.

Pour bloquer ou débloquer l'accès à des sites spécifiques

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Sites**.
5. Dans la fenêtre Sites, cliquez sur **Sélectionner les sites interdits**.
6. Cliquez sur **Ajouter**.
7. Dans la fenêtre Ajout à la liste des sites Web interdits, saisissez l'URL du site à ajouter.
8. Cliquez sur **OK**.
9. Répétez les trois étapes précédentes pour chaque site Web à ajouter.
10. Quand vous avez terminé, cliquez sur **OK**.

Création d'exceptions pour des sites spécifiques

Si des utilisateurs doivent accéder à un site d'une catégorie bloquée, vous pouvez créer une exception pour ce site. Cela vous permet d'autoriser l'accès à certains sites Web appartenant à des catégories interdites, tout en bloquant les autres sites de ce type.

Vous pouvez créer des exceptions pour des sites individuelles ou des domaines entiers. Si vous créez une exception pour un domaine, tous les sites Web du domaine sont inclus. Par exemple, si vous créez une exception pour le domaine msn.com, le Contrôle parental autorisera tous les sites Web de ce domaine, y compris www.msn.com et messenger.msn.com. Si vous autorisez messenger.msn.com, seul ce site Web sera autorisé.

Pour créer des exceptions pour des sites spécifiques

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Sites**.
5. Dans la fenêtre Sites, cliquez sur **Sélectionner les sites interdits**.
6. Cliquez sur **Exceptions**.
7. Dans la fenêtre Exceptions, cliquez sur **Ajouter**.
8. Dans la fenêtre Ajout de sites à la liste, saisissez l'URL du site à ajouter.
9. Cliquez sur **OK**.
10. Répétez les trois étapes précédentes pour chaque site Web à ajouter à la liste d'exceptions.
11. Quand vous avez terminé, cliquez sur **OK**.

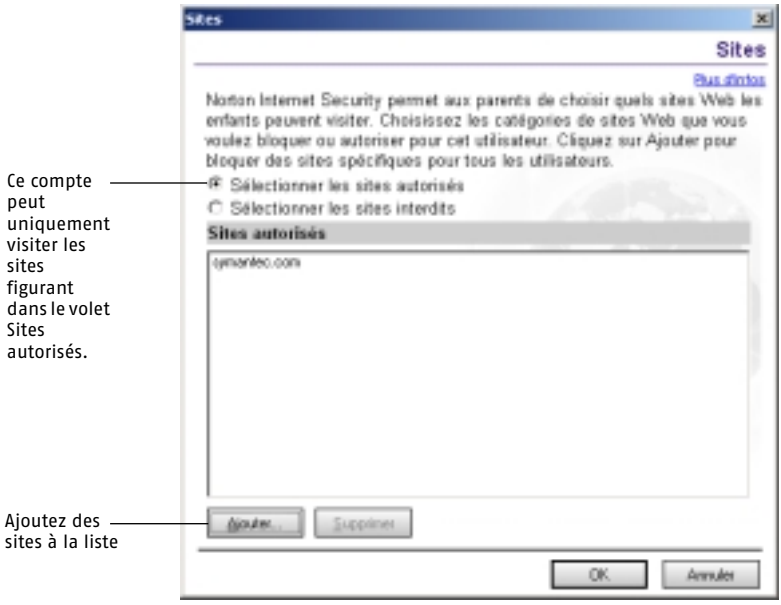
Création d'une liste de sites Web autorisés

Pour contrôler étroitement l'accès au Web des utilisateurs, créez la liste des sites Web dont l'accès est autorisé. Tous les sites qui ne figurent pas sur cette liste sont automatiquement bloqués. Un utilisateur de l'ordinateur ne pourra visiter que les sites approuvés, quel que soit son type de compte.

Pour créer une liste des sites Web autorisés

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Sites**.

5 Dans la fenêtre Classification de sites, choisissez **Sélectionner les sites autorisés**.



6 Cliquez sur **Ajouter** pour créer une nouvelle entrée dans la liste.

7 Dans la fenêtre Ajouter à la liste des sites Web autorisés, saisissez l'URL complète (adresse Web) entière du site à ajouter.
Par exemple, pour autoriser l'accès au site www.ajax.fr, saisissez ajax.fr.

8 Répétez les deux étapes précédentes pour chaque site Web à ajouter.

9 Cliquez sur **OK**.

Soumission de sites Web à Symantec

Symantec actualise régulièrement la liste des sites Web interdits par Norton Internet Security. Pour apporter vos contributions à cette liste, vous pouvez proposer de nouveaux sites, de nouvelles catégories de sites et des sites à supprimer de la liste. Pour proposer des modifications à Symantec, visitez le site http://www.symantec.com/avcenter/cgi-bin/nisurl.cgi.

Restriction des applications qui accèdent à Internet

Les applications se connectent à Internet pour diverses raisons. Votre *navigateur* Web se connecte à Internet pour afficher des pages Web. LiveUpdate accède à Internet pour actualiser les programmes et les protections de Symantec. Microsoft NetMeeting se connecte à Internet pour permettre aux utilisateurs d'organiser des téléconférences.

Si la plupart des tentatives d'accès à Internet sont sans danger, certains *chevaux de Troie* et d'autres programmes téléchargent du code nuisible ou envoient des informations confidentielles. Contrôle parental vous permet de contrôler les modalités selon lesquelles les programmes accèdent à Internet. Contrôle parental peut bloquer certaines catégories de programmes et limiter l'utilisation de certaines autres.

Les limitations des programmes concernent les comptes de type Adolescent et Enfant. Les utilisateurs de type Adulte peuvent neutraliser les restrictions pour chaque programme.

Blocage et autorisation de catégories d'applications Internet

Le Contrôle parental organise les programmes Internet en catégories. Par défaut, les utilisateurs de type Enfant peuvent uniquement se connecter à Internet avec des applications figurant dans les catégories Général, Courrier électronique, Navigateurs Web et Utilisateur. Les catégories sont les suivantes :

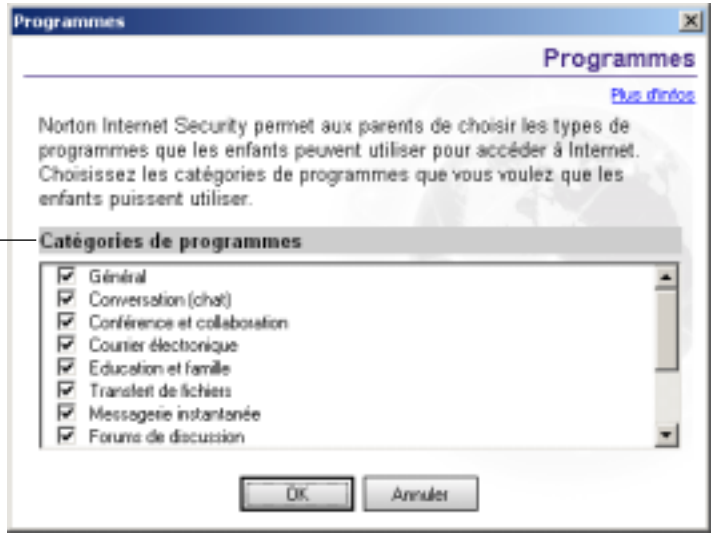
Général	Applications qui ne rentrent dans aucune autre catégorie.
Conversation	Applications permettant d'entrer en conversation avec des personnes ou des groupes, en mode textuel, vocal ou vidéo. Cette catégorie inclut, par exemple, les applications mIRC, Pirch, ICQ, NetMeeting, Internet Phone, Net2Phone et CU-SeeMe. Le blocage de cette catégorie n'empêche pas d'utiliser les sites de discussion Web accessibles par navigateur.
Conférences et collaboration	Applications permettant à plusieurs personnes de communiquer directement. Cette catégorie inclut des applications permettant aux utilisateurs de collaborer grâce à l'utilisation d'un logiciel de tableau blanc (whiteboard) ou de navigateur Web. Exemples : NetMeeting, ICQ, Microsoft Instant Messenger, Yahoo! Messenger et Internet Phone.

Courrier électronique	Applications accédant aux serveurs de messagerie, aussi appelées clients de messagerie. Cette catégorie inclut par exemple Microsoft Outlook Express et Eudora. Le blocage de cette catégorie n'empêche pas d'utiliser les applications de messagerie électronique accessibles par navigateur, comme Hotmail.
Education et famille	Programmes éducatifs accédant à Internet.
Transfert de fichiers	Applications permettant aux utilisateurs de transférer des fichiers depuis et vers leur ordinateur. Cette catégorie comprend par exemple CuteFTP et BulletFTP.
Messagerie instantanée	Applications permettant aux utilisateurs d'envoyer instantanément des messages et des fichiers à d'autres utilisateurs exécutant la même application de messagerie instantanée. Exemples : ICQ, Yahoo! Messenger, Microsoft Instant Messenger et AOL Instant Messenger.
Lecteurs de groupes de discussion	Applications permettant d'accéder aux groupes de discussion. Cette catégorie comprend par exemple Xnews et Agent.
Jeux en réseau	Jeux accédant à un réseau ou à Internet pour permettre à plusieurs utilisateurs de jouer ensemble ou de s'affronter.
Navigateurs Web	Applications permettant aux utilisateurs d'accéder au World Wide Web. Exemples : Microsoft Internet Explorer et Netscape Navigator.
Catégories utilisateur	Catégories supplémentaires dans lesquelles vous pouvez créer d'autres catégories d'applications.

Pour autoriser et interdire des catégories d'applications Internet

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.

4 Cliquez sur **Programmes**.



5 Dans la boîte de dialogue Programmes, sélectionnez les catégories d'applications que ce compte est autorisé à utiliser.

6 Cliquez sur **OK**.

Le blocage de l'accès à Internet d'une application n'empêche pas les utilisateurs d'utiliser l'application. Un programme que Norton Internet Security empêche d'accéder à Internet peut ne plus répondre. Avant de modifier les paramètres des applications, précisez aux utilisateurs que leur ordinateur peut se bloquer s'ils tentent de se connecter à Internet avec des applications interdites.

Restriction de l'accès aux groupes de discussion

Norton Internet Security interdit l'accès aux groupes de discussion en fonction de chaînes de texte, groupes de lettres détectés dans le nom des groupes de discussion.

Lorsque les utilisateurs accèdent à des groupes de discussion, Contrôle parental compare le nom des groupes à une liste de chaînes de texte. Contrôle parental interdit ou autorise l'accès aux groupes de discussion dont le nom contient l'une des chaînes de texte.

Quand des groupes de discussion sont bloqués, les lecteurs de discussion n'incluent pas leur nom dans la liste principale des groupes de discussion auxquels les utilisateurs peuvent accéder. Norton Internet Security bloque automatiquement tout message qu'un utilisateur tente de publier sur un groupe de discussion interdit.

Se reporter à "Pour autoriser et interdire des catégories d'applications Internet" à la page 201.

Par défaut, les utilisateurs de type Enfant ne sont pas autorisés à utiliser les programmes de lecture de discussion. Pour autoriser ces utilisateurs à afficher les groupes de discussion, vous devez lever l'interdiction sur la catégorie des applications de discussion.

A propos des noms des groupes de discussion

Les noms des groupes de discussion deviennent plus spécifiques de la gauche vers la droite. Par exemple, le groupe de discussion alt.histoire est une discussion générale sur les événements et les peuples de l'Histoire. Il contient des discussions plus spécifiques. Le forum alt.histoire.paquebots porte plus particulièrement sur l'histoire des paquebots tandis que alt.histoire.paquebots.titanic traite plus spécifiquement du Titanic.

Vous pouvez utiliser cette structure pour identifier avec précision les groupes de discussion interdits et autorisés. Par exemple, pour interdire le groupe inf.sécurité.piratage.outils (discussion sur les outils de piratage informatique) en autorisant néanmoins les utilisateurs à accéder à inf.sécurité (discussion générale sur les problèmes de sécurité informatique), tapez inf.sécurité.piratage.outils. Cette opération interdit les groupes de discussion dont le nom contient inf.sécurité.piratage.outils et autorise l'accès à tous les autres groupes de discussion commençant par inf.sécurité.

Vous pouvez également interdire ou autoriser des groupes de discussion en utilisant des noms de groupes partiels. Par exemple, vous pouvez bloquer tous les groupes de discussion dont le nom contient le mot sexe en tapant le mot sex dans la liste des groupes de discussion bloqués.

Soyez prudent avec les chaînes de texte courtes. Le filtre des groupes de discussion autorise ou interdit tous les groupes de discussion dont le nom correspond à une chaîne de texte ; vous risquez d'interdire par inadvertance des groupes de discussion auxquels les utilisateurs doivent pouvoir accéder. Par exemple, le mot sex interdit les groupes de discussion dont le nom contient des mots tels que sextant et sexagénaire.

Dans les chaînes de texte, n'utilisez pas de caractères génériques comme les astérisques.

Saisie de chaînes de texte à interdire ou autoriser

Norton Internet Security inclut une liste de chaînes de texte qui bloque les groupes de discussion au contenu contestable. Vous pouvez ajouter des chaînes pour adapter le Contrôle parental à votre famille.

Chaque ordinateur ne peut comporter qu'une seule liste de groupes de discussion autorisés ou interdits.

Pour saisir les chaînes de texte à interdire ou autoriser

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Groupes de discussion**.
5. Dans la fenêtre Groupes de discussion, sélectionnez l'action appropriée. Les options sont les suivantes :

Spécifier les groupes de discussion autorisés	Identifie les chaînes de texte à autoriser.
Spécifier les groupes de discussion bloqués	Identifie les chaînes de texte à bloquer.

6 Cliquez sur **Ajouter**.

7 Saisissez une chaîne de texte à bloquer ou autoriser.

8 Cliquez sur **OK**.

Création d'exceptions aux groupes de discussion interdits

Si vous créez une liste de sites interdits, vous risquez d'interdire l'accès à un groupe de discussion dont les utilisateurs ont besoin. Le Contrôle parental vous permet de créer des exceptions pour donner accès à des groupes bloqués spécifiques. Par exemple, vous pouvez interdire l'accès à tous les groupes de discussion inf.sécurité à l'exception de inf.sécurité.parefeu.

Pour créer des exceptions aux groupes de discussion interdits

1. Démarrez Norton Internet Security.
2. Cliquez deux fois sur **Contrôle parental**.
3. Dans la fenêtre Contrôle parental, sélectionnez le compte à modifier dans la liste déroulante Paramètres du Contrôle parental pour.
4. Cliquez sur **Groupes de discussion**.
5. Dans la fenêtre Groupes de discussion, cliquez sur **Spécifiez les groupes de discussion bloqués**.
6. Cliquez sur **Exceptions**.
7. Cliquez sur **Ajouter**.
8. Dans la fenêtre Exceptions de la liste des groupes de discussion bloqués, saisissez le nom entier du groupe de discussion dont vous souhaitez lever l'interdiction.
9. Cliquez sur **OK**.
10. Quand vous avez terminé, cliquez sur **OK**.

Contrôle de Norton Internet Security

15

Norton Internet Security tient des enregistrements de toutes les connexions Internet entrantes et sortantes et de toutes les actions exécutées par le programme pour protéger votre ordinateur. Consultez périodiquement ces informations afin d'identifier les problèmes éventuels.

Quatre sources d'informations sur Norton Internet Security sont disponibles :

Fenêtre Statut et paramètres	Informations de base sur les fonctions de protection actives.
Fenêtre Statistiques	Informations récentes relatives au pare-feu et aux activités de blocage de contenu.
Fenêtre Statistiques détaillées	Statistiques détaillées sur l'activité du réseau et les actions exécutées par Norton Internet Security.
Journal des événements	Activités des utilisateurs sur Internet et actions exécutées par Norton Internet Security.

Lorsque vous examinez les informations consignées, recherchez :

- les attaques récentes dans la fenêtre Paramètres d'état
- les refus d'accès multiples, particulièrement ceux correspondant à une même adresse *IP address*
- les séries de *numéros de port* émanant de la même adresse IP, indiquant éventuellement un *sondage de ports*
- une activité réseau excessive due à des programmes inconnus
- les alertes de virus récentes.

Les tentatives d'accès refusées sont normales si elles sont aléatoires, c'est-à-dire si elles ne proviennent pas de la même adresse IP et si elles ne concernent pas une séquence de numéros de port. Vous pouvez également constater des tentatives d'accès consignées en raison d'une activité sur votre ordinateur, comme la connexion à un serveur FTP ou l'envoi de *courrier électronique*.

Si vous vous trouvez dans l'une des situations énoncées ci-dessus, il peut s'agir d'une preuve d'une attaque ou d'une infection de virus.

Fenêtre Statut et paramètres

La fenêtre Statut et paramètres fournit un cliché de la protection de votre ordinateur. Vous pouvez vérifier rapidement les fonctions de protection actives, identifier les trous de sécurité et personnaliser Norton Internet Security.

Pour afficher la fenêtre Statut et paramètres

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Statut et paramètres**.
3. Pour modifier des paramètres, cliquez deux fois sur une fonction de protection.

Affichage de la fenêtre Statistiques

La fenêtre Statistiques fournit un instantané de l'activité *réseau* de votre ordinateur depuis le dernier démarrage de Windows. Ces informations permettent d'identifier les tentatives d'attaques en cours et de vérifier comment les paramètres de Confidentialité et de Contrôle parental influent sur la protection de votre ordinateur.

La fenêtre Statistiques fournit des informations sur :

Pare-feu personnel	Toutes les attaques récentes sur cet ordinateur, notamment l'heure de la dernière attaque et l'adresse de l'ordinateur à l'origine de l'attaque.
Blocage de contenu en ligne	Nombre de cookies, publicités Web et messages spam bloqués et nombre de fois où les informations confidentielles ont été bloquées
Contrôle parental	Sites Web et applications bloqués

Pour afficher la fenêtre Statistiques

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.

Réinitialisation des informations de la fenêtre Statistiques

Norton Internet Security efface automatiquement toutes les informations de la fenêtre Statistiques quand vous redémarrez Windows. Vous pouvez également effacer les statistiques manuellement. Cette opération peut s'avérer utile pour déterminer l'incidence sur les statistiques d'une modification de la configuration.

Pour réinitialiser les informations de la fenêtre Statistiques

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Statistiques**.

3 Dans la fenêtre Statistiques, cliquez sur **Effacer les statistiques**.

Affichage des statistiques détaillées

Outre les statistiques globales de la fenêtre Statistiques, Norton Internet Security tient à jour des compteurs réseau en temps réel qui suivent l'usage d'Internet par les utilisateurs et toute action exécutée par Norton Internet Security.

Les statistiques détaillées fournissent les informations suivantes.

Réseau	Octets TCP et UDP envoyés et reçus, nombre de connexions réseau ouvertes et nombre le plus élevé de connexions réseau ouvertes simultanément depuis le démarrage du programme
Navigation	Graphiques, cookies et demandes d'informations sur le navigateur bloqués, nombre d'octets et de paquets traités, et nombre de connexions HTTP
Images Web/ bannières publicitaires bloquées	Taille approximative des graphiques bloqués et gain de temps réalisé en ne chargeant pas les graphiques bloqués
Filtrage des connexions TCP	Nombre de connexions TCP bloquées et autorisées
Filtrage des datagrammes UDP	Nombre de connexions UDP bloquées et autorisées
Règles de filtrage	Toutes les règles définies pour le pare-feu et informations sur le nombre de tentatives de communication bloquées, autorisées ou ne correspondant pas aux règles de filtrage
Connexions réseau	Informations relatives aux connexions courantes, notamment l'application utilisant la connexion, le protocole utilisé et l'adresse ou le nom des ordinateurs connectés
Dernières 60 secondes	Nombre de connexion réseau et HTTP ainsi que la vitesse de chaque type de connexion

Pour afficher les statistiques détaillées

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.

Réinitialisation des statistiques détaillées

Réinitialisez les compteurs afin d'effacer toutes les statistiques et de recommencer à les enregistrer. Cette opération peut s'avérer utile pour déterminer l'incidence sur les statistiques d'une modification de la configuration.

Pour réinitialiser les compteurs

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans le menu Affichage, choisissez **Réinitialiser les valeurs**.

Définition des statistiques affichées dans la fenêtre Statistiques détaillées

Les utilisateurs peuvent afficher toutes les statistiques détaillées à la fois ou seulement certaines catégories.

Pour définir les statistiques affichées dans la fenêtre Statistiques détaillées

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, cliquez sur **Options** dans le menu Affichage.
5. Dans la fenêtre Options sur les statistiques de Norton Internet Security, sélectionnez une ou plusieurs catégories de statistiques à afficher.
6. Cliquez sur **OK**.

Configuration des colonnes de la fenêtre Statistiques détaillées

La fenêtre Statistiques détaillées permet d'afficher les informations sur une ou deux colonnes. Ces deux présentations contiennent les mêmes statistiques.

Pour configurer les colonnes de la fenêtre Statistiques détaillées

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, effectuez l'une des opérations suivantes :
   - Pour adapter automatiquement le nombre de colonnes en fonction de la largeur de la fenêtre active, sélectionnez **Colonnes** > **Automatique** dans le menu Affichage.
   - Pour afficher toujours une seule colonne, sélectionnez **Colonnes** > **Une** dans le menu Affichage.
   - Pour afficher toujours deux colonnes, sélectionnez **Colonnes** > **Deux** dans le menu Affichage.

Fenêtre Statistiques détaillées toujours visible

Vous pouvez afficher la fenêtre Statistiques détaillées au premier plan, même si une application s'exécute dans une fenêtre plein écran. Cela peut s'avérer utile pour détecter une activité réseau inhabituelle susceptible d'indiquer un problème de sécurité.

Pour que la fenêtre Statistiques détaillées reste toujours visible

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, cliquez sur **Toujours visible** dans le menu Affichage.

Affichage des journaux de Norton Internet Security

Norton Internet Security consigne des informations sur les sites Web visités par les utilisateurs, les actions du pare-feu et toute alerte déclenchée. Les *journaux* incluent des détails sur une partie de l'activité rapportée dans la fenêtre Statistiques.

Les journaux sont organisés en 14 onglets.

Onglet	Information
Alertes de virus	Détails sur les virus ou chevaux de Troie détectés sur votre ordinateur.
Activités d'application	Historique de toutes les actions effectuées par Norton AntiVirus pour protéger votre ordinateur.
Erreurs	Informations sur tout problème rencontré par Norton AntiVirus pendant la recherche de virus sur votre ordinateur.
Blocage de contenu	Détails sur les publicités, les images, les applets Java et les contrôles ActiveX bloqués par Norton Internet Security.
Connexions	Historique de toutes les connexions réseau TCP/IP établies avec cet ordinateur et indiquant la date et l'heure de la connexion, l'adresse de l'ordinateur auquel vous vous êtes connecté, le service ou le numéro de port utilisé, la quantité d'informations transférée et la durée totale de la connexion.
Pare-feu	Communications interceptées par le pare-feu, incluant les règles appliquées, les alertes affichées, les ports inutilisés bloqués et les événements AutoBlock.
Détection d'intrusion	Etat de la détection d'intrusion (active ou inactive), signatures d'attaques contrôlées et nombre d'intrusions bloquées.
Confidentialité	Cookies bloqués, avec le nom du cookie et celui du site Web qui a demandé le cookie.
Informations confidentielles	Historique de toutes les informations confidentielles protégées envoyées sur Internet.
Restrictions	Programmes Internet, groupes de discussion et sites Web bloqués par Norton Internet Security.
Système	Erreurs système graves, état courant du filtrage IP, si le programme connecté a démarré en tant que service Windows, programmes utilisant trop de ressources ou ne fonctionnant pas dans des conditions optimales.

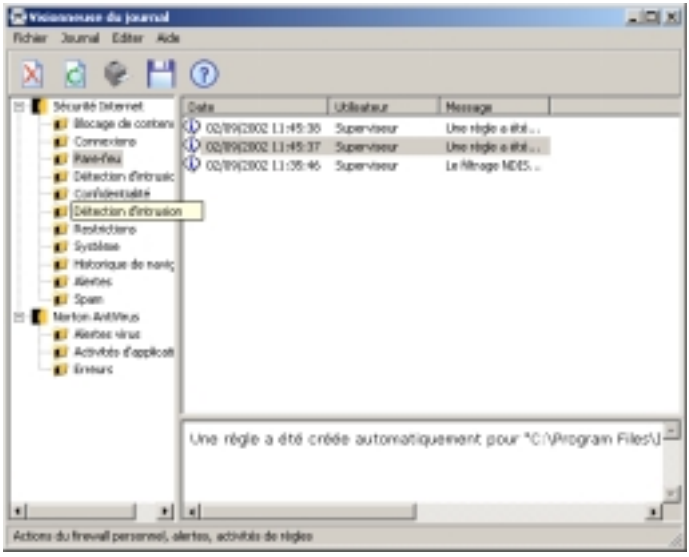
Onglet	Information
Historique de navigation	URL visitées par l'ordinateur, fournissant un historique de l'activité Web.
Alertes	Toutes les activités d'alerte déclenchées par d'éventuelles attaques sur votre ordinateur.
Spam	Détails sur les courriers électroniques identifiés comme spam par l'Alerte spam.

Affichage des journaux

Affichez les journaux Norton Internet Security depuis la fenêtre Statistiques.

Pour afficher les journaux

1. Ouvrez Norton Internet Security.
2. Effectuez l'une des opérations suivantes :
   - Dans Security Center, cliquez sur **Statistiques** > **Afficher les journaux** .
   - Dans Security Monitor, cliquez sur **Afficher le journal** dans le menu Sélectionner une tâche.



3 Dans la fenêtre Afficheur du journal, sélectionnez le journal à consulter.

4 Quand vous avez terminé, cliquez sur un autre journal ou cliquez sur **OK** pour fermer l'Afficheur.

Actualisation des journaux

Les journaux sont automatiquement actualisés lorsque vous passez de l'un à l'autre. Pour afficher les événements *réseau* qui se sont produits depuis que vous avez commencé à consulter l'Afficheur, vous pouvez actualiser manuellement tous les journaux ou des journaux individuels.

Pour actualiser tous les journaux à la fois

1 Dans l'Afficheur du journal, sélectionnez l'une des options suivantes :
   - Norton Internet Security
   - Norton AntiVirus

2 Cliquez sur **Actualiser toutes les catégories**.

Pour actualiser un journal individuel

❖ Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à actualiser, puis cliquez sur **Actualiser la catégorie**.

Désactivation de la consignation

Vous pouvez choisir les types d'informations que Norton Internet Security suit dans les journaux. Par défaut, Norton Internet Security suit les événements de toutes les catégories. Vous pouvez désactiver des journaux individuels si vous n'avez pas besoin des informations qu'ils contiennent.

Pour désactiver la consignation

1 Ouvrez Norton Internet Security.

2 Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.

3 Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.

4 Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à désactiver, puis cliquez sur **Désactiver la consignation**.

Purge des journaux

Si vous utilisez Internet de façon intense ou si d'autres ordinateurs se connectent régulièrement au vôtre, vos fichiers journaux peuvent contenir des informations sur des centaines de *connexions*. Ce facteur risque de compliquer l'identification d'activités spécifiques ou l'évaluation de l'impact de toute modification apportée aux paramètres de Norton Internet Security.

Purgez les journaux afin de supprimer les informations sur d'anciennes connexions. Cette opération permet de constater la façon dont les changements de paramètres affectent votre protection. Vous pouvez purger un seul journal ou tous les journaux à la fois.

Pour supprimer un seul journal

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à purger, puis cliquez sur **Purger la catégorie**.

Pour purger tous les journaux à la fois

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, sélectionnez l'une des options suivantes :
   - Norton Internet Security
   - Norton AntiVirus
5. Cliquez sur **Actualiser toutes les catégories**.

Modification de la taille des journaux

Norton Internet Security stocke les informations de chaque journal dans un fichier distinct. Vous pouvez modifier la taille de ces fichiers afin de contrôler l'espace disque qu'ils occupent. Lorsque les fichiers atteignent leur taille maximale, les nouveaux événements remplacent les plus anciens.

Par défaut, la taille des fichiers journaux est de 64 Ko à 512 Ko. Pour que les informations couvrent une période plus longue, augmentez la taille du journal. Si vous avez besoin de libérer de l'espace sur le disque dur, réduisez cette taille. Le changement de taille d'un fichier journal efface toutes les informations qu'il contient.

Pour modifier la taille d'un journal

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur, cliquez avec le bouton droit de la souris sur un journal, puis cliquez sur **Changer la taille du fichier journal**.
   La boîte de dialogue Taille de fichier journal affiche la taille actuelle du journal.
5. Dans la boîte de dialogue Taille de fichier journal, sélectionnez une nouvelle taille de fichier.
6. Cliquez sur **OK**.

Réglage de la largeur d'une colonne

Vous pouvez modifier la largeur des colonnes dans le journal des événements.

Réglage de la largeur d'une colonne

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, sur l'onglet à afficher, pointez sur la bordure à droite du titre de la colonne.
   Le curseur prend la forme d'une croix.
5. Faites glisser la bordure de la colonne pour redimensionner cette dernière.

Impression ou enregistrement des journaux et des statistiques

Lorsque vous accédez à Internet, les informations les plus anciennes des *journaux* et des statistiques sont remplacées par des données plus récentes. Pour conserver les anciennes informations sur l'utilisation d'Internet ou pour transférer ces informations dans un traitement de texte ou un autre document, imprimez ou exportez le journal des événements et les statistiques.

Pour imprimer des informations de journal

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à imprimer, puis cliquez sur **Imprimer la catégorie**.

Pour imprimer des informations statistiques

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, cliquez sur **Imprimer** dans le menu Fichier.
5. Dans la fenêtre d'impression, cliquez sur **Imprimer**.

Pour enregistrer des informations de journal dans un fichier texte

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Afficher les journaux**.
4. Dans l'Afficheur du journal, cliquez avec le bouton droit de la souris sur le journal à enregistrer, puis cliquez sur **Exporter la catégorie sous**.
5. Indiquez l'emplacement et le nom du fichier texte.
6. Cliquez sur **Enregistrer**.

Pour enregistrer les statistiques dans un fichier texte

1. Ouvrez Norton Internet Security.
2. Dans la fenêtre principale de Security Center, cliquez sur **Statistiques**.
3. Dans la fenêtre Statistiques, cliquez sur **Statistiques détaillées**.
4. Dans la fenêtre Statistiques détaillées, cliquez sur **Enregistrer** dans le menu Fichier.
5. Indiquez l'emplacement et le nom du fichier texte.
6. Cliquez sur **Enregistrer**.

Dépannage de Norton Internet Security

A

Les informations de ce chapitre vous permettent de résoudre les problèmes les plus courants. Si vous ne trouvez pas ici la solution au problème, vous trouverez sur le site Web de Symantec une véritable mine d'informations. Vous y trouverez des mises à jour, des correctifs, des didacticiels en ligne, des articles de base de connaissances et des outils de suppression de virus.

Pour explorer le site Web de support technique Symantec

1. Accédez au site www.symantec.fr/frsupport/.
2. Sur la page Web Service et support, cliquez sur la catégorie d'utilisateur dont vous faites partie.
3. Sur la page d'accueil, cliquez sur le lien vers les informations qui vous intéressent.

Si vous ne trouvez pas ce que vous cherchez avec les liens, lancez une recherche sur le site.

Pour explorer le site Web de support technique Symantec

1. Du côté gauche d'une fenêtre du site Symantec, cliquez sur **Chercher**.
2. Tapez un mot ou une phrase correspondant aux informations que vous cherchez. Suivez ces consignes pour rechercher des informations sur le site de Symantec :
   - Tapez un terme unique en minuscules pour trouver toutes les correspondances du terme, y compris les correspondances partielles. Par exemple, tapez install pour trouver les articles contenant le terme installe, installation, installer, etc.

- Tapez plusieurs termes pour trouver toutes les occurrences de n'importe quel terme. Par exemple, tapez définitions virus pour trouver les articles contenant définitions, virus ou les deux termes.
- Tapez une phrase entre guillemets pour trouver les articles contenant la phrase exacte.
- Utilisez le signe plus (+) devant tous les termes de recherche pour trouver les articles contenant tous les termes. Par exemple, tapez +Internet +Security pour trouver les articles contenant les deux termes.
- Pour rechercher une correspondance exacte, tapez les termes recherchés en majuscules.
- Pour rechercher des phrases multiples, encadrez chacune avec des guillemets et séparez-les avec des virgules. Par exemple, "achat de produits", "MAC", "Norton SystemWorks" recherche les trois phrases et trouve tous les articles contenant l'une des trois.

3 Sélectionnez la zone du site Web sur laquelle vous voulez mener la recherche.

4 Cliquez sur **Chercher**.

Dépannage des problèmes de Norton Internet Security

Consultez l'onglet Sommaire pour des solutions aux problèmes éventuels de Norton Internet Security.

Quel est le problème avec ce site Web ?

Norton Internet Security peut bloquer certains éléments d'un site Web et empêcher l'affichage correct des données dans le navigateur Web. Dans certains cas, l'accès au site est impossible.

Dans la plupart des cas, Norton Internet Security vous protège contre les contenus inconvenants. Votre meilleure solution est peut-être d'aller sur un autre site plus approprié.

Se reporter à "Désactivation temporaire de Norton Internet Security" à la page 73.

Si vous êtes Superviseur, vous pouvez désactiver Norton Internet Security et essayer de nouveau d'accéder au site Web. Rappelez-vous que quand vous désactivez Norton Internet Security, votre ordinateur est vulnérable aux attaques par Internet.

Si vous ne parvenez toujours pas à vous connecter au site Web avec Norton Internet Security désactivé, il se peut que le problème soit lié à Internet ou à votre *fournisseur d'accès Internet*.

Problème	Solution
Il peut s'agir du Blocage des cookies	De nombreux sites Web nécessitent pour s'afficher correctement que les cookies soient activés sur l'ordinateur. Se reporter à "Modification du paramètre Blocage des cookies" à la page 171.
Il peut s'agir du Contrôle parental	Si vous avez configuré le Contrôle parental pour bloquer certaines catégories de sites Web, il bloque peut-être actuellement le site que vous tentez de visiter. Quand le Contrôle parental bloque un site, il affiche toujours un message pour vous le signaler. Se reporter à "Restriction de l'accès aux sites Web" à la page 195.
Il peut s'agir d'une règle de filtrage.	Une règle de filtrage peut bloquer le site Web. Si c'est le cas, vous verrez probablement un message indiquant que la connexion n'a pu être établie. Se reporter à "Personnalisation de la protection du pare-feu" à la page 107.
Il peut s'agir du Blocage des publicités	Le blocage de publicités sur Internet empêche parfois un site Web tout entier de s'afficher dans votre navigateur. Se reporter à "Blocage des publicités sur Internet" à la page 175.
Il peut s'agir du Blocage ActiveX ou Java.	Certains sites Web n'affichent que des contrôles ActiveX ou des applets Java. Si vous les bloquez, aucun élément ne sera affiché sur ces sites. Se reporter à "Modification de paramètres de sécurité individuels" à la page 109.
Il peut s'agir du Blocage Flash	Certains sites Web utilisent Macromedia Flash pour créer des pages d'accueil interactives. Si vous bloquez Flash, aucun élément ne sera affiché sur ces sites. Se reporter à "Activation ou désactivation du Blocage Flash" à la page 178.

Pourquoi ne puis-je pas publier des informations en ligne ?

Se reporter à "Identification des informations confidentielles à protéger" à la page 166.

Si vous ne parvenez pas à publier des informations sur un site Web, vérifiez si la fonction Confidentialité bloque ces informations. Vérifiez dans la liste Informations confidentielles de la fenêtre Confidentialité si les données que vous souhaitez saisir sont bloquées.

Pourquoi un courrier électronique que j'ai envoyé n'est-il jamais arrivé ?

Si vous choisissez de bloquer un *courrier électronique* contenant des informations confidentielles, Norton Internet Security supprime immédiatement le message. Votre programme de messagerie indiquera que le courrier a été envoyé mais le destinataire ne le recevra pas.

Si votre programme de messagerie enregistre le courrier sortant, vous pouvez ouvrir le dossier Eléments envoyés, modifier le message et l'envoyer.

Pourquoi un programme ne se connecte-t-il pas à Internet ?

Un utilisateur de type Enfant ou Adolescent peut être incapable d'utiliser une application pour se connecter à Internet pour l'une des raisons suivantes :

L'application appartient à une catégorie bloquée pour ce compte.	Se reporter à "Restriction des applications qui accèdent à Internet" à la page 200.
Il n'y a aucune règle de filtrage permettant à l'application de créer une connexion à Internet.	Se reporter à "Réponse aux alertes de Norton Internet Security" à la page 55.
Il se peut que Norton Internet Security empêche votre compte d'utiliser cette application sur Internet.	Se reporter à "Protection des enfants avec le Contrôle parental" à la page 193.

Si un enfant ou un adolescent a besoin d'utiliser ce programme, un superviseur peut ajuster les paramètres du Contrôle parental.

Pourquoi Norton Internet Security ne m'envoie-t-il pas d'avertissement avant d'autoriser des applications à accéder à Internet ?

Si le Contrôle automatique des programmes est activé, Norton Internet Security crée des règles pour les applications reconnues sans vous en avertir.

Se reporter à "Activation du Contrôle des programmes automatique" à la page 114.

Pourquoi ne puis-je pas imprimer vers une imprimante partagée ou me connecter à un ordinateur du réseau local ?

Norton Internet Security bloque l'utilisation du réseau Microsoft afin d'éviter une connexion à votre ordinateur depuis Internet.

Pour autoriser l'utilisation du réseau local, notamment le partage de fichiers et d'imprimantes, placez les ordinateurs du réseau dans la zone Approuvés.

Se reporter à "Organisation des ordinateurs en zones de réseau" à la page 93.

Pourquoi ne puis-je pas me connecter à Internet par l'intermédiaire d'un modem câble ?

Si votre réseau accède à Internet au moyen d'une *connexion* par câble, vous aurez peut-être besoin de rendre visible le nom NetBIOS de votre ordinateur. Le nom NetBIOS est visible, mais les fichiers et les dossiers de l'ordinateur restent cachés.

Pour rendre visible le nom NetBIOS

1. Ouvrez Norton Internet Security.
2. Dans Security Center, cliquez deux fois sur **Personal firewall**.
3. Dans la fenêtre Personal firewall, cliquez sur **Règles générales** sur l'onglet Avancé.
4. Dans la boîte de dialogue Règles générales, cliquez sur **Nom NetBIOS entrant par défaut**.
5. Cliquez sur **Modifier**.
6. Sur l'onglet Action de la boîte de dialogue Modifier une règle, cliquez sur **Autoriser l'accès à Internet**.

7 Cliquez sur **OK**.

8 Dans la boîte de dialogue Règles générales, cliquez sur **OK**.

9 Dans la fenêtre Personal firewall, cliquez sur **OK**.

Certains fournisseurs de services Internet analysent les ports sur les ordinateurs des utilisateurs afin de s'assurer qu'ils respectent les accords de niveau de service. Norton Internet Security peut considérer cette opération comme une *analyse de port* malveillante et interrompre les communications avec le système câble. Si c'est le cas, vous devrez laisser votre opérateur exécuter des analyses de port.

Pour autoriser les analyses de port du FAI

1 Ouvrez Norton Internet Security.

2 Dans Security Center, cliquez deux fois sur **Détection d'intrusion**.

3 Dans la fenêtre Détection d'intrusion, cliquez sur **Adresse IP**.

4 Dans la boîte de dialogue Exclusions, sélectionnez l'adresse IP utilisée par votre FAI pour les analyses de port.
Renseignez-vous auprès de votre FAI pour connaître l'adresse IP utilisée.

5 Cliquez sur **Exclure**.

6 Cliquez sur **OK**.

Pourquoi LiveUpdate n'obtient-il pas de liste de mises à jour ?

La première fois que vous lancez LiveUpdate après l'installation de Norton Internet Security, une alerte d'accès à Internet apparaît afin de vous aider à définir une règle qui autorise LiveUpdate à accéder à Internet. Les utilisateurs de type Enfant et Adolescent ne peuvent pas créer ces règles.

Connectez-vous à un compte Adulte ou Superviseur et exécutez LiveUpdate. Cette opération crée des règles permettant à quiconque d'exécuter LiveUpdate.

Comment un site Web peut-il accéder aux informations sur mon navigateur ?

Les paramètres de Confidentialité de navigation empêchent le navigateur de transmettre des informations le concernant. Toutefois, certains sites de diagnostic sur Internet peuvent accéder aux informations sur le navigateur, même si les paramètres de Confidentialité de navigation sont activés pour les bloquer.

Si vous avez bloqué les *applets Java*, les *contrôles ActiveX* ou les scripts, il est possible que le site utilise l'une de ces méthodes pour lire ces informations. Parfois, lorsque des serveurs Web n'accèdent pas aux informations sur le navigateur, ils utilisent les dernières informations reçues. Dans ce cas, vous pourrez voir les informations de la dernière personne qui a visité le site.

Résolution des problèmes de Norton AntiVirus

Consultez l'onglet Sommaire pour des solutions aux problèmes éventuels de Norton AntiVirus.

Ma disquette de sauvetage ne fonctionne pas

Du fait du nombre de technologies spécifiques utilisées par les fabricants pour configurer et initialiser les disques durs, le programme Rescue ne peut pas toujours créer automatiquement un disque d'amorçage. Si votre disquette d'amorçage de sauvetage ne fonctionne pas correctement, effectuez l'une des opérations suivantes :

- Si vous avez une disquette d'amorçage spéciale pour l'ordinateur, ajoutez-la au jeu de disquettes de sauvetage. En cas d'urgence, démarrez à partir de cette disquette. Retirez la disquette du lecteur et remplacez-la par la disquette d'amorçage de sauvetage. A l'invite du DOS, tapez **A:RSHELL**, appuyez sur Entrée et suivez les instructions affichées à l'écran.
- Utilisez Disk Manager ou un programme de nom similaire fourni avec votre ordinateur pour rendre votre disquette de sauvetage amorçable. Veillez à tester votre disquette d'amorçage de sauvetage après sa modification.

Il arrive que le disque d'amorçage de sauvetage ne fonctionne pas correctement si plusieurs *systèmes d'exploitation* sont installés, comme Windows 2000 et Windows 98.

Pour modifier la disquette d'amorçage de sauvetage

1. Démarrez à partir du disque dur.
2. Insérez la disquette d'amorçage de sauvetage dans le lecteur A.
3. A l'invite du DOS, tapez **SYS A:**.
4. Appuyez sur **Entrée**.
   Cette opération transfère le système d'exploitation sur la disquette d'amorçage de sauvetage. Veillez à tester de nouveau vos disquettes de sauvetage.

Une alerte me demande d'utiliser mes disquettes de sauvetage, mais je n'en ai pas créé

Se reporter à "Création de disquettes d'urgence" à la page 30.

Le CD-ROM Norton Internet Security vous permet de créer des disquettes d'urgence. Bien qu'elles n'offrent pas des fonctionnalités aussi puissantes que celles des disquettes de sauvetage, vous pouvez les utiliser dans la plupart des situations d'urgence.

Se reporter à "Si vous utilisez le CD comme disquette d'urgence" à la page 149.

Vous pouvez utiliser le CD de Norton AntiVirus comme disque d'urgence si votre ordinateur peut démarrer depuis le lecteur de CD-ROM.

Une fois les disquettes d'urgence créées, utilisez-les pour résoudre le problème.

Impossible de démarrer depuis le lecteur A

Si l'ordinateur n'accède pas d'abord au lecteur A lors du démarrage, utilisez le programme Setup du BIOS pour modifier les paramètres.

Soyez prudent lorsque vous modifiez des paramètres via le programme Setup de l'ordinateur. Si vous ne l'avez jamais utilisé auparavant, il est sans doute préférable de vous reporter à la documentation du fabricant de l'ordinateur.

Pour modifier les paramètres de l'ordinateur

1. Redémarrez votre ordinateur.>Un message vous indique les touches à enfoncer pour exécuter SETUP, par exemple Appuyez sur <SUPPR> pour exécuter SETUP".
2. Appuyez sur ces touches pour lancer le programme Setup.

3 Paramétrez la séquence d'amorçage sur le lecteur A, puis sur le lecteur C.
Les programmes de configuration varient d'un fabricant à l'autre. Si vous ne trouvez pas l'option de séquence d'amorçage, utilisez le système d'aide du programme Setup, reportez-vous à la documentation fournie avec le système ou contactez son fabricant.

4 Enregistrez les modifications et quittez le programme Setup.

Vous pouvez être amené à utiliser une disquette d'amorçage spéciale à la place de la disquette d'amorçage de sauvetage. Si c'est le cas, utilisez la disquette de démarrage ou d'amorçage fournie avec l'ordinateur.

Si l'ordinateur est équipé de plusieurs systèmes d'exploitation, comme Windows 2000 et Windows 98, vous pouvez être amené à modifier le disque d'amorçage de sauvetage.

Auto-Protect ne se charge pas au démarrage de l'ordinateur

Si l'icône de Norton AntiVirus Auto-Protect n'apparaît pas dans l'angle droit de la barre des tâches de Windows, la protection automatique n'est pas chargée. Il y a trois raisons probables à cette situation :

Vous avez peut-être lancé Windows en mode Sans échec. Windows redémarre en mode sans échec si l'arrêt précédent a échoué. Par exemple, vous avez mis l'ordinateur hors tension sans choisir Arrêter dans le menu Démarrer de Windows.

Pour redémarrer Windows

1 Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Arrêter**.

2 Dans la boîte de dialogue Arrêt de Windows, cliquez sur **Redémarrer**.

3 Cliquez sur **OK**.

Norton Internet Security n'est peut-être pas configuré pour lancer automatiquement Auto-Protect.

Pour configurer Auto-Protect en vue d'un démarrage automatique

1 Démarrez Norton Internet Security.

2 Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.

3 Dans la fenêtre Options, sous Système, cliquez sur **Auto-Protect**.

4 Vérifiez que l'option Lancer Auto-Protect au démarrage de Windows est cochée.

Norton Antivirus n'est peut être pas configuré pour faire apparaître l'icône d'Auto-Protect dans la barre d'état système.

Pour afficher l'icône Auto-Protect dans la barre d'état système

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la fenêtre Options, sous Système, cliquez sur **Auto-Protect**.
4. Vérifiez que l'option Montrer l'icône Auto-Protect dans la corbeille système est cochée.

J'ai effectué une analyse et supprimé un virus, mais il continue d'infecter mes fichiers

Il existe quatre causes possibles de réapparition d'un virus.

Le virus se trouve peut-être dans un fichier programme portant une extension inhabituelle, que Norton AntiVirus n'est pas configuré pour rechercher.

Pour réinitialiser les options d'analyse de Norton AntiVirus

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la fenêtre Options, sous Système, cliquez sur **Analyses manuelles**.
4. Dans la zone Types de fichier à analyser, cliquez sur **Tous les fichiers**.
5. Cliquez sur **Analyses manuelles** > **Bloodhound**.
6. Vérifiez que la fonction Activer heuristiques Bloodhound est cochée, et cliquez sur **Niveau de protection le plus élevé**.
7. Cliquez sur **OK**.
8. Analysez tous les disques que vous utilisez et réparez tous les fichiers infectés.

La source de l'infection peut également être une disquette. Analysez toutes les disquettes que vous utilisez pour vous assurer qu'elles sont exemptes de virus.

Se reporter à "Si vous devez utiliser les disques de sauvetage (Windows 98/98SE/Me)" à la page 148.

Il est également possible que le virus reste en mémoire après sa suppression de la *zone amorce*. Si tel est le cas, il infecte à nouveau votre zone amorce. Utilisez les disquettes de sauvetage pour supprimer le virus.

Si le problème concerne un cheval de Troie ou un ver transmis par un disque partagé en *réseau*, vous devez vous déconnecter du réseau ou protéger le disque par un mot de passe pour que Norton AntiVirus puisse éliminer le problème.

Norton AntiVirus ne peut pas réparer mes fichiers infectés

Se reporter à "Mises à jour avec LiveUpdate" à la page 83.

La raison la plus courante pour laquelle Norton AntiVirus ne peut pas réparer vos *fichiers infectés* est que vous n'avez pas la protection antivirus la plus récente sur votre ordinateur. Actualisez régulièrement votre protection antivirus pour protéger l'ordinateur contre les nouveaux virus.

Si l'utilisation de LiveUpdate ne permet pas d'éliminer le virus, le fichier est peut-être endommagé ou contient un autre virus. Il y a deux options supplémentaires :

Se reporter à "Si des fichiers sont en quarantaine" à la page 145.

- Mettre le fichier en quarantaine et le transmettre à Symantec.
- S'il existe une copie non infectée du fichier, supprimer le fichier infecté et le remplacer par la sauvegarde.

Je reçois un message d'erreur lors du test du jeu de disques de sauvetage de base

Si vous obtenez le message "Disque non système. Remplacez et appuyez sur une touche" pendant le test des disquettes de sauvetage, Rescue n'a peut-être pas correctement préparé les fichiers d'amorçage des disquettes.

Pour corriger le problème sans avoir à reformater la disquette et à créer un nouveau jeu de sauvetage

1. Retirez la disquette d'amorçage du lecteur et redémarrez l'ordinateur.
2. Insérez la disquette de sauvetage dans le lecteur.
3. Dans la barre des tâches de Windows, cliquez sur **Démarrer** > **Exécuter**.
4. Dans la boîte de dialogue Exécuter, tapez **SYS A:**
5. Cliquez sur **OK**.

Je ne peux pas recevoir de courriers électroniques

Il existe deux solutions à ce problème.

Désactivez temporairement la protection du courrier électronique. Cela peut permettre de télécharger le courrier à problème. Une fois le téléchargement effectué, vous pouvez réactiver la protection de messagerie. Vous êtes protégé par Auto-Protect et le Blocage de script pendant que la protection de messagerie est désactivée.

Pour désactiver temporairement la protection du courrier électronique entrant

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la zone Internet de la boîte de dialogue Options, cliquez sur **Protection de messagerie**.
4. Désélectionnez l'option **Analyser les courriers entrants**.
5. Cliquez sur **OK**.
6. Téléchargez les courriers électroniques.
7. Réactivez la protection des courriers entrants.

Se reporter à "A propos des options Internet" à la page 69.

Le délai de votre client de messagerie a peut-être expiré. Vérifiez que la protection contre les *délais dépassés* est activée.

Si vous avez toujours des problèmes pour télécharger des courriers électroniques, désactivez la protection de messagerie.

Pour désactiver la protection de messagerie

1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la zone Internet de la boîte de dialogue Options, cliquez sur **Protection de messagerie**.
4. Désélectionnez l'option **Analyser les courriers entrants**.
5. Désélectionnez l'option **Analyser les courriers sortants**.
6. Cliquez sur **OK**.

Je ne peux pas envoyer de courriers électroniques

Si vous obtenez le message "Norton AntiVirus n'a pu envoyer votre message car la connexion au serveur de messagerie a été déconnectée", votre client de messagerie est peut-être configuré pour se déconnecter automatiquement après avoir envoyé et reçu le courrier.

Pour rechercher les virus dans les courriers électroniques sortants, Norton AntiVirus intercepte et analyse les courriers avant qu'ils ne soient transmis à votre fournisseur de services de messagerie. Pour résoudre ce problème, désactivez cette option dans votre client de messagerie. Consultez le manuel d'utilisation de votre client de messagerie pour des instructions à ce propos ou désactivez l'analyse de Norton AntiVirus sur les courriers sortants.

Pour désactiver l'analyse des courriers sortants

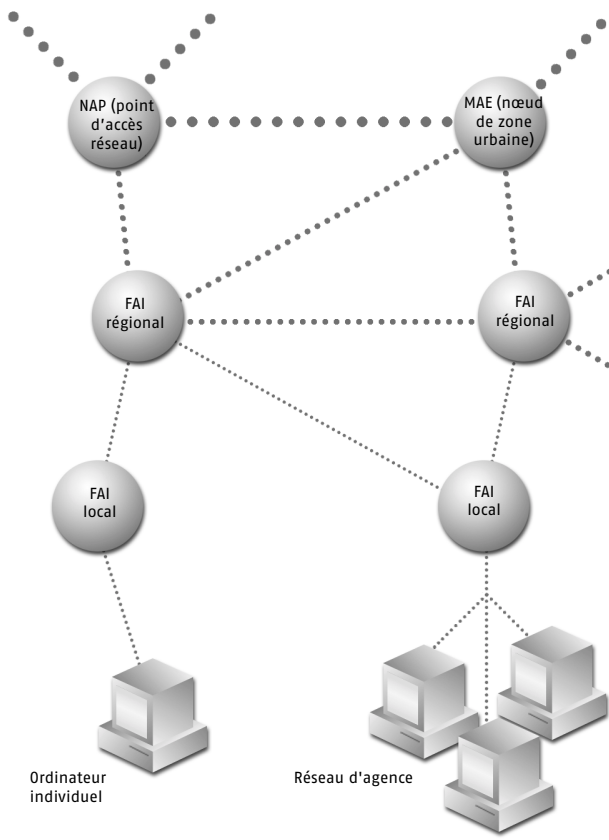
1. Démarrez Norton Internet Security.
2. Dans Security Center, cliquez sur **Options** > **Norton AntiVirus**.
3. Dans la zone Internet de la boîte de dialogue Options, cliquez sur **Protection de messagerie**.
4. Désélectionnez l'option **Analyser les courriers sortants**.
5. Cliquez sur **OK**.

A propos d'Internet

B

Internet est l'interconnexion de millions d'ordinateurs à travers le monde. Il se compose de tous les ordinateurs et de toutes les connexions qui permettent à un ordinateur sur Internet de communiquer avec tout autre ordinateur sur Internet.

Internet peut se comparer à un système de routes et d'autoroutes. Les grands axes d'Internet constituent l'infrastructure et véhiculent de gros volumes d'informations sur de longues distances. Sur ces axes, il y a des interconnexions, appelés NAP (Network Access Point - point d'accès réseau) et des MAE (Metropolitan Area Exchanges - nœud de zone urbaine). Il existe également des "autoroutes régionales", fournies par de grands FAI et des "rues" fournies par des FAI locaux.



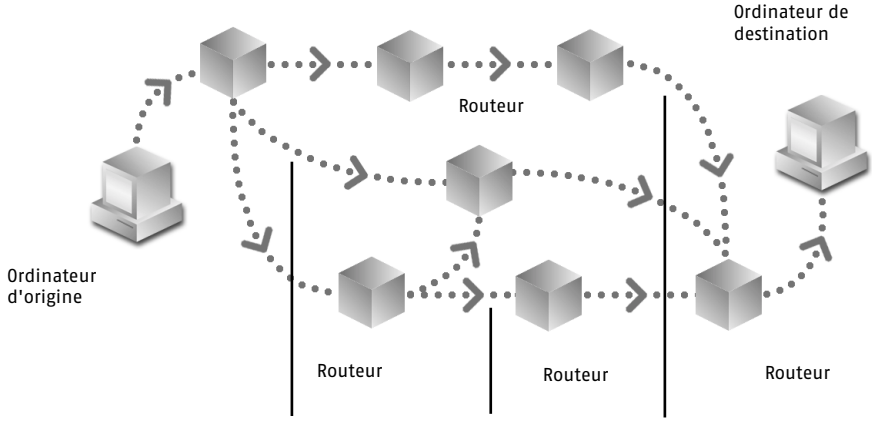
Tout comme un système de routes et d'autoroutes, Internet fournit plusieurs itinéraires pour aller d'un point à un autre. Si une partie d'Internet est encombrée ou endommagée, les informations sont redirigées.

Transmission des informations sur Internet

Toutes les informations envoyées sur Internet sont transmises à l'aide d'un protocole appelé *TCP/IP*. Comme tous les ordinateurs sur Internet comprennent ce protocole, ils peuvent tous communiquer entre eux. TCP et IP sont des parties distinctes de ce protocole.

Internet est un *réseau de commutation par paquets*. Chaque communication est divisée en *paquets* par le protocole TCP (Transmission Control Protocol). Chaque paquet contient les adresses des ordinateurs d'origine et de destination, ainsi que les informations à communiquer.

Le protocole *IP (Internet Protocol)* est chargé de l'acheminement des paquets vers leur destination. Chaque paquet peut suivre un itinéraire différent sur Internet et être subdivisé en *fragments*. Les paquets traversent Internet, en se déplaçant d'un *routeur* à un autre. Les routeurs consultent l'adresse de destination et transmettent le paquet au routeur suivant. IP ne garantit toutefois pas la livraison de chaque paquet.



Itinéraires qu'un paquet ou des fragments de paquet peuvent suivre

Sur l'ordinateur de destination, le protocole TCP réunit les paquets afin de reconstituer la communication complète. Il peut avoir à réorganiser les paquets s'ils ne sont pas arrivés dans l'ordre ainsi qu'à reconstruire les paquets fragmentés. Le protocole TCP demande également la retransmission des paquets manquants.

Le terme TCP/IP est souvent utilisé pour faire référence à un groupe de protocoles utilisés sur Internet, incluant UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) et IGMP (Internet Group Membership Protocol).

A propos du protocole UDP

Le protocole UDP (User Datagram Protocol) est utilisé dans les cas où la fiabilité de TCP n'est pas nécessaire, comme la diffusion d'images vidéo sur plusieurs ordinateurs simultanément. Le protocole UDP n'assure pas la correction des erreurs ni la retransmission des paquets perdus. Du point de l'importance pour la navigation sur Internet, UDP occupe le deuxième rang après TCP.

A propos du protocole ICMP

Les paquets ICMP (Internet Control Message Protocol) contiennent des informations sur les erreurs et des informations de contrôle. Ils sont utilisés pour signaler les erreurs réseau, la congestion du réseau et les dépassements de délai ainsi que pour faciliter le dépannage.

Norton Internet Security accepte normalement les paquets ICMP entrants qui fournissent des informations et présentent un risque minimal. Vous pouvez créer des règles pour bloquer tout ou partie des paquets ICMP.

A propos du protocole IGMP

Le protocole IGMP (Internet Group Membership Protocol) sert à établir des appartenances à des groupes de multidiffusion, séries d'ordinateurs recevant des messages simultanés d'un seul ordinateur. En général, le protocole IGMP sert à diffuser de la vidéo et d'autres données multimédia sur Internet. Votre ordinateur indique à un routeur proche qu'il désire recevoir les messages adressés à un groupe de multidiffusion spécifique.

Le protocole IGMP ne présente pas de risque de sécurité majeur, mais Norton Internet Security vous permet néanmoins de le bloquer totalement. Vous pouvez le bloquer si aucun de vos programmes ne nécessite IGMP. Si vous avez des problèmes de réception d'informations de multidiffusion, par exemples des films ou des présentations PowerPoint, vérifiez que le protocole IGMP n'est pas bloqué.

Stockage des informations du Web sur Internet

Les informations du Web sont stockées sous forme de pages, chacune ayant un nom unique appelé *URL (Uniform Resource Locator)*.

Lorsque vous tapez une adresse Web dans la barre d'adresse du navigateur ou que vous cliquez sur un lien du navigateur Web pour afficher un nouveau site Web, vous fournissez au navigateur l'URL de la page à afficher. Par exemple, www.symantec.fr est une URL standard.

Chaque URL se rattache à l'adresse IP de l'ordinateur qui stocke la page Web. Les URL sont utilisées car elles sont plus faciles à mémoriser que des adresses IP.

Avant de demander une page, votre navigateur demande à un *serveur DNS (Domain Naming System)* l'adresse IP du site Web. Les adresses IP sont des nombres sur 32 bits qui se présentent sous la forme de quatre nombres décimaux, compris entre 0 et 255 et séparés par des points : 206.204.104.148. Chaque ordinateur sur Internet possède une adresse IP distincte.

Demande d'une page

Quand le navigateur dispose de l'adresse IP, il établit une *connexion* TCP au serveur Web et demande la page. Chaque page affichée nécessite une nouvelle connexion au serveur Web. En fait, la plupart des pages nécessitent plusieurs connexions, car chaque graphique (ainsi que de nombreux autres éléments de page) nécessitent une connexion distincte.

Une fois la page chargée, toutes les connexions sont abandonnées. Le processus se répète pour chaque page du site, bien que le navigateur garde en mémoire son adresse IP. Certains sites Web récentes utilisent le protocole HTTP 1.1 (HyperText Transfer Protocol version 1.1), capable d'établir une seule connexion pour transmettre plusieurs fichiers et rester ouverte pour plusieurs pages.

Présentation des URL

Une URL standard se présente comme suit : http://www.symantec.com/securitycheck/index.html. Etant donné que vous pouvez souhaiter bloquer certaines parties seulement d'un *domaine*, vous devez connaître la composition d'une URL.

http://	Protocole de programme utilisé pour établir la connexion. Le protocole le plus utilisé pour naviguer sur le Web est HTTP (HyperText Transfer Protocol). Si vous n'indiquez pas de protocole de programme, votre navigateur utilise http par défaut. FTP (File Transfer Protocol) et gopher sont d'autres protocoles souvent utilisés.
.com	Domaine racine ou domaine de premier niveau. Il existe plusieurs domaines racine courants, notamment .com, .net, .edu, .org, .mil et .gov. Il existe également des domaines racine de deux lettres pour la plupart des pays, par exemple .fr pour la France, .ca pour le Canada et .uk pour le Royaume-Uni.
symantec.com	Domaine. Il s'agit du domaine avec lequel le navigateur établit une connexion. Un domaine correspond souvent à une seule société ou organisation qui peut disposer de plusieurs sites Web sur Internet.
www.symantec.com	Hôte. C'est le site Web spécifique avec lequel le navigateur communique. C'est également le nom pour lequel le serveur DNS fournit une adresse IP.
securitycheck	Dossier ou répertoire qui contient le fichier à afficher.
index.html	Nom du fichier à afficher.

Une URL spécifique, localhost, identifie votre ordinateur vis-à-vis de lui-même. Si votre ordinateur est équipé d'un logiciel de serveur Web, saisissez http://localhost pour afficher votre page Web. L'adresse IP correspondant à localhost est 127.0.0.1.

Identification des programmes sur les serveurs par les ports

Les *ports*, également appelés *sockets*, indiquent l'emplacement de programmes ou de serveurs spécifiques de l'ordinateur distant avec lequel vous essayez d'établir une communication. Il est ainsi possible d'exécuter plusieurs programmes Internet simultanément sur un même ordinateur. Par exemple, de nombreux ordinateurs connectés à Internet exécutent à la fois des serveurs Web et FTP. Le serveur Web utilise le port 80, alors que le serveur FTP utilise le port 21.

Les ports sont numérotés de 1 à 65535. Les ports 1 à 1 023 sont dits "ports connus" et sont utilisés par défaut pour de nombreux programmes Internet.

Les ports font partie des *URL*, mais sont rarement affichés. Le *numéro de port* suit le nom de l'hôte et un signe deux-points. Par exemple :

http://www.symantec.com:80/securitycheck/index.html

Les ports les plus utilisés étant standard, leur numéro est rarement affiché. Les navigateurs Web, par exemple, utilisent pratiquement toujours le port 80. Il n'est donc pas nécessaire de l'indiquer, à moins d'utiliser un port différent.

Les termes serveur et *service* sont utilisés de manière pratiquement interchangeable. Par exemple, un serveur Web fournit le service HTTP, et on dit généralement qu'un ordinateur exécute le service *Finger*.

Ports connus

Voici quelques-uns des ports connus les plus courants.

Port par défaut	Nom du service	Programme
20	ftp-data	Données FTP (File Transfer Protocol)
21	ftp	Contrôle FTP (File Transfer Protocol)
23	telnet	Gestionnaire de terminal Telnet
25	smtp	Protocole SMTP (Simple Mail Transfer Protocol)
53	domaine	Recherche DNS (Domain Naming System)
79	finger	Finger

Port par défaut	Nom du service	Programme
80	http	Protocole HTTP (HyperText Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Service d'authentification d'identité
119	nntp	Protocole NNTP (Network News Transfer Protocol)
137	nbname	Nom NetBIOS (réseau Microsoft)
138	nbdatagram	Datagramme NetBIOS (réseau Microsoft)
139	nbsession	Session NetBIOS (réseau Microsoft)
143	imap	Protocole IMAP (Internet Message Access Protocol)
194	irc	Protocole IRC (Internet Relay Chat)
389	ldap	Protocole LDAP (Lightweight Directory Access Protocol)
443	https	Protocole HTTPS (HTTP sécurisé)

Identification des ordinateurs sur Internet

Des millions d'ordinateurs sont connectés à Internet. Lorsque vous essayez d'identifier des ordinateurs, il est plus simple de travailler avec des groupes d'ordinateurs plutôt que de les identifier individuellement. Les masques de *sous-réseau* permettent d'identifier un groupe d'ordinateurs apparentés, par exemple ceux de votre réseau local.

Un masque de sous-réseau standard se présente comme suit : 255.255.255.0. Les nombres 255 indiquent les parties de l'adresse IP identiques pour tous les ordinateurs du sous-réseau, alors que le 0 indique une partie différente de l'adresse IP.

Les masques de sous-réseau sont toujours utilisés en conjonction avec une adresse IP de base. L'adresse IP de base est une adresse IP qui, lorsqu'elle est traitée avec le masque de sous-réseau, peut indiquer toutes les adresses IP d'un sous-réseau.

Exemple d'adresse IP de base/paire de sous-réseau :

Adresse IP de base : 10.0.0.1

Masque de sous-réseau : 255.255.255.0

Dans cet exemple, la plage d'adresses IP identifiée par l'adresse IP de base et le masque de sous-réseau est comprise entre 10.0.0.1 et 10.0.0.255. Le masque de sous-réseau le plus utilisé est le masque 255.255.255.0 car il identifie un groupe d'adresses IP relativement petit, jusqu'à 254 ordinateurs. Il est généralement utilisé pour de très petits groupes d'ordinateurs, par exemple des groupes de deux ordinateurs seulement.

Risques et menaces liés à Internet

Norton Internet Security vous protège contre les risques majeurs liés à Internet. Ces risques incluent des menaces telles qu'une intrusion dans votre réseau, un code malveillant dans un *contenu actif*, l'exposition à un contenu inopportun, la divulgation d'informations confidentielles et la contamination par des virus provenant de fichiers infectés.

Risques liés aux pirates

A l'origine, les *hackers* étaient des personnes capables de résoudre des problèmes informatiques complexes et d'écrire des programmes rapidement. La signification de ce terme a toutefois changé et désigne aujourd'hui un "pirate" qui utilise ses connaissances en informatique à des fins illicites. Le mot hacker ayant au départ une connotation positive, on utilise parfois le terme *cracker* comme forme péjorative. Dans le présent document, le terme "pirate" correspond à cette connotation péjorative.

D'autres termes anglais désignent les pirates, comme script-kiddies, wannabes et packet monkeys. Ils s'appliquent tous à des pirates en herbe qui utilisent des applications écrites par des pirates plus expérimentés pour attaquer des ordinateurs sur Internet.

Déroulement d'une attaque de pirate

La plupart des attaques de pirate se déroulent de la manière suivante :

- Collecte d'informations
  Le pirate rassemble le maximum d'informations sur votre ordinateur. Il tente ensuite de trouver des failles, sans que vous sachiez que votre ordinateur subit une attaque.
- Accès initial
  Le pirate exploite une faille décelée pendant la collecte d'informations et établit un point d'entrée dans votre ordinateur.
- Escalade des droits
  Le pirate gagne l'accès à davantage de programmes et de *services* sur votre ordinateur.
- Effacement des traces :
  le pirate masque ou supprime toute trace de sa visite, en laissant parfois une porte ouverte pour une future intrusion.

Collecte d'informations

La première étape de la collecte d'informations consiste à définir une cible. Un pirate peut choisir une personne ou une société à attaquer ou rechercher sur Internet une cible non protégée qui sera facile à attaquer. La quantité d'informations disponibles à votre propos sur Internet est directement proportionnelle à votre présence sur le Web. Si vous avez un nom de *domaine* et un site Web, une plus grande quantité d'informations est à la portée de tout le monde que si vous ne disposez que d'une *adresse électronique*.

Si un pirate a choisi une cible spécifique, comme une société ou une organisation, de nombreuses ressources sur Internet lui permettent de collecter des informations. Grâce à Internet, un pirate peut en apprendre beaucoup sur une cible potentielle. Avec un nom de domaine, il est facile de trouver le nom et l'adresse du propriétaire, ainsi que le nom et le numéro de téléphone des contacts administratifs et techniques. Ces informations ne peuvent généralement pas être utilisées directement pour attaquer un réseau ou un ordinateur, mais peuvent servir à rassembler plus informations.

Si un pirate n'a pas de cible précise, de nombreux outils permettent d'analyser Internet pour rechercher des cibles potentielles. L'analyse la plus simple consiste à utiliser la commande "ping", qui permet d'analyser rapidement des milliers d'ordinateurs. Le pirate utilise un programme pour lancer des "ping" à des ordinateurs dans des plages définies d'adresses IP. Une réponse indique au pirate qu'un ordinateur est connecté et utilise l'adresse IP correspondante. Lorsque Norton Internet Security est en cours d'exécution, votre ordinateur est masqué aux analyses ping car il ne répond pas. Le pirate ne peut donc pas déterminer qu'un ordinateur se trouve à votre adresse IP avec une simple commande ping.

Les *analyses de port* permettent une analyse plus approfondie, généralement effectuée sur un seul ordinateur. Une analyse de port peut indiquer à un pirate les services en cours d'exécution, comme HTTP et FTP. Chaque service en cours d'exécution fournit un point d'entrée potentiel au pirate. Sur des ordinateurs non protégés, les ports non utilisés répondent qu'ils sont fermés, indiquant ainsi au pirate qu'un ordinateur existe à cette adresse IP. Norton Internet Security ne répond pas aux analyses de ports non utilisés, en les *masquant*.

Accès initial

Le moyen le plus facile pour un pirate d'accéder à un ordinateur Windows consiste à utiliser la fonctionnalité de réseau Microsoft. Sur de nombreux ordinateurs, le réseau Microsoft est activé afin que les utilisateurs du réseau puissent s'y connecter.

La fonction de réseau NetBIOS de Microsoft utilise trois des ports les plus connus. Ces ports sont utilisés pour établir des *connexions* entre des ordinateurs d'un réseau Microsoft. En fait, ils indiquent normalement le nom de l'ordinateur sur le réseau local. C'est l'effet recherché sur votre réseau, mais pas du tout sur Internet. Norton Internet Security est configuré par défaut pour bloquer ces ports et éviter ainsi qu'une personne sur Internet ne puisse se connecter à votre ordinateur à l'aide de la fonctionnalité de réseau Microsoft. Si votre ordinateur est connecté à un réseau local ainsi qu'à Internet, vous devez modifier certains paramètres pour permettre les communications avec les autres ordinateurs du réseau. Norton Internet Security continue à vous protéger contre les risques liés à Internet tout en vous permettant d'utiliser votre réseau local.

Escalade des droits

Une fois qu'un pirate est connecté à votre ordinateur, son objectif suivant consiste à augmenter le plus possible son contrôle. Les étapes impliquées et les résultats obtenus varient en fonction de la version de Windows installée sur l'ordinateur cible.

Sur les ordinateurs équipés de Windows 95/98/Me, un pirate n'a pas besoin d'augmenter son contrôle une fois qu'il a accès à l'ordinateur. Il détient un contrôle total sur l'ordinateur. Heureusement, ces versions de Windows ne possèdent pas de nombreuses fonctions de contrôle à distance et sont donc relativement faciles à protéger.

Sur les ordinateurs équipés de Windows NT/2000/XP, le pirate va tenter d'obtenir des droits d'administrateur sur l'ordinateur. La clé pour obtenir ces droits est généralement un *mot de passe*. Un pirate peut télécharger votre fichier de mots de passe et le décoder.

Une autre tactique consiste à placer un *cheval de Troie* sur votre ordinateur. Si un pirate parvient à placer un programme comme Back Orifice, Subseven ou NetBus sur votre ordinateur et à l'exécuter, il peut prendre le contrôle total de l'ordinateur.

D'autres chevaux de Troie peuvent enregistrer le texte tapé au clavier afin de capturer les mots de passe et d'autres données stratégiques. Norton Internet Security et Norton AntiVirus fournissent deux niveaux de protection contre les chevaux de Troie. Norton AntiVirus vous protège contre l'exécution accidentelle de ces programmes. Norton Internet Security bloque les ports que les chevaux de Troie d'accès à distance utilisent pour communiquer sur Internet.

Effacement des traces

Lorsqu'un pirate a gagné un maximum de contrôle sur un ordinateur, il cherche ensuite à effacer les preuves. Tant que vous n'êtes pas conscient qu'un pirate a investi votre ordinateur, vous n'agissez pas pour l'arrêter.

Dans le cas d'ordinateurs fonctionnant sous Windows 2000/XP, les pirates tentent de désactiver les fonctions d'audit et de modifier ou d'effacer le *journal* des événements. Sur tout ordinateur, un pirate peut cacher des fichiers afin de les avoir à disposition lors de visites ultérieures. Dans des cas extrêmes, un pirate peut formater le disque dur d'un ordinateur attaqué afin d'éviter d'être identifié.

Risques liés à des contenus actifs

Les *contrôles ActiveX* et les *applets Java* sont désignés *contenus actifs* parce qu'ils vont au-delà du simple affichage de texte ou de graphiques. La plupart des contenus actifs ne sont pas dangereux. Ils sont couramment utilisés pour afficher des menus contextuels et le cours actualisé de valeurs boursières, par exemple.

Les contrôles ActiveX et les applets Java sont supposés être sûrs pour être exécutés dans votre navigateur. ActiveX utilise un système de certificats numériques qui vous permet de décider si vous souhaitez exécuter un contrôle ActiveX. Les certificats numériques se présentent sous la forme de boîtes de dialogue qui vous demandent si vous souhaitez installer et exécuter un contrôle qui apparaît lorsque vous naviguez sur le Web.

L'utilisation de certificats numériques pose plusieurs problèmes. Certains contrôles ne sont pas accompagnés de certificats et certains certificats fournissent très peu d'informations sur les fonctions du contrôle.

Le sandbox ("bac à sable") Java a été conçu pour empêcher les applets Java d'accéder à des informations en dehors du navigateur et de faire quoi que ce soit qui risque d'endommager l'ordinateur. Toutefois, les *pirates* trouvent sans cesse des moyens de contourner les protections Java et d'utiliser les fonctionnalités de Java de façon non prévue par leurs développeurs.

Norton Internet Security contrôle les contenus actifs et peut les bloquer tous ou vous avertir chaque fois qu'il rencontre un contenu actif. La fonction de protection automatique de Norton AntiVirus détecte les contrôles ActiveX et les applets Java dangereux et empêche leur exécution.

Norton Personal Firewall contrôle les contenus actifs et peut les bloquer tous ou vous avertir chaque fois qu'il rencontre un contenu actif.

Risques liés à des activités et des contenus inadaptés

Internet offre un trésor d'informations aisément accessible à tous. Certains sujets ne conviennent toutefois pas à tous les publics. Par exemple, la plupart des gens estiment que les sites consacrés à la pornographie ou à la violence sont inadaptés aux enfants. Vous pouvez également souhaiter restreindre l'accès à d'autres types de contenus.

Blocage de catégories de sites et de groupes de discussion

Norton Internet Security vous permet de sélectionner les sites Web et les groupes de discussion auxquels les utilisateurs auront accès depuis cet ordinateur. Comme il peut être nécessaire d'attribuer différents niveaux d'accès à différents publics, Norton Internet Security permet de bloquer des contenus spécifiques pour chaque utilisateur.

Restriction d'accès aux applications

Certaines applications Internet peuvent également être inappropriées sur votre ordinateur. Vous pouvez, par exemple, ne pas souhaiter que vos enfants utilisent des applications de discussion en direct. Vous pouvez également vouloir restreindre l'utilisation des programmes de transfert de fichiers. Vous réduirez ainsi le risque d'introduire dans votre ordinateur ou votre réseau des virus, des vers, des zombies, des *chevaux de Troie* et autre code dangereux.

Norton Internet Security permet de sélectionner les catégories de programmes qui auront accès à Internet. Il tient à jour la liste de programmes, de sorte que votre protection reste actualisée, même en cas de sortie de nouveaux programmes. Vous pouvez également ajouter des applications personnalisées et contrôler leur utilisation.

Risques liés à la confidentialité

Internet présente un certain nombre de risques en matière de confidentialité. Certains sites collectent et enregistrent des informations personnelles, comme les numéros de carte de crédit. D'autres suivent l'utilisation que vous faites d'Internet. Certaines applications envoient à votre insu à des sites Web des informations sur l'utilisation que vous faites de votre ordinateur.

Envoi d'informations confidentielles

Vous ne souhaitez certainement pas que des données confidentielles comme votre numéro de carte de crédit ou votre numéro de téléphone personnel, circulent pas en clair sur Internet. Le Contrôle de confidentialité empêche la saisie d'informations confidentielles sur les sites Web qui n'utilisent pas des communications sécurisées et chiffrées, et leur envoi avec des programmes de messagerie instantanée.

Si vous voulez éviter l'envoi de données confidentielles sur Internet, Norton Internet Security peut interdire l'accès des utilisateurs aux sites sécurisés qui risquent de demander des informations personnelles.

Les cookies

Les *cookies* sont des messages envoyés à votre navigateur par un site Web et stockés sous la forme de petits fichiers sur votre ordinateur. Ils sont souvent utilisés par des sites Web pour le suivi de vos visites. Dans la plupart des cas, les cookies ne contiennent aucune information personnelle, mais plutôt des informations permettant aux sites Web de vous identifier.

Bons cookies

Dans leur forme la plus inoffensive, les cookies cessent d'exister lorsque vous fermez votre navigateur. Ce type de cookie est principalement utilisé pour rappeler des choix effectués lors de la consultation d'un site Web.

De nombreux sites laissent des cookies sur votre ordinateur de manière à pouvoir vous identifier lors de votre visite suivante sur le même site. Ces cookies vous identifient de manière à utiliser les options que vous aviez sélectionnées auparavant. Si vous fréquentez un site qui garde en mémoire les valeurs mobilières dont vous souhaitez effectuer le suivi, par exemple, il est probable que ce site utilise ce type de cookie.

Mauvais cookies

Dans l'une de leurs formes malveillantes, les cookies d'un site Web peuvent suivre vos visites sur un autre site Web. Par exemple, la plupart des publicités que vous voyez sur des sites Web ne proviennent pas des sites que vous visitez, mais de sites qui fournissent des publicités à de nombreux autres sites. Lorsque le site de publicité affiche la publicité, il a accès aux cookies de votre ordinateur. Le site de publicité peut ainsi surveiller votre utilisation du Web sur une large gamme de sites et établir un profil.

Blocage des cookies

Norton Internet Security peut bloquer tous les cookies ou vous informer de toutes les demandes de cookie. Si vous bloquez tous les cookies, des fonctionnalités ne seront plus disponibles dans de nombreux sites Web. Par exemple, vous ne pourrez plus effectuer d'achats dans certains magasins en ligne sur Internet. Si vous choisissez d'être informé chaque fois qu'un site Web essaye de créer un cookie, vous serez en mesure d'étudier chaque demande et de bloquer celles qui ne proviennent pas du site que vous visitez. Norton Internet Security peut également bloquer ou autoriser les cookies issus de *domaines* ou de sites Web spécifiques.

Suivi de l'utilisation d'Internet

La plupart des navigateurs transmettent des informations que vous pouvez considérer comme confidentielles. Un élément généralement transmis par votre navigateur aux sites Web est l'*URL* de la page dont vous provenez. Cette information est utilisée par certains sites Web pour vous aider à visiter le site, mais elle peut également servir à surveiller vos habitudes de navigation sur le Web. Norton Internet Security bloque ce genre d'informations.

Votre navigateur envoie également des informations sur lui-même et sur le système d'exploitation utilisé. Norton Internet Security peut bloquer ces informations, mais elles sont généralement utilisées par les sites Web pour fournir les pages Web correspondant à votre navigateur.

Un risque potentiellement plus grand en matière de confidentialité est constitué par les programmes que vous installez sur votre ordinateur et qui, à votre insu, transmettent des informations aux sites Web. Plusieurs programmes dont la fonction est de vous aider à télécharger et à installer des fichiers, transmettent des informations sur vos activités sur Internet. Norton Internet Security préserve votre vie privée en vous prévenant de ces communications.

Risques liés aux chevaux de Troie et aux virus

De nos jours, avec de si nombreux ordinateurs connectés à des réseaux et à Internet, les virus peuvent se propager bien plus rapidement qu'à l'époque où les fichiers étaient transmis d'un ordinateur à un autre à l'aide de disquettes. En outre, le risque ne se limite plus aux virus, mais s'est élargi aux *chevaux de Troie*, vers et zombies.

Un virus est un programme ou un code qui se duplique en s'associant à un autre programme, un secteur d'amorçage, un secteur de partition ou un document qui prend en charge des macros. Si de nombreux virus ne font que se dupliquer, d'autres causent des dommages. Un virus peut arriver dans un *courrier électronique*..

Un cheval de Troie est un programme qui ne se duplique pas, mais qui endommage ou menace la sécurité de l'ordinateur. En principe, il vous est envoyé par courrier électronique par une personne, mais ne s'envoie pas de lui-même. Un cheval de Troie peut arriver déguisé sous la forme d'un utilitaire. Certains chevaux de Troie ont des effets malveillants sur l'ordinateur sur lequel ils sont exécutés, alors que d'autres, comme Back Orifice, fournissent des fonctionnalités de contrôle à distance aux *pirates*.

Un ver est un programme qui crée des copies de lui-même, par exemple d'un disque à un autre ou par courrier électronique. Il peut provoquer des dommages ou menacer la sécurité de l'ordinateur. Un ver peut arriver sous forme de pièce jointe d'un courrier électronique dont le sujet semble intéressant.

Un zombie est un programme installé secrètement qui sommeille sur un ordinateur. Il se réveille ultérieurement, pour contribuer à une attaque collective sur un autre ordinateur. Les programmes zombie ne causent normalement pas de dommages sur l'ordinateur sur lequel ils résident et servent à attaquer d'autres ordinateurs. Un zombie peut arriver sous forme de pièce jointe à un courrier électronique.

Norton AntiVirus vous protège contre la réception et l'exécution de virus, chevaux de Troie, vers et zombies. Il analyse les courriers électroniques lors de leur réception et vérifie les fichiers lors de leur ouverture, apportant ainsi deux niveaux de protection.

Norton Internet Security garantit que les chevaux de Troie ne communiquent pas sur Internet. Vous êtes ainsi protégé des pirates qui utilisent des chevaux de Troie.

Probabilité de subir une attaque

Internet présente de nombreux risques. Quelles sont vos chances d'être victime d'une attaque ? La probabilité qu'un pirate choisisse votre ordinateur en particulier parmi tous ceux connectés à Internet est certainement très faible. Cependant, avec la généralisation des programmes d'analyse de ports et autres outils de détection utilisés par les pirates, les analyses de failles dont votre ordinateur peut faire l'objet sont relativement fréquentes. Plus les failles sont nombreuses, plus votre ordinateur devient tentant pour les pirates.

Les outils permettant de trouver des cibles sont capables d'analyser de très grands groupes d'ordinateurs sur Internet. Le pirate doit simplement indiquer une plage d'adresses IP à analyser. Le programme vérifie chaque adresse IP afin de déterminer la présence éventuelle d'un ordinateur. Si un ordinateur est trouvé, une série de tests est lancée pour déceler des failles, comme la fonctionnalité de réseau Microsoft activée pour Internet. Le pirate revient ensuite consulter une liste d'ordinateurs, avec leurs failles.

Norton Internet Security vous protège contre ces analyses en rendant votre ordinateur invisible. Votre ordinateur ne répond pas à la plupart des requêtes envoyées par ces programmes d'analyse. Puisqu'il ne présente aucune faille au pirate, votre ordinateur devient ainsi une mauvaise cible, le rendant inintéressant pour une attaque.

Glossaire

Ce glossaire fournit la définition de termes Internet couramment utilisés.

adresse IP (adresse Internet Protocol) Identificateur numérique sur 32 bits qui identifie un ordinateur sur Internet.Les adresses IP se présentent généralement sous la forme de quatre groupes de nombres, compris entre 0 et 255 et séparés par des points. Par exemple, 206.204.52.71.

adresse réseau Partie d'une adresse IP commune à tous les ordinateurs d'un réseau ou sous-réseau spécifique.

alerte Boîte de dialogue qui apparaît dans une interface utilisateur graphique (GUI) afin de signaler une erreur ou pour fournir un avertissement.

analyse de port Tentative d'accès à un ordinateur par recherche des ports ouverts.Généralement effectué par un programme automatisé qui envoie une demande à chaque port d'une adresse IP et attend les réponses pouvant révéler une vulnérabilité.

applet Java Petit programme qui s'exécute dans un environnement restreint géré par votre navigateur.La plupart des applets Java servent à ajouter des effets multimédia, une interactivité ou d'autres fonctionnalités à une page Web, mais peuvent également être utilisées à des fins malveillantes, par exemple pour dérober des mots de passe.

bannière publicitaire Graphique publicitaire, souvent animé, qui apparaît en haut d'une page Web et peut contenir un lien vers le site Web à l'origine de la publicité.

boot record A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot record also contains a program that loads the operating system.

cheval de Troie Programme destructeur souvent conçu pour endommager un ordinateur, bien que déguisé en application utile ou intéressante.

communication entrante Tentative d'un ordinateur externe d'établir une connexion avec votre ordinateur. La connexion peut être utilisée pour envoyer des données vers ou depuis l'ordinateur.

communication sortante Tentative effectuée par votre ordinateur pour établir une connexion avec un ordinateur distant.La connexion peut être utilisée pour envoyer des données vers ou depuis votre ordinateur.

fichier compressé Fichier compressé dans un format de stockage des données spécial afin d'économiser de l'espace disque.

connexion Méthode d'échange de données qui permet un transfert fiable entre deux ordinateurs.

contenu actif Matériau d'une page Web qui change dans le temps ou en réponse à une action de l'utilisateur. Les contenus actifs sont mis en œuvre par l'intermédiaire de contrôles ActiveX, de scripts Visual Basic, de scripts Java et d'applets Java dans le code HTML qui définit la page.

contrôle ActiveX Programme qui s'exécute dans un navigateur utilisant la technologie Microsoft pour ajouter des animations à une page Web, de l'audio et de la vidéo en continu, des films, etc.Lorsque vous visitez une page Web contenant un contrôle ActiveX, celui-ci est téléchargé dynamiquement et enregistré sur votre disque dur. Contrairement aux applets Java, les contrôles ActiveX ne s'exécutent pas dans un environnement restreint et peuvent potentiellement prendre le contrôle de votre ordinateur.

cookie
Petit fichier de données que certains sites Web placent sur votre disque dur lors de l'affichage d'une page Web.Les serveurs Web peuvent utiliser des cookies pour stocker vos informations personnelles et vos préférences, afin de vous éviter d'avoir à les indiquer de nouveau lors de votre visite suivante.

courrier électronique ("e-mail")
Méthode d'échange de messages et de fichiers avec d'autres personnes par l'intermédiaire de réseaux d'ordinateurs.SMTP (Simple Mail Transfer Protocol) est un protocole répandu pour envoyer des courriers électroniques. Les protocoles couramment utilisés pour la réception de messages sont POP3 (Post Office Protocol 3) et IMAP4 (Internet Message Access Protocol 4). Les services de messagerie Web utilisent le protocole HTTP (HyperText Transfer Protocol) pour l'envoi et la réception de courriers électroniques.

cracker
Personne qui "craque" du code, pas obligatoirement pour des raisons malveillantes. Terme parfois utilisé pour faire référence à un pirate mal intentionné.

délai limite
Période prédéterminée pendant laquelle une tâche donnée doit être exécutée. Si la valeur du délai est atteinte avant ou pendant l'exécution de la tâche, cette dernière est annulée.

DHCP (Dynamic Host Configuration Protocol)
Protocole TCP/IP qui attribue automatiquement une adresse IP temporaire à chaque périphérique d'un réseau.

DNS (Domain Naming System)
Système d'attribution de noms hiérarchique qui convertit les noms de domaine (comme www.symantec.com) en adresses IP (comme 206.204.212.71).

domaine
Adresse commune d'une société ou d'une organisation (comme symantec.com) sur Internet, qui peut représenter plusieurs hôtes.

domaine de niveau supérieur	Dernière partie d'un nom de domaine, qui identifie le type d'entité titulaire de l'adresse (comme .com pour des entreprises ou .edu pour les institutions du secteur de l'éducation) ou l'emplacement géographique de l'adresse (par exemple .fr pour la France, .ca pour le Canada ou .uk pour le Royaume-Uni).
executable file	A file containing program code that can be launched. Generally includes any file that is a program, extension, or a system file.
FAI (fournisseur d'accès à Internet)	Société qui fournit un accès à Internet à des particuliers et à des entreprises.La plupart des FAI offrent d'autres services de connectivité Internet, comme l'hébergement de site Web.
type de fichier	Code stocké dans chaque fichier qui l'associe à un programme ou une activité.
finger	Dans certains systèmes d'exploitation, commande qui demande des informations de compte d'utilisateur réseau.
fragment	Paquet IP qui a été divisé en deux ou plusieurs parties (ou fragments).Lorsque la taille d'un paquet IP dépasse la taille de trame maximale d'un réseau qu'il traverse, le paquet doit être divisé en paquets (fragments) plus petits.
furtif	Donner l'impression de ne pas exister en ne répondant pas aux demandes d'informations.
HTML (Hypertext Markup Language)	Langage standard des documents sur le World Wide Web. Les codes insérés dans un fichier texte indiquent au navigateur Web comment afficher le texte et les images d'une page Web sur l'écran de l'utilisateur et définissent des liens hypertexte entre les documents.
icône	Symbole graphique employé pour représenter un fichier, un dossier, un disque ou une autre entité.
fichier infecté	Fichier contenant un virus, un cheval de Troie ou un ver.

IP (Internet Protocol) Protocole dominant utilisé pour transmettre des données d'un ordinateur à un autre sur Internet. IP achemine les paquets vers les destinations appropriées.

JavaScript Langage de script similaire à Java, mais offrant moins de capacités. Le code JavaScript peut être inclus dans des pages Web pour ajouter une interactivité et d'autres fonctionnalités.

journal Enregistrement des actions et des événements qui se produisent sur un ordinateur de bureau ou un ordinateur de poche.

local Terme qui fait référence à votre ordinateur, par opposition à un ordinateur distant.

menace Circonstance, événement ou personne pouvant potentiellement porter atteinte à un système par destruction, divulgation, modification de données et/ou refus de service.

modem Dispositif de modulation (conversion en données analogiques) et démodulation (conversion de données analogiques) de données numériques en vue de leur transmission sur une ligne téléphonique.Inclut également les périphériques d'interface destinés aux connexions numériques sur Internet, comme les périphériques RNIS, câble et DSL.

mot de passe Séquence de caractères saisie par les utilisateurs pour de s'identifier auprès d'un réseau ou d'un programme. Les mots de passe les plus sûrs sont difficiles à deviner ou à trouver dans un dictionnaire et qui sont constitués d'une combinaison de lettres majuscules et minuscules, de chiffres et de symboles.

NAT (Network Address Translation) Méthode de conversion des adresses IP utilisées sur un intranet ou un réseau local en adresses Internet IP.Cette méthode permet de partager une adresse IP Internet entre plusieurs ordinateurs. De plus, elle permet de masquer les adresses IP des ordinateurs du réseau vis-à-vis de l'extérieur.

navigateur Application qui facilite la navigation sur Internet en fournissant une interface utilisateur graphique. L'utilisateur dispose de menus, d'icônes et de boutons qui lui évitent d'assimiler des commandes complexes. Egalement appelé client Web.

numéro de port Canal de communication logique utilisé par une application TCP/IP spécifique. Des numéros de port uniques sont associés à chaque application. Par convention, certains protocoles utilisent un numéro de port connu (par exemple, le protocole HTTP utilise le port 80), mais ces numéros restent configurables.

page Web Document unique sur le World Wide Web (WWW) identifié par une URL unique. Une page Web peut contenir du texte, des liens hypertexte et des graphiques.

paquet Unité de données acheminée entre une source et une destination sur Internet. Outre les données transmises, un paquet contient des informations qui permettent aux ordinateurs d'un réseau de déterminer s'ils doivent le recevoir.

pare-feu Système de sécurité qui utilise des règles pour bloquer ou autoriser des connexions et des transmissions de données entre votre ordinateur et Internet.

pirate Personne qui tente d'accéder à des ordinateurs sans autorisation dans le but de détourner les informations de ces ordinateurs ou de les endommager.

pop3 (Post Office Protocol 3) Protocole de courrier électronique servant à récupérer du courrier depuis un serveur distant sur une connexion Internet.

port

Identification d'utilisateur de transport utilisée par un programme client pour spécifier un programme serveur particulier sur un ordinateur. Egalement appelé service.

Certaines applications ont des ports aux numéros préaffectés. D'autres ont des numéros de port affectés dynamiquement lors de chaque connexion. Lorsqu'un service (programme serveur) démarre, il se rattache au numéro de port qui lui a été associé. Lorsqu'un programme client veut utiliser ce serveur, il doit également demander à se rattacher à ce numéro de port.

proxy

Mécanisme qui permet à un système d'agir au nom d'un autre système pour répondre aux demandes des protocoles. Les programmes de sécurité des pare-feu utilisent des services proxy pour protéger le réseau sécurisé des utilisateurs d'Internet.

quarantaine

Emplacement d'un disque configuré par Norton AntiVirus pour isoler les fichiers soupçonnés de contenir un virus afin qu'on ne puisse pas les ouvrir ni les exécuter.

règle de filtrage

Ensemble de paramètres qui définit un type de paquet de données ou de communication réseau et indique la marche à suivre (autorisation ou blocage) vis-à-vis de cet élément.

réseau

Ensemble d'ordinateurs et de périphériques associés reliés ensemble pour partager des informations et du matériel entre des utilisateurs.

réseau de commutation par paquets

Réseau d'ordinateurs (comme Internet) qui transmet des fichiers en les scindant en paquets et en acheminant chaque paquet par l'itinéraire disponible le plus avantageux entre la source et la destination.

routeur

Périphérique d'un réseau qui relie les ordinateurs ou les réseaux interconnectés. Un routeur reçoit des paquets et les transmet à leur destination selon l'itinéraire le plus avantageux.

serveur Ordinateur de contrôle d'un réseau local, qui contrôle l'accès des logiciels aux postes de travail, imprimantes et autres composants du réseau.

serveur DNS (serveur Domain Naming System) Ordinateur qui stocke une base de données de noms de domaine avec les adresses IP correspondantes.Lorsqu'un ordinateur envoie un nom de domaine à un serveur DNS, ce dernier lui renvoie l'adresse IP correspondant au domaine.

service Protocoles permettant à un ordinateur d'accéder à un type de données stockées sur un autre ordinateur. De nombreux ordinateurs hôtes connectés à Internet offrent des services. Ainsi, les serveurs HTTP utilisent Hypertext Transfer Protocol pour fournir un service World Wide Web et les serveurs FTP offrent des services File Transfer Protocol. *Voir aussi* port.

site Web Groupe de pages Web gérées par une même société, organisation ou personne.Un site Web peut inclure du texte, des images, des fichiers audio et vidéo et des liens hypertexte vers d'autres pages Web.

socket Identificateur d'un service spécifique, sur un ordinateur spécifique. Un socket est constitué de l'adresse IP de l'ordinateur suivie du signe deux points et du numéro de port.

sous-réseau Réseau local appartenant à un intranet plus important ou à Internet.

système d'exploitation Programme qui relie les fonctionnalités des matériels et logiciels informatiques à des périphériques d'entrée/sortie tels que des disques, des claviers et des souris.

TCP/IP (Transmission Control Protocol/ Internet Protocol) Gamme standard de protocoles utilisée pour communiquer avec les périphériques Internet.

télécharger Transférer des données entre deux ordinateurs, généralement sur un modem ou un réseau. Se réfère en général à l'action de transférer un fichier depuis Internet, un système BBS ou un service en ligne vers son ordinateur.

tentative de connexion Demande par le transfert de données de l'établissement d'une connexion.

virus inconnu Virus pour lequel Norton AntiVirus ne possède pas de définition. Voir aussi définition de virus.

URL (Uniform Resource Locator) Adresse globale des documents et d'autres ressources sur le World Wide Web, et convention que les navigateurs Web utilisent pour localiser les fichiers et d'autres services distants.

virus Programme qui s'auto-reproduit et qui a été écrit dans le but de porter atteinte au fonctionnement de votre ordinateur, à votre insu et sans votre accord. Un virus peut se propager à d'autres fichiers. S'il est activé, il peut endommager les fichiers, perturber le fonctionnement de l'ordinateur ou afficher des messages gênants.

définition de virus Informations sur le virus permettant aux programmes antivirus de détecter la présence d'un virus et de vous en avertir. Voir aussi virus inconnus.

activité suspecte Activité ou action que Norton AntiVirus perçoit comme éventuellement issue d'un virus inconnu. Les alertes liées aux activités suspectes n'indiquent pas nécessairement la présence d'un virus, mais elles doivent être prises en compte.

World Wide Web (WWW) Ensemble de documents hypertexte stockés sur des serveurs Web dans le monde entier. Egalement appelé WWW ou simplement Web. Le Web permet un accès universel à une vaste collection de documents stockés au format HTML sous forme de pages Web.

ver Programme qui crée des copies de lui-même, par exemple d'un disque à un autre, ou qui s'envoie lui-même par courrier électronique. Il peut provoquer des dommages ou menacer la sécurité de l'ordinateur.

zombie Programme dormant installé secrètement sur un ordinateur et qui est réveillé pour participer à l'attaque collective d'un autre ordinateur ou serveur. En général, les programmes zombie ne causent pas de dommages sur l'ordinateur sur lequel ils résident mais servent à attaquer d'autres ordinateurs.

Index

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Solutions de service et de support EMEA

Service Clientèle - vous aide pour les questions non techniques telles que les commandes, les mises à jour, les échanges et les remises.

Support technique - vous aide pour les questions techniques telles que l'installation, la configuration ou le dépannage des produits Symantec.

Les systèmes de support technique et de service clientèle varient en fonction des pays. Pour vous renseigner sur les offres de service dans votre région, visitez le site Web approprié.

Si ce produit vous a été fourni lors de l'achat de votre ordinateur, le fabricant du système prend la responsabilité du support, sauf indication contraire.

Service Clientèle

Le site de support Web vous indique comment :

- localiser des revendeurs et des consultants dans votre région ;
- remplacer des CD défectueux et des manuels ;
- mettre à jour l'enregistrement de votre produit ;
- vous informer sur les commandes, les retours et les remises ;
- accéder à la Foire aux questions (FAQ) du service Clientèle ;
- adresser une question à un agent du Service Clientèle ;
- obtenir des informations une documentation produit ou un logiciel d'essai.

Pour les commandes de mises à jour produit, consultez les informations correspondant à votre région.

Royaume-Uni, Irlande :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Allemagne, Autriche et Suisse :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/gdocid/20000531114300925

France, Belgique, Luxembourg :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/fdocid/20000530164002925

Pays-Bas, Belgique :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/ddocid/20000531114633925

Italie :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/idocid/20001114142714925

Espagne :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/sdocid/20000531113344925

Suède, Norvège, Danemark, Finlande :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/swdocid/20000531113940925

Autres pays :

http://service1.symantec.com/SUPPORT/INTER/emeacustserv.nsf/eedocid/199991585523

Support technique

Symantec propose deux options de support technique pour vous aider à installer, configurer ou dépanner des produits Symantec.

Service et support en ligne

Connectez-vous au site Web de service et de support Symantec pour votre région. Spécifiez un type d'utilisateur puis sélectionnez votre produit et sa version pour :

- accéder aux rubriques d'actualité ;
- consulter la base de connaissances ;
- suivre des didacticiels en ligne ;
- vous informer sur les options de contact ;
- adresser une question à un agent du support technique en ligne.

Support téléphonique

Des services de support payants par téléphone sont accessibles à tous les utilisateurs enregistrés. Visitez le site de support de votre pays pour obtenir des informations de contact.

Prise en charge des anciennes versions et des versions abandonnées

Lorsque Symantec annonce qu'un produit n'est plus commercialisé, le support téléphonique est assuré pendant 60 jours suivant cette annonce. Certaines informations techniques restent cependant disponibles sur le site de support Symantec.

Politique d'abonnement

Si votre produit Symantec inclut une protection antivirus, un pare-feu (firewall) ou une protection de contenu de site, vous pouvez avoir droit à des mises à jour via LiveUpdate. La durée de l'abonnement dépend de votre produit Symantec.

Quand l’abonnement initial expire, vous devez le renouveler pour continuer à actualiser votre protection. Ces mises à jour limitent votre vulnérabilité aux attaques.

Lorsque vous exécutez LiveUpdate vers la fin de votre abonnement, un message vous rappelle de vous réabonner pour un coût réduit. Suivez simplement les instructions affichées à l'écran.

Pour d'autres informations, visitez le site Web de service et de support Symantec pour votre région.

Bureaux service et support

Europe, Moyen Orient et Afrique

Service Clientèle de Symantec
Postbus 1029
3600 BA Maarssen
Pays-Bas
http://www.symantec.com/region/reg_eu/

Sites Web de service et de support

Europe/Anglais :
http://www.symantec.com/eusupport

Allemagne, Autriche et Suisse :
http://www.symantec.de/desupport/

France :
http://www.symantec.fr/frsupport/

Pays-Bas :
http://www.symantec.nl/nlsupport/

Italie :
http://www.symantec.it/itsupport/

Espagne :
http://www.symantec.com/region/mx/techsupp/index.html

Suède :
http://www.symantec.com/region/se/techsupp/index.html

Norvège :
http://www.symantec.com/region/no/techsupp/index.html

Danemark :
http://www.symantec.com/region/dk/techsupp/index.html

Finlande :
http://www.symantec.com/region/fi/techsupp/index.html

Pologne :
http://www.symantec.com/region/pl/techsupp/index.html

République tchèque :
http://www.symantec.com/region/cz/techsupp/index.html

République slovaque :
http://www.symantec.com/region/cz/techsupp/index.html

Russie :
http://www.symantec.com/region/ru/techsupp/index.html

Hongrie :
http://www.symantec.com/region/hu/techsupp/index.html

Pour les solutions de service et de support dans d'autres pays, visitez le site suivant et sélectionnez votre région.

http://www.symantec.com/globalsites.html

Tous les efforts ont été fournis pour garantir la précision de ces informations. Celles-ci peuvent toutefois faire l'objet de modifications sans préavis. Symantec Corporation se réserve le droit d'apporter de telles modifications sans avertissement préalable.