

**Les cybercriminels  
constituent une menace  
pour votre sécurité !**

Accepter

Refuser

**Logiciels espions, virus, etc.**  
Menaces Internet

**Norton**<sup>™</sup>  
from symantec



NO

---

## Sommaire

---

Cela vous concerne aussi	4-5
Cybercriminalité – les faits	6-7
Menaces Internet – des bots aux vers	9-17
5 cas incroyables de cybercriminalité	18-19
Symantec Global Intelligence Network	20-21
10 conseils des experts de la sécurité	22-23

---

# Cela vous concerne aussi.

---

Le réseau Internet nous permet de nous connecter à des ordinateurs situés partout dans le monde. Un simple clic suffit pour joindre une autre personne où qu'elle se trouve. Toutefois, c'est un peu comme partir en vacances : il y a beaucoup à découvrir, mais aussi malheureusement de nombreux dangers.

**Aujourd'hui encore, de nombreux internautes n'ont pas conscience des dangers qui les menacent sur Internet. Un utilisateur sur 20 a été victime d'un vol de données personnelles ayant occasionné une perte financière. Sans oublier que ce chiffre ne prend pas en compte les désagréments que peuvent provoquer les programmes malveillants tels que les virus ou les vers.**

La mission de Norton est d'avertir les utilisateurs et de protéger ses clients contre les menaces véhiculées par Internet. Nous ne voulons pas que les cybercriminels puissent vous empêcher de surfer sur le Web en toute liberté.

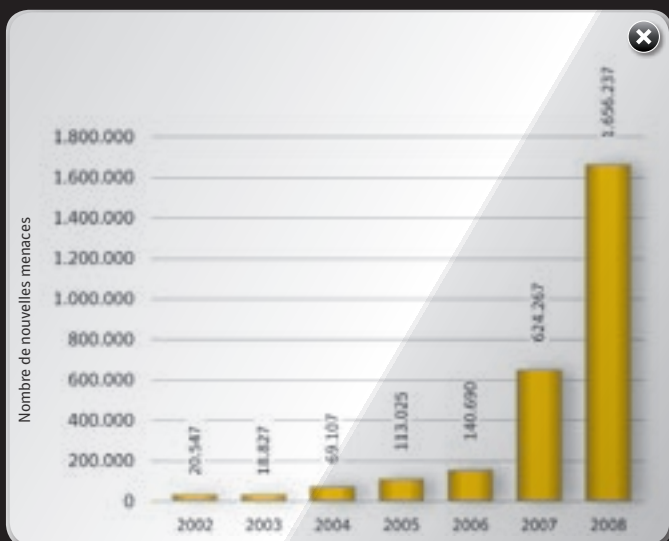
**Vous pouvez nous aider dans cette lutte en lisant cette brochure consacrée aux menaces Internet et en réagissant en conséquence. Après tout, cela ne concerne pas seulement votre ordinateur. Cela vous concerne aussi.**



# Cybercriminalité – les faits

La cybercriminalité est en plein développement. En 2008, Symantec a identifié sur Internet plus de 1,6 million de nouveaux codes malveillants tels que des virus, des chevaux de Troie ou des logiciels espions.

## Augmentation du nombre de logiciels malveillants :



Source : 14e édition du Symantec Global Internet Security Threat Report, avril 2009

---

## Quelques données clés à propos de la cybercriminalité :

- En 2008, l'office fédéral allemand de police criminelle a enregistré **167 451 actes criminels commis "au moyen d'Internet"** sur le seul territoire allemand. Le nombre de cas non signalés est bien plus élevé.
- Dans son rapport intitulé "Situation de la sécurité informatique en Allemagne en 2009", l'office fédéral allemand pour la sécurité informatique (BSI) a décrit la situation comme étant "extrêmement grave" et "pire que prévue".
- Selon le rapport du BSI, on compte à ce jour près de **4 millions de victimes** de la cybercriminalité en Allemagne.
- D'après le rapport "Symantec Global Internet Security Threat Report" (2009), **une moyenne de 75 158 ordinateurs a été infectée par des bots actifs** chaque jour en 2008.
- En 2007, les internautes se connectant à partir du territoire allemand ont été victimes de pertes financières d'un montant supérieur à 19 millions d'euros en raison d'actes de phishing. Ce montant a été fourni par le BITKOM, l'association allemande des entreprises du secteur de l'informatique.
- En 2008, **62 milliards de messages de spam** ont été envoyés dans le monde entier. Ils ont provoqué le gaspillage de 33 milliards de kilowattheures, soit suffisamment d'énergie pour alimenter une ville de 2,4 millions d'habitants pendant un an ! Ces calculs ont été réalisés par les spécialistes du climat de la société de consulting ICF International.



# Menaces Internet – des bots aux vers

---

Plus les fonctionnalités d'Internet sont variées, plus les menaces présentes sur le Web le sont également. Les opportunités offertes aux pirates et aux voleurs de données ne cessent de se développer. Qui plus est, les cybercriminels ont de plus en plus tendance à combiner les différentes techniques qu'ils utilisent.

---

Selon le dernier rapport (2009) de l'office fédéral allemand pour la sécurité informatique (BSI), "un cheval de Troie peut par exemple avoir des fonctionnalités de porte dérobée et de logiciel espion, utiliser un enregistreur de frappe et connecter l'ordinateur infecté à un réseau de bots".

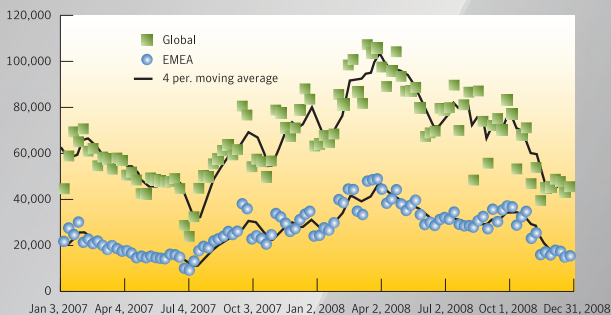
**Le BSI souligne également que "les criminels peuvent désormais très facilement créer des programmes malveillants ou adapter des versions existantes en fonction de leurs besoins".**

Les pages suivantes contiennent une rapide description des principales menaces véhiculées par Internet.

# Bots

Selon un rapport de l'organisation gouvernementale internationale OCDE, les cybercriminels ont déjà levé des "armées de zombies" et contrôlent plus d'un million d'ordinateurs.

Les bots exploitent les failles de sécurité afin de s'installer sur les ordinateurs et de les transformer en "zombies". Les pirates peuvent alors contrôler ces ordinateurs à distance et les utiliser par exemple pour l'envoi en masse de messages de spam. Il est même possible de louer des réseaux de bots existants hébergés sur des serveurs "souterrains". Le tarif est d'environ 500 euros pour un réseau capable d'envoyer 10 millions de messages de spam.



Selon Symantec, 4 776 967 ordinateurs infectés par des bots actifs ont été découverts dans la zone EMEA (Europe, Moyen-Orient et Afrique) au cours de l'année 2008.

## Le commerce des données personnelles

On estime que la vente des données volées rapporte 200 millions d'euros chaque année aux cybercriminels.

Numéros de cartes de crédit, coordonnées bancaires ou identités complètes : tout se vend sur le marché noir d'Internet. Des serveurs "souterrains" permettent aux amateurs d'acheter les informations d'une carte de crédit pour quelques centimes seulement. Le prix des coordonnées bancaires varie de 7,50 euros à 750 euros, en fonction du montant disponible sur le compte.

## Téléchargements insidieux

En moyenne, plus de 13 000 sites Web infectés sont identifiés chaque jour.

Des voleurs de données placent des codes malveillants invisibles sur des sites Web. Les internautes utilisent ces sites en toute confiance et finissent par installer des logiciels espions sur leur ordinateur sans s'en rendre compte. Les criminels peuvent alors espionner leurs informations privées et leurs mots de passe.

## Vol d'identité



Le rapport du BSI dresse un constat sans appel : "Les dommages dans le monde entier se chiffrent déjà en milliards, et le problème ne cesse de prendre de l'ampleur".

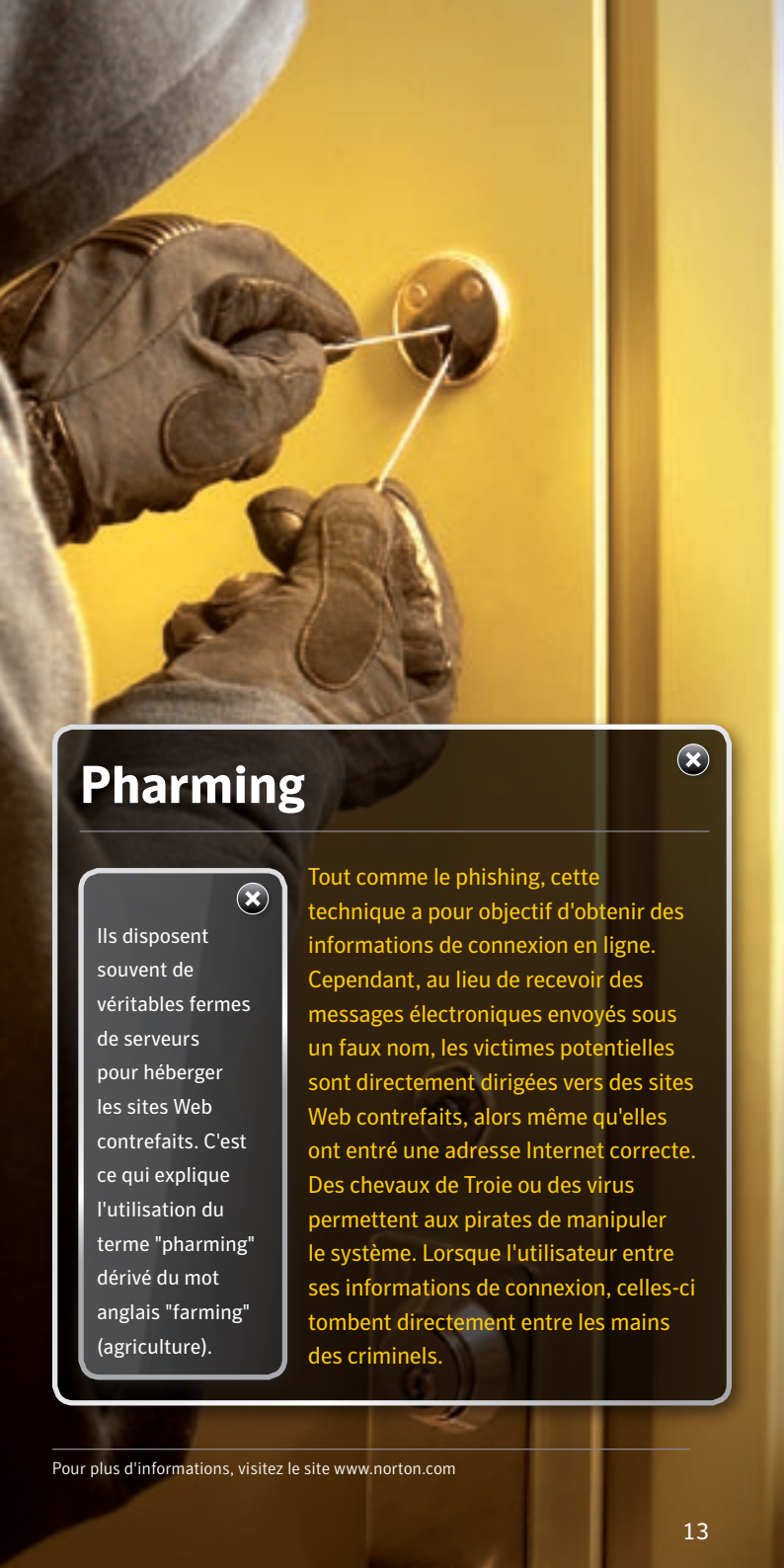
Les criminels souhaitent voler et utiliser vos données personnelles. Il s'agit souvent d'informations obtenues à partir de cartes de crédit ou à l'occasion de l'utilisation de services bancaires en ligne. Cependant, les dates de naissance, les adresses et les numéros de permis de conduire peuvent également être volés et utilisés par exemple dans le cadre de transactions frauduleuses sur des sites de vente en ligne.

## Utilisation d'enregistreurs de frappe



Les enregistreurs de frappe sont souvent proposés et vendus au marché noir sur certains sites Web.

Cette technique est particulièrement sournoise. Les criminels installent un code malveillant sur un ordinateur et peuvent ensuite enregistrer, lettre par lettre, chacun des mots saisis au clavier par la victime.



## Pharming

Ils disposent souvent de véritables fermes de serveurs pour héberger les sites Web contrefaits. C'est ce qui explique l'utilisation du terme "pharming" dérivé du mot anglais "farming" (agriculture).

Tout comme le phishing, cette technique a pour objectif d'obtenir des informations de connexion en ligne. Cependant, au lieu de recevoir des messages électroniques envoyés sous un faux nom, les victimes potentielles sont directement dirigées vers des sites Web contrefaits, alors même qu'elles ont entré une adresse Internet correcte. Des chevaux de Troie ou des virus permettent aux pirates de manipuler le système. Lorsque l'utilisateur entre ses informations de connexion, celles-ci tombent directement entre les mains des criminels.

# Phishing



Toujours en 2008, Symantec a identifié 55 389 sites Web de phishing, soit 68 % de plus qu'en 2007.

Les fraudeurs s'y présentent comme des personnes dignes de confiance afin de pouvoir accéder à des données sensibles. Ils utilisent souvent des sites Web contrefaits pour tenter d'arracher à leurs victimes mots de passe ou codes de transactions. Ces criminels communiquent généralement par courrier électronique ou par messagerie instantanée.

# Messages de spam



Selon la société de consulting ICF, plus de 150 milliards de messages de spam ont été envoyés chaque jour au cours de l'année 2008.

Ces messages indésirables saturent nos boîtes aux lettres et sont pour la plupart envoyés via des ordinateurs piratés (réseaux de bots). Les autorités fédérales allemandes ont effectué des statistiques au niveau de la passerelle de leur réseau : sur 100 messages reçus, le nombre moyen de messages bienvenus ne s'élevait qu'à 1,5. Les messages de spam contiennent une grande variété d'offres, des concours aux médicaments en passant par des promesses de gains financiers.



## Logiciels espions

Les logiciels espions peuvent également enregistrer et transmettre des noms d'utilisateurs et des mots de passe.

Ces types de programmes espionnent les habitudes de navigation de leurs victimes sur Internet afin de créer des profils d'utilisateurs. Bien souvent, ces informations sont ensuite vendues à des sociétés qui les utilisent pour faire de la publicité ciblée.

## Chevaux de Troie

Les chevaux de Troie constituent la principale menace sur Internet. Nombre d'entre eux s'installent de manière à être automatiquement activés lors du démarrage de l'ordinateur.

Les chevaux de Troie s'installent secrètement et permettent à un pirate de prendre le contrôle des ordinateurs infectés. Il s'agit du principal outil que les criminels utilisent pour voler des mots de passe ou espionner une victime de manière ciblée. Les chevaux de Troie se répandent souvent par l'intermédiaire des pièces jointes aux courriers électroniques.

## Vers

N'oublions pas non plus les vers qui affectent désormais à présent les téléphones portables ! La plupart d'entre eux infectent tous les téléphones environnants à l'aide de la fonction Bluetooth.

Un ver infecte un ordinateur de la même manière qu'un virus. Cependant, il cherche activement à se répandre via les réseaux informatiques ou le courrier électronique.



# 5 cas incroyables de cybercriminalité

Bien souvent, les actes des cybercriminels et les préjudices qu'ils occasionnent pour les personnes qui en sont victimes ne font l'objet d'aucune médiatisation. Pourtant, il arrive aussi que des cas incroyables défraient la chronique et impressionnent l'opinion publique. Nous avons choisi de vous présenter 5 cas.

## 1 Un vol de données rapporte 11 millions de dollars

En août 2008, le département américain de la Justice décide d'engager des poursuites à l'encontre de 11 pirates informatiques. Ces personnes étaient accusées d'avoir volé plus de 40 millions de cartes de crédit. Les données provenaient des cartes utilisées par les clients de plusieurs chaînes de magasins. Après avoir été acquises, ces données étaient chiffrées et placées sur des serveurs situés aux Etats-Unis et en Europe de l'Est à partir desquels elles étaient vendues. Ces activités illégales auraient permis à l'un des accusés de gagner à lui seul 11 millions de dollars.

## 2 Un virus paralyse un gouvernement régional

Le virus Conficker est apparu en octobre 2008. En janvier 2009, il a notamment paralysé 3 000 postes de travail du gouvernement régional de Carinthie (Autriche) pendant plusieurs jours. Peu de temps après, le site SpiegelOnline a annoncé que 50 millions d'ordinateurs étaient infectés dans le monde entier. Les forces armées allemandes et l'armée de l'air française étaient également touchées. Microsoft, l'Université de Bonn et Symantec ont fourni des outils spéciaux pour éliminer ce virus.

### **3 Des gangsters vendent "leurs chansons" pour 537 000 euros**

Le magazine britannique en ligne The Register a relaté le fait divers suivant : un groupe de fraudeurs, aidé par une entreprise américaine, a placé quelques chansons autoproduites sur les sites de vente en ligne Amazon et Apple iTunes. Ils ont ensuite acheté leurs propres chansons pour un montant équivalent à 537 000 euros. En tant qu'artistes, ils ont obtenu 214 000 euros de royalties de la part des exploitants des sites. Au premier abord, l'opération était totalement légale. Toutefois, les informations des cartes bancaires utilisées avaient été volées.

### **4 Un étudiant philippin provoque des milliards de dommages**

C'est au cours de l'année 2000 que le légendaire virus Loveletter est apparu. L'objet du message était "I Love You". Ce virus a détruit d'énormes quantités de données sur les ordinateurs infectés. Les dommages se sont chiffrés en milliards dans le monde entier. L'auteur du virus était vraisemblablement un étudiant philippin frustré.

### **5 Une célébrité victime d'un cheval de Troie pornographique sur Twitter**

Les 140 000 "suiveurs" de Guy Kawasaki sur Twitter ont été très étonnés lorsque le jeune entrepreneur bien connu aux Etats-Unis a publié sur Twitter un lien permettant d'accéder à un site pornographique. Son site était infecté par un cheval de Troie capable d'attaquer à la fois les PC sous Windows et les Mac d'Apple. Des cybercriminels avaient piraté le compte Twitter de Guy Kawasaki et en avaient pris le contrôle. Selon des experts de l'Université d'Alabama, près de 2 000 "suiveurs" de l'entrepreneur auraient été victimes du dangereux lien.

# Symantec Global Intelligence Network : **240 000 capteurs dans 200 pays**

---

---

**Pour pouvoir se protéger efficacement, il est nécessaire de connaître ses ennemis.** C'est la raison pour laquelle Symantec utilise son réseau Global Intelligence Network pour collecter des données complètes sur les menaces en ligne. 240 000 capteurs recueillent des informations actualisées sur l'état des menaces et alimentent ce réseau dans plus de 200 pays.

Plus de 130 millions de clients, de serveurs et de passerelles protégés par des antivirus fournissent des informations sur les codes malveillants existants. Symantec Probe Network collecte des données sur les tendances en matière de spam et de phishing et utilise pour cela environ 2,5 millions de comptes leurres et l'infrastructure de MessageLabs.

Ce système permet d'analyser plus de 8 milliards de courriers électroniques et plus d'un milliard de requêtes Web dans plus de 86 pays.

---

Source : 14e édition du Symantec Global Internet Security Threat Report, avril 2009

---

Pour plus d'informations, visitez le site [www.norton.com](http://www.norton.com)



# 10 conseils à suivre pour utiliser Internet en toute sécurité

---

Comment vous protéger ? Candid Wüest, qui figure au rang des experts en sécurité chez Symantec, sait ce que vous devez faire pour vous protéger contre les menaces. Les 10 conseils suivants sont immédiatement efficaces et peuvent être mis en œuvre facilement et rapidement. Ils vous permettront d'utiliser Internet en toute sécurité.

---

**1 Ne stockez pas de données d'accès ou de mots de passe dans votre navigateur Internet.**

Les navigateurs ont eux aussi des points faibles que les cybercriminels n'hésitent pas à exploiter. En un rien de temps, les données stockées sont volées et vendues sur Internet.

**2 Les mots de passe ne doivent pas être trop simples et doivent être modifiés régulièrement.**

Les mots de passe composés d'une date de naissance, d'un prénom d'enfant ou de tout autre mot facile à rechercher ne sont pas recommandés. Il est préférable d'utiliser une combinaison de chiffres, de caractères spéciaux et de lettres en majuscules et en minuscules.

**3 N'utilisez pas les liens contenus dans les courriers électroniques provenant d'expéditeurs inconnus ou qui prétendent vous connaître.**

Il peut s'agir d'une tentative de phishing utilisant un site Web contrefait. Les pages contrefaites sont souvent de très bonne qualité et il est difficile de les distinguer des pages qu'elles imitent. Il est préférable de ne pas utiliser les liens qu'elles contiennent, d'entrer l'adresse du site Web manuellement en la contrôlant soigneusement.

**4 Lorsque vous faites des achats ou utilisez des services bancaires en ligne, assurez-vous que les données sont transmises sous forme chiffrée.**

Une connexion est sécurisée lorsque le texte "https" (hypertext transfer protocol secure) figure dans l'adresse Internet. Lorsque vous faites des achats en ligne, les données doivent toujours être transmises via un serveur sécurisé, par exemple avec la technologie SSL (Secure Sockets Layer).

**5 Ne surfez pas sur le Web si vous êtes connecté à votre ordinateur en tant qu'administrateur. Créez plutôt un profil d'utilisateur fictif.**

Il vous suffit de sélectionner l'option Comptes d'utilisateurs dans le Panneau de configuration et de créer un compte. Cela ne vous prendra qu'une minute...

---



**6** **Contrôlez régulièrement les données présentes sur votre ordinateur et sauvegardez-les.**

De nombreuses données personnelles et financières sont stockées sur les ordinateurs. Est-il vraiment nécessaire qu'elles s'y trouvent en permanence ? Archivez ces données sur DVD, sur un disque dur externe ou sur une carte mémoire. Mieux encore, archivez-les deux fois. Vous disposerez ainsi d'une copie de sauvegarde. Supprimez ensuite le plus grand nombre possible de données de votre ordinateur. Là où il n'y a pas de données, rien ne peut être volé.

**7** **Afin que vos logiciels et vos navigateurs Internet puissent toujours bénéficier des derniers correctifs, pensez à télécharger régulièrement les mises à jour.**

Internet continue à se développer à un rythme effréné et de nouvelles menaces apparaissent. La mise à jour régulière des programmes et des systèmes d'exploitation corrige les failles que les codes malveillants peuvent exploiter.

**8** **Vous devez également faire preuve de prudence sur les sites de réseaux sociaux.**

Après tout, vous n'accepteriez pas qu'un inconnu croisé dans la rue devienne votre "nouvel ami". Pour chaque personne à laquelle vous décidez d'accorder une autorisation d'accès à vos données privées, interrogez-vous sur les données qui doivent être accessibles et sur celles qui ne doivent pas l'être. De même, au moment de vous connecter à nouveau au site, vérifiez que votre page publique ne contient pas trop de données...

**9** **Utilisez les ordinateurs dits publics avec prudence (dans les cybercafés, les bars, les hôtels ou les aéroports).**

Faites en sorte de ne pas entrer de données personnelles sur ces ordinateurs, par exemple des numéros de comptes, des mots de passe ou des codes secrets. Ces données risqueraient de se retrouver rapidement en de mauvaises mains. Evitez donc dans ce cas d'utiliser des services bancaires en ligne. De plus, si vous utilisez votre ordinateur portable en dehors de votre domicile, n'oubliez pas de le "vacciner". Le logiciel de sécurité, le pare-feu et les divers autres outils assurant sa protection doivent toujours être parfaitement à jour.

**10** **Compte tenu des menaces actuelles, il est essentiel que chaque ordinateur soit protégé par un logiciel de sécurité Internet.**

Ce produit doit proposer les fonctionnalités suivantes : une protection contre les virus, le phishing, le pharming, le spam, les bots, les logiciels espions et les rootkits, ainsi qu'un pare-feu, une protection du navigateur et une fonction de détection proactive basée sur l'analyse comportementale. Toutes ces fonctionnalités sont disponibles dans Norton Internet Security. Ce logiciel vous permet également de gérer plusieurs identités en ligne.



**Cela ne concerne pas  
seulement votre ordinateur.  
Cela vous concerne aussi.**

---

Accepter

Refuser

Copyright © 2009 Symantec Corporation.

Tous droits réservés. Symantec, le logo Symantec, Norton, Norton Internet Security et Norton AntiVirus sont des marques commerciales ou des marques déposées de Symantec Corporation ou de ses filiales aux Etats-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs.