

Kaspersky Internet Security for Mac

KASPERSKY **lab**

Manuel de l'utilisateur

VERSION DE L'APPLICATION : 15.0

Cher utilisateur,

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce document vous sera utile et qu'il répondra à la majorité des questions que vous pourrez vous poser.

Attention ! Ce document demeure la propriété de Kaspersky Lab et il est protégé par les législations de la Fédération de Russie et les accords internationaux sur les droits d'auteur. Toute copie ou diffusion illicite de ce document, en tout ou en partie, est passible de poursuites civiles, administratives ou judiciaires conformément aux lois applicables.

La copie sous n'importe quelle forme et la diffusion, y compris la traduction, de n'importe quel document sont admises uniquement sur autorisation écrite de Kaspersky Lab.

Ce document et les illustrations qui l'accompagnent peuvent être utilisés uniquement à des fins personnelles, non commerciales et à titre d'information.

Ce document peut être modifié sans préavis. La version la plus récente du manuel est disponible sur le site de Kaspersky Lab, à l'adresse suivante : <http://www.kaspersky.com/fr/docs>.

Kaspersky Lab ne pourra être tenue responsable du contenu, de la qualité, de l'actualité et de l'exactitude des textes utilisés dans ce manuel et dont les droits appartiennent à d'autres entités. La responsabilité de Kaspersky Lab en cas de dommages liés à l'utilisation de ces textes ne pourra pas non plus être engagée.

Date d'édition : 30/10/2014

© 2014 Kaspersky Lab ZAO. Tous droits réservés.

<http://www.kaspersky.com/fr/>
<http://support.kaspersky.com/fr>

TABLE DES MATIERES

PRESENTATION DU MANUEL.....	6
Dans ce document	6
Conventions.....	8
SOURCES D'INFORMATIONS SUR L'APPLICATION.....	9
Sources d'informations pour une recherche indépendante.....	9
Discussion des applications de Kaspersky Lab sur le forum.....	10
KASPERSKY INTERNET SECURITY	11
Présentation de Kaspersky Internet Security	11
Distribution.....	13
Service pour les utilisateurs	13
Configuration matérielle et logicielle.....	13
INSTALLATION ET SUPPRESSION DE L'APPLICATION	14
Préparatifs pour l'installation de l'application.....	14
Procédure d'installation de l'application.....	14
Téléchargement de l'application suivi de son installation depuis le portail My Kaspersky	15
Présentation du compte d'utilisateur d'accès au portail My Kaspersky	16
A propos du portail My Kaspersky	16
Installation de l'application depuis une distribution.....	17
Préparation de l'application au travail.....	18
Suppression de l'application	18
INTERFACE DE L'APPLICATION	19
Icône de Kaspersky Internet Security	19
Fenêtre principale de l'application	20
Fenêtre de configuration de l'application	21
Fenêtre de configuration du Contrôle Parental.....	22
Fenêtre Protection bancaire.....	22
Fenêtres de notification et fenêtres contextuelles	23
Présentation des fenêtres de notification.....	23
Présentation des types d'événement	24
Présentation des fenêtres contextuelles.....	24
Désactivation des notifications.....	24
Kiosque d'informations	25
LICENCE DE L'APPLICATION.....	26
Présentation du Contrat de licence	26
Présentation de la licence.....	26
Présentation de l'abonnement.....	27
Présentation du code d'activation.....	28
Présentation de la clé.....	28
Présentation des données proposées	29
Consultation des informations relatives à la licence	32
Achat d'une licence	32
Renouvellement de la licence	33
Renouvellement de l'abonnement	33
Mise à jour de l'état de l'abonnement	34

Activation de Kaspersky Internet Security.....	34
Activation de la version d'évaluation de l'application.....	34
Activation de l'application à l'aide du code d'activation.....	35
LANCEMENT ET ARRÊT DE L'APPLICATION.....	37
ÉTAT DE LA PROTECTION DE L'ORDINATEUR.....	38
Évaluation de l'état de la protection de l'ordinateur.....	38
Désactivation de la protection de l'ordinateur.....	39
Rétablissement de la protection de l'ordinateur.....	40
Utilisation du Centre de Protection.....	40
RESOLUTION DES PROBLEMES TYPES.....	42
Procédure d'exécution d'une analyse complète de l'ordinateur.....	42
Réalisation d'une analyse rapide de l'ordinateur.....	43
Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque.....	43
Procédure d'achat d'une licence.....	43
Procédure de renouvellement de la licence.....	44
Procédure de mise à jour des bases de l'application.....	44
Procédure de protection contre l'interception des données saisies à l'aide du clavier traditionnel.....	45
Comment protéger les transactions financières et les achats en ligne sur le site Internet de la banque, le système de paiement ou les boutiques en ligne.....	45
Procédure de restriction de la durée de navigation de l'enfant ou de l'adolescent sur Internet.....	46
Restriction des consultations de sites Internet et du téléchargement de fichiers pour les enfants ou les adolescents.....	47
Restriction des contacts et des communications sur les réseaux sociaux pour les enfants ou les adolescents.....	48
Procédure d'interdiction du transfert de données personnelles pour les enfants ou les adolescents.....	48
Que faire si l'application a bloqué l'accès au fichier.....	49
Procédure de restauration d'un fichier supprimé ou réparé par l'application.....	50
Emplacement du rapport sur le fonctionnement de l'application.....	50
Que faire en cas d'affichage de fenêtres de notification et de messages contextuels.....	50
UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE.....	51
Consultation de l'aide.....	52
Recherche de virus.....	52
Mise à jour de l'application.....	54
Annulation de la dernière mise à jour.....	55
Lancement/arrêt d'un composant ou d'une tâche.....	55
Statistiques du fonctionnement du composant ou de la tâche.....	56
Exportation des paramètres de protection.....	56
Importation des paramètres de protection.....	57
Arrêt de l'application.....	57
Codes de retour de la ligne de commande.....	57
CONTACTER LE SUPPORT TECHNIQUE.....	58
Modes d'obtention du support technique.....	58
Support technique par téléphone.....	58
Support technique via le portail My Kaspersky.....	59
Utilisation du fichier de traçage.....	59
Création d'un fichier de traçage.....	60
Envoi des fichiers comportant des informations sur l'erreur à Kaspersky Lab.....	60

GLOSSAIRE	61
KASPERSKY LAB.....	63
INFORMATIONS SUR LE CODE TIERS.....	64
NOTIFICATIONS SUR LES MARQUES DE COMMERCE	65
INDEX.....	66

PRESENTATION DU MANUEL

Ce document représente le Manuel de l'utilisateur de Kaspersky Internet Security for Mac.

Pour une utilisation réussie de Kaspersky Internet Security, les utilisateurs doivent posséder les connaissances d'utilisation de l'interface du système d'exploitation Mac OS X, maîtriser les principales tâches, maîtriser le courrier électronique et Internet.

Le guide est conçu pour les buts suivants :

- Aider à installer Kaspersky Internet Security, activer et utiliser l'application.
- Offrir un accès rapide aux informations pour répondre aux questions liées à Kaspersky Internet Security.
- Présenter les sources complémentaires d'informations sur l'application et les méthodes pour obtenir une assistance technique.

DANS CETTE SECTION

Dans ce document.....	6
Conventions.....	8

DANS CE DOCUMENT

Les sections suivantes sont incluses dans le Manuel de l'utilisateur de Kaspersky Internet Security :

Sources d'informations sur l'application (à la page [9](#))

Cette section décrit les sources d'informations relatives à l'application.

Kaspersky Internet Security (à la page [11](#))

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Internet Security. Elle reprend la configuration matérielle et logicielle requise pour l'application, ainsi que les informations relatives au service pour les utilisateurs.

Installation et suppression de l'application (à la page [14](#))

Cette section explique, étape par étape, comment installer et désinstaller Kaspersky Internet Security.

Interface de l'application (à la page [19](#))

Cette section décrit les principaux éléments de l'interface utilisateur graphique de Kaspersky Internet Security : icône de l'application et son menu contextuel, fenêtre principale, fenêtre des paramètres de l'application, fenêtre Contrôle Parental, fenêtre Protection bancaire et kiosque d'informations. Cette section contient également des informations sur les fenêtres de notification et les messages contextuels.

Licence de l'application (à la page [26](#))

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du contrat de licence, les modes d'activation de l'application et le renouvellement de la durée de validité de la licence.

Lancement et arrêt de l'application (à la page [37](#))

Cette rubrique explique comment lancer et arrêter l'application.

Etat de la protection de l'ordinateur (à la page [38](#))

Cette section explique comment déterminer la présence de problèmes et de menaces contre la sécurité de l'ordinateur et comment configurer le niveau de protection. Vous apprendrez également à activer ou désactiver la protection pendant l'utilisation de l'application.

Résolution des problèmes types (à la page [42](#))

Cette section explique comment exécuter pas à pas les principales fonctions de l'application.

Utilisation de l'application au départ de la ligne de commande (à la page [51](#))

Cette section décrit l'utilisation de Kaspersky Internet Security via la ligne de commande.

Contacter le Support technique (à la page [58](#))

Cette section décrit les modes de support technique et les conditions nécessaires pour bénéficier du Support technique.

Glossaire

Cette section contient la liste des termes qui apparaissent dans le document, et leurs définitions.

Kaspersky Lab (à la page [63](#))

Cette section contient les informations sur Kaspersky Lab ZAO.

Informations sur le code tiers (à la page [64](#))

Cette section contient des informations sur le code tiers utilisé dans l'application.

Notifications sur les marques de commerce (à la page [65](#))

Cette section énumère les marques de commerce des propriétaires tiers, utilisées dans le document.

Index

Cette section permet de trouver rapidement les informations souhaitées dans le document.

CONVENTIONS

Le présent document respecte des conventions (cf. tableau ci-dessous).

Tableau 1. Conventions

EXEMPLE DE TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que ...	Les avertissements apparaissent en rouge et sont encadrés. Ils contiennent des informations sur les actions pouvant avoir des conséquences indésirables.
Il est conseillé d'utiliser ...	Les remarques sont encadrées. Les remarques contiennent des informations complémentaires ou d'aide.
Exemple: ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".
<i>Mise à jour – est...</i> L'événement <i>Bases dépassées</i> survient.	Les éléments de texte suivants apparaissent en italique : <ul style="list-style-type: none"> • nouveaux termes ; • noms des états et des événements de l'application.
Command-A.	Les noms des touches du clavier sont en caractères mi-gras. Deux noms de touche unis par le caractère "-" (moins) représentent une combinaison de touches.
Cliquez sur le bouton Activer .	Les noms des éléments de l'interface de l'application, par exemple, les champs de saisie, les options du menu, les boutons, sont en caractères mi-gras.
➡ <i>Pour planifier une tâche, procédez comme suit :</i>	Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".
kav update	Les types suivants du texte apparaissent dans un style spécial : <ul style="list-style-type: none"> • texte de la ligne de commande ; • texte des messages affichés sur l'écran par l'application ; • données à saisir à l'aide du clavier.
<adresse IP de votre ordinateur>	Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.

SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section décrit les sources d'informations relatives à l'application.

Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

Sources d'informations pour une recherche indépendante	9
Discussion des applications de Kaspersky Lab sur le forum	10

SOURCES D'INFORMATIONS POUR UNE RECHERCHE INDEPENDANTE

Vous pouvez vous servir des sources suivantes pour rechercher vous-même les informations sur l'application :

- la page sur le site Internet de Kaspersky Lab ;
- la page sur le site Internet du Support Technique (banque de solutions) ;
- aide électronique.

Si vous n'avez pas trouvé la solution à votre problème, nous vous conseillons de contacter le Support Technique de Kaspersky Lab. Pour pouvoir consulter les sources d'information sur le site Internet de Kaspersky Lab, il est nécessaire d'être connecté à Internet.

Page sur le site Internet de Kaspersky Lab

Le site Internet de Kaspersky Lab contient une page spécifique pour chaque application.

La page dédiée à Kaspersky Internet Security sur le site de Kaspersky Lab (<http://www.kaspersky.fr/mac-security>) permet de consulter les informations générales sur l'application, ses possibilités et particularités de fonctionnement.

La page <http://www.kaspersky.fr> contient un lien vers la boutique en ligne. Vous pouvez y acheter l'application ou renouveler la licence.

La page sur le site Internet du Support Technique (base de connaissances)

Base de connaissances est une section du site Internet du Support Technique contenant les recommandations de travail avec les applications de Kaspersky Lab. La base de connaissances comprend des articles d'aide classés par thème.

A la page de l'application dans la base de connaissances (<http://support.kaspersky.com/fr/kis15mac>), vous allez trouver des articles reprenant des informations utiles, recommandations et réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions concernant non seulement Kaspersky Internet Security, mais également d'autres applications de Kaspersky Lab, contenir les actualités du Support Technique.

Pour accéder à la Banque de solutions, ouvrez le menu principal de l'application (à la page [20](#)), cliquez sur le bouton  et dans la fenêtre qui s'ouvre, cliquez sur le bouton **Support Technique**.

Aide électronique

L'aide électronique de l'application est composée de fichiers de l'aide contextuel.

L'aide contextuelle contient les informations sur chaque fenêtre et sur l'onglet de Kaspersky Internet Security : la liste et la description des paramètres et la liste des tâches résolues.

DISCUSSION DES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs sur notre forum (<http://forum.kaspersky.com/index.php?showforum=129>).

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

KASPERSKY INTERNET SECURITY

Cette section décrit les fonctions, les modules et la distribution de Kaspersky Internet Security. Elle reprend la configuration matérielle et logicielle requise pour l'application, ainsi que les informations relatives au service pour les utilisateurs.

DANS CETTE SECTION

Présentation de Kaspersky Internet Security.....	11
Distribution	13
Service pour les utilisateurs	13
Configuration matérielle et logicielle	13

PRESENTATION DE KASPERSKY INTERNET SECURITY

Kaspersky Internet Security a été développé pour assurer la protection des ordinateurs régis par le système d'exploitation Mac OS X contre l'action des virus et autres programmes menaçant la sécurité de l'ordinateur.

Les composants suivants font partie du programme :

Anti-Virus Fichiers

Le module Anti-Virus Fichiers protège en temps réel le système de fichiers de l'ordinateur : il assure l'interception et l'analyse des requêtes adressées aux fichiers. Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés. Kaspersky Internet Security affiche par défaut une fenêtre de notification dans laquelle il faudra sélectionner l'action à réaliser sur l'objet détecté.

Anti-Virus Internet

Le module Anti-Virus Internet protège les informations entrantes et sortantes de votre ordinateur via les navigateurs Safari, Google Chrome™ et Firefox™, et les protocoles HTTP et HTTPS. Ce module inclut des extensions pour les navigateurs Internet que vous pouvez installer : il s'agit d'un module d'analyse des liens et d'un clavier virtuel. Le module d'analyse des liens analyse les liens présents sur les pages Internet ouvertes afin de déterminer s'il s'agit de liens de phishing ou de liens vers des URL malveillantes. Le clavier virtuel protège contre l'interception des données saisies.

Prévention des intrusions

Le module Prévention des intrusions protège votre ordinateur contre les intrusions dans le système d'exploitation. Ce module assure la protection contre les actions malveillantes exécutées par les malfaiteurs (par exemple, le balayage des ports et l'appairage des mots de passe). Il assure également la protection contre les actions entreprises par les programmes malveillants installés par les malfaiteurs sur l'ordinateur attaqué (par exemple, la communication de données protégées au malfaiteur).

Contrôle Parental

Ce composant Contrôle Parental permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur Internet. Il permet également de configurer, pour chaque utilisateur, une restriction du temps de navigation sur Internet, de limiter l'accès aux ressources et applications Internet, d'établir une liste de contacts autorisés ou interdits sur les réseaux sociaux et de contrôler le transfert de données pré-définies. En outre, le Contrôle Parental permet de consulter des rapports sur les actions des utilisateurs de l'ordinateur.

Protection bancaire

Le module Protection bancaire assure la protection des données de paiement et des opérations financières lors de l'utilisation des sites Internet des banques, des systèmes de paiement et des boutiques en ligne au paiement intégré (celles où vous saisissez les données de votre carte bancaire). Le module Protection bancaire s'appuie sur Kaspersky Security Network pour vérifier l'authenticité des sites Internet des banques, des systèmes de paiement ou des boutiques en ligne, ainsi que des certificats qui établissent les connexions sécurisées.

L'application offre les fonctions suivantes :

Analyse

Kaspersky Internet Security recherche et neutralise les virus et autres programmes menaçant la sécurité de l'ordinateur, à votre demande dans la zone d'analyse définie. Vous pouvez également configurer des actions que l'application doit exécuter sur les fichiers infectés ou potentiellement infectés. Kaspersky Internet Security affiche par défaut une fenêtre de notification dans laquelle il faudra sélectionner l'action à réaliser sur l'objet détecté. Kaspersky Internet Security exécute l'analyse complète de l'ordinateur, l'analyse rapide des zones importantes et l'analyse de la zone définie.

Mise à jour

Kaspersky Internet Security met à jour les bases anti-virus depuis les serveurs de mises à jour de Kaspersky Lab et crée une sauvegarde de tous les fichiers actualisés au cas où il serait nécessaire de revenir à l'état antérieur à la dernière mise à jour. L'application permet également de télécharger et d'installer automatiquement les nouvelles versions de Kaspersky Internet Security.

Quarantaine

Kaspersky Internet Security crée une copie du fichier infecté dans la quarantaine avant de le réparer ou de le supprimer. Vous pourrez ainsi restaurer ce fichier.

Rapports

Kaspersky Internet Security génère un rapport sur le fonctionnement des modules de la protection.

Notifications

Kaspersky Internet Security signale les événements qui surviennent au cours de son fonctionnement à l'aide de fenêtres de notification ou de messages contextuels. La fenêtre de notification peut être accompagnée de notifications sonores.

Centre de protection

Lors de son fonctionnement, Kaspersky Internet Security affiche des messages sur l'état de la protection dans la fenêtre Centre de protection. Le Centre de protection permet d'obtenir des informations sur l'état actuel de la protection de l'ordinateur et d'éliminer les problèmes et les menaces concernant la sécurité de ce dernier.

Administration à distance via le portail My Kaspersky

Le portail My Kaspersky permet d'administrer à distance la protection de l'ordinateur doté de Kaspersky Internet Security. Via ce portail, il est possible de : recevoir des informations sur l'état actuel de la protection de l'ordinateur et corriger à distance les problèmes et les menaces à l'encontre de la sécurité de l'ordinateur, activer et désactiver la protection des modules (Anti-virus Fichiers, Anti-virus Internet, prévention des intrusions), lancer l'analyse antivirus, mettre à jour les bases de l'application et administrer les licences de Kaspersky Internet Security.

DISTRIBUTION

Vous pouvez acheter l'application sous une des formes suivantes :

- Dans une boîte. Le produit est distribué via notre réseau de partenaires.
- Via la boutique en ligne. L'application peut être achetée dans la boutique en ligne de Kaspersky Lab (par exemple <http://www.kaspersky.com/fr>, section Boutique en ligne) ou du site d'un partenaire.

Si vous achetez le produit en boîte, vous recevez les éléments suivants :

- Bref manuel de l'utilisateur contenant les instructions pour télécharger et installer l'application, ainsi que le code d'activation de l'application ;
- Contrat de licence reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction de la région où l'application est diffusée.

Si vous achetez Kaspersky Internet Security via la boutique en ligne, vous devrez télécharger l'application depuis le site Internet. Les informations indispensables à l'activation de l'application, dont le code d'activation, sont envoyées par courrier électronique après le paiement.

Si vous achetez Kaspersky Internet Security sur le portail My Kaspersky, vous obtiendrez la version la plus récente de l'application. Les informations relatives à l'activation de l'application, y compris le code d'activation, apparaissent sur la page du portail My Kaspersky après l'achat. Vous les recevez également par courrier électronique. Vous pouvez également télécharger depuis My Kaspersky une version de l'application dotée d'un code d'activation prédéfini.

SERVICE POUR LES UTILISATEURS

En achetant une licence sur l'utilisation de l'application, vous pouvez obtenir les services suivants durant la durée de validité de la licence :

- Mise à jour des bases et offre des nouvelles versions de l'application ;
- Consultation par téléphone et courrier électronique sur toute question en rapport avec l'installation, la configuration et l'utilisation de l'application ;
- notification sur les nouvelles applications de Kaspersky Lab et les informations sur les nouveaux virus et les épidémies de virus. Afin de bénéficier de ce service, vous devez être abonné à la diffusion d'informations de Kaspersky Lab ZAO sur le site Internet du Support Technique.

Aucune consultation n'est offerte sur l'utilisation du système d'exploitation ou des logiciels ou technologies tiers.

CONFIGURATION MATERIELLE ET LOGICIELLE

Kaspersky Internet Security fonction sous la configuration matérielle et logicielle suivante :

- système d'exploitation Mac OS X 10.7, OS X 10.8, 10.9, 10.10 ;
- 500 Mo d'espace disponible sur le disque dur (selon la taille des bases antivirus).

INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section explique, étape par étape, comment installer et désinstaller Kaspersky Internet Security.

Le paquet d'installation de Kaspersky Internet Security contient le programme d'installation et le programme de suppression de Kaspersky Internet Security.

DANS CETTE SECTION

Préparatifs pour l'installation de l'application	14
Procédure d'installation de l'application	14
Préparation de l'application au travail	18
Suppression de l'application.....	18

PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Avant d'installer Kaspersky Internet Security sur l'ordinateur, il est recommandé d'exécuter toute une série d'actions de préparation :

- Assurez-vous que votre ordinateur correspond aux exigences système (cf. section "Configuration matérielle et logicielle" à la page [13](#)).
- Vérifier la connexion de votre ordinateur à Internet. Une connexion Internet est requise pour accéder au portail My Kaspersky (cf. section "A propos portail My Kaspersky" à la page [16](#)), télécharger une nouvelle version de Kaspersky Internet Security, activer l'application à l'aide du code d'activation et obtenir les mises à jour.
- Supprimer les autres applications antivirus de l'ordinateur pour éviter l'apparition des conflits de système et le ralentissement de la rapidité du système d'exploitation.

PROCEDURE D'INSTALLATION DE L'APPLICATION

L'installation de Kaspersky Internet Security sur l'ordinateur peut s'opérer d'une des manières suivantes :

- Téléchargement suivi de l'installation depuis le portail My Kaspersky (cf. section "Téléchargement de l'application et installation depuis le portail My Kaspersky" à la page [15](#)).

Utilisation du code utilisateur d'accès au portail My Kaspersky (cf. section "Présentation du compte d'utilisateur d'accès au portail My Kaspersky" à la page [16](#)). Permet de réaliser le téléchargement depuis le portail My Kaspersky (cf. section "A propos du portail My Kaspersky" à la page [16](#)) et d'installer une nouvelle version de Kaspersky Internet Security sur l'ordinateur.

- Installation de l'application depuis une distribution téléchargée sur le site de Kaspersky Lab ou d'un de ses partenaires (cf. section "Installation de l'application depuis une distribution" à la page [17](#)).

Exécuté via le programme d'installation. Permet de vérifier la présence éventuelle sur le portail My Kaspersky (cf. section "A propos du portail My Kaspersky" à la page. [16](#)) d'une nouvelle version de Kaspersky Internet Security, de la télécharger et de l'installer.

DANS CETTE SECTION

Téléchargement de l'application suivi de son installation depuis le portail My Kaspersky	15
Installation de l'application depuis une distribution	17

TELECHARGEMENT DE L'APPLICATION SUIVI DE SON INSTALLATION DEPUIS LE PORTAIL MY KASPERSKY

Les fenêtres **Contrat de licence** et **Participation au Kaspersky Security Network** du programme d'installation apparaissent uniquement lors de l'installation de Kaspersky Internet Security en allemand et en russe. Dans les autres cas, pour lire les textes du contrat de licence et les informations relatives à la participation au Kaspersky Security Network, il suffit de cliquer sur les liens correspondants dans la fenêtre du programme d'installation de Kaspersky Internet Security.

➔ Pour installer Kaspersky Internet Security depuis le portail My Kaspersky, procédez comme suit :

1. Connectez-vous au portail My Kaspersky (cf. section "A propos du portail My Kaspersky" à la page [16](#)) à l'aide de votre compte utilisateur (cf. section "Présentation du compte d'utilisateur d'accès au portail My Kaspersky" à la page [16](#)).

2. Téléchargez le fichier Kaspersky Internet Security.dmg. depuis le portail My Kaspersky.

La fenêtre comprenant la distribution s'ouvre automatiquement.

Si cette fenêtre n'apparaît pas, accédez au dossier qui contient le fichier Kaspersky Internet Security.dmg sur votre ordinateur et ouvrez-la manuellement.

3. Dans la fenêtre contenant la distribution, double-cliquez sur **Installer Kaspersky Internet Security**.

Le programme d'installation de Kaspersky Internet Security est lancé.

4. Cliquez sur le bouton **Télécharger et installer**.

Le programme d'installation télécharge la nouvelle version de Kaspersky Internet Security depuis le portail My Kaspersky et l'installe sur l'ordinateur.

5. Dans la fenêtre **Contrat de licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Internet Security, qui a été conclu entre vous et Kaspersky Lab. Une fois que vous avez lu le Contrat de licence, réalisez une des opérations suivantes :

- Si vous acceptez les termes du Contrat de licence, cliquez sur **Accepter**.

L'installation de Kaspersky Internet Security se poursuit.

- Si vous n'acceptez pas les termes du Contrat de licence, cliquez sur **Annuler**.

L'installation de l'application est interrompue.

6. Lisez les informations relatives à la participation au Kaspersky Security Network dans la fenêtre **Participation au Kaspersky Security Network**.

La participation à Kaspersky Security Network implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées et sur les applications signées téléchargées, ainsi que l'envoi d'un identifiant unique attribué à votre exemplaire de Kaspersky Internet Security et d'informations relatives au système. Aucune donnée personnelle n'est transmise.

- Si vous acceptez les dispositions relatives à l'utilisation de Kaspersky Security Network, cochez la case **J'accepte les conditions de participation à KSN**.

Si vous n'acceptez pas les conditions de participation à Kaspersky Security Network, ne cochez pas la case **J'accepte les conditions de participation à KSN**.

Sachez qu'à tout moment de votre utilisation de Kaspersky Internet Security vous pouvez décider de rejoindre le Kaspersky Security Network ou vous en retirer.

- Pour poursuivre l'installation de l'application, cliquez sur le bouton **Installer**.
- Confirmez l'installation de Kaspersky Internet Security dans la fenêtre de saisie des informations d'identification de l'administrateur de l'ordinateur.

L'installation de Kaspersky Internet Security sur l'ordinateur démarre.

- Cliquez sur **Terminer** pour arrêter l'installation de l'application.

Kaspersky Internet Security démarre automatiquement à l'issue de l'installation. Le redémarrage de l'ordinateur n'est pas requis.

PRESENTATION DU COMPTE D'UTILISATEUR D'ACCES AU PORTAIL MY KASPERSKY

Le compte utilisateur d'accès au portail My Kaspersky (cf. section "A propos du portail My Kaspersky" à la page [16](#)) est votre compte unique pour accéder à tous les services de Kaspersky Lab.

Pour créer un compte utilisateur ou entrer sur le portail My Kaspersky, ouvrez la fenêtre principale de l'application (à la page [20](#)), cliquez sur le bouton , puis cliquez sur le bouton **My Kaspersky** dans la fenêtre qui s'ouvre.

Le compte utilisateur d'accès au portail My Kaspersky est votre adresse de messagerie électronique et le mot de passe que vous avez indiqués lors de la création du compte utilisateur. Le mot de passe doit comporter au moins huit caractères, un chiffre et une lettre majuscule.

Après la création du compte utilisateur d'accès au portail My Kaspersky, vous recevrez un message avec un lien d'activation de votre compte utilisateur à l'adresse que vous aurez indiquée.

Une fois le compte utilisateur, vous pouvez l'utiliser pour accéder au portail My Kaspersky. Si vous n'activez pas le compte utilisateur via le lien du message dans un délai d'une semaine, le compte est supprimé.

Si vous possédez déjà un compte d'accès au portail My Kaspersky, vous pouvez l'utiliser avec Kaspersky Internet Security.

A PROPOS DU PORTAIL MY KASPERSKY

Le portail My Kaspersky constitue votre unique ressource en ligne pour la gestion de la protection de l'ensemble de vos périphériques et de vos licences Kaspersky Lab.

Le portail My Kaspersky vous permet d'acheter une licence ou d'en renouveler une pour l'utilisation de Kaspersky Internet Security, de télécharger une nouvelle version de l'application ou de consulter les informations sur les bases anti-virus utilisées par l'application. De même, vous pouvez administrer à distance la protection de l'ordinateur doté de Kaspersky Internet Security. Via ce portail, il est possible de : recevoir des informations sur l'état actuel de la protection de l'ordinateur et corriger à distance les problèmes et les menaces à l'encontre de la sécurité de l'ordinateur, activer et désactiver la protection des modules (Antivirus Fichiers, Antivirus Internet, prévention des intrusions), lancer l'analyse antivirus, mettre à jour les bases de l'application.

Pour entrer sur le portail My Kaspersky, il est nécessaire d'utiliser un compte utilisateur (cf. section "Présentation du compte d'utilisateur d'accès au portail My Kaspersky" à la page [16](#)).

INSTALLATION DE L'APPLICATION DEPUIS UNE DISTRIBUTION

Les fenêtres **Contrat de licence** et **Participation au Kaspersky Security Network** du programme d'installation apparaissent uniquement lors de l'installation de Kaspersky Internet Security en allemand et en russe. Dans les autres cas, pour lire les textes du contrat de licence et les informations relatives à la participation au Kaspersky Security Network, il suffit de cliquer sur les liens correspondants dans la fenêtre du programme d'installation de Kaspersky Internet Security.

► Pour installer Kaspersky Internet Security depuis une distribution, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Internet Security.

Si vous avez acheté Kaspersky Internet Security en ligne et que vous avez téléchargé la distribution au format DMG depuis le site de Kaspersky Lab, ouvrez le fichier dmg.

2. Dans la fenêtre contenant la distribution, double-cliquez sur **Installer Kaspersky Internet Security**.

Le programme d'installation de Kaspersky Internet Security est lancé. Le programme d'installation commence par vérifier s'il existe une version plus récente de Kaspersky Internet Security sur le portail My Kaspersky.

3. Choisissez l'action en fonction des résultats de la recherche d'une version plus récente :

- Si vous souhaitez ignorer la recherche d'une version plus récente de Kaspersky Internet Security sur le portail My Kaspersky, cliquez sur le bouton **Ignorer**, puis sur le bouton **Installer**.

Le programme d'installation commence à installer la version de Kaspersky Internet Security sur votre ordinateur depuis la distribution.

- Si le programme découvre une nouvelle version de Kaspersky Internet Security sur le portail My Kaspersky, vous pouvez la télécharger et l'installer. Pour ce faire, cliquez sur **Télécharger et installer**.
- Si le programme d'installation ne détecte pas de nouvelle version de Kaspersky Internet Security sur le portail My Kaspersky, vous pouvez installer la version depuis la distribution. Pour ce faire, cliquez sur le bouton **Installer**.

4. Dans la fenêtre **Contrat de licence**, lisez le texte du contrat de licence sur l'utilisation de Kaspersky Internet Security, qui a été conclu entre vous et Kaspersky Lab. Une fois que vous avez lu le Contrat de licence, réalisez une des opérations suivantes :

- Si vous acceptez les termes du Contrat de licence, cliquez sur **Accepter**.

L'installation de Kaspersky Internet Security se poursuit.

- Si vous n'acceptez pas les termes du Contrat de licence, cliquez sur **Annuler**.

L'installation de l'application est interrompue.

5. Lisez les informations relatives à la participation au Kaspersky Security Network dans la fenêtre **Participation au Kaspersky Security Network**.

La participation à Kaspersky Security Network implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées et sur les applications signées téléchargées, ainsi que l'envoi d'un identifiant unique attribué à votre exemplaire de Kaspersky Internet Security et d'informations relatives au système. Aucune donnée personnelle n'est transmise.

6. Si vous acceptez les dispositions relatives à l'utilisation de Kaspersky Security Network, cochez la case **J'accepte les conditions de participation à KSN**.

Si vous n'acceptez pas les conditions de participation à Kaspersky Security Network, ne cochez pas la case **J'accepte les conditions de participation à KSN**.

Sachez qu'à tout moment de votre utilisation de Kaspersky Internet Security vous pouvez décider de rejoindre le Kaspersky Security Network ou vous en retirer.

7. Pour poursuivre l'installation de l'application, cliquez sur le bouton **Installer**.
8. Confirmez l'installation de Kaspersky Internet Security dans la fenêtre de saisie des informations d'identification de l'administrateur de l'ordinateur.

L'installation de Kaspersky Internet Security sur l'ordinateur démarre.

9. Cliquez sur **Terminer** pour arrêter l'installation de l'application.

Kaspersky Internet Security démarre automatiquement à l'issue de l'installation. Le redémarrage de l'ordinateur n'est pas requis.

PREPARATION DE L'APPLICATION AU TRAVAIL

Après l'installation de Kaspersky Internet Security, il est conseillé de procéder comme suit :

- Activer Kaspersky Internet Security (cf. section "Activation de Kaspersky Internet Security" à la page [34](#)). L'activation de l'application vous permettra d'actualiser régulièrement les bases antivirus et les modules de l'application et assurera l'accès aux services du Support Technique.
- Evaluer l'état actuel de la protection de l'ordinateur (cf. section "Evaluation de l'état de la protection de l'ordinateur" à la page [38](#)).
- Mettre à jour Kaspersky Internet Security (cf. section "Procédure de mise à jour des bases et des modules de l'application" à la page [44](#)).
- Lancer une analyse complète de l'ordinateur sur les virus et sur les autres applications qui présentent une menace pour la sécurité de l'ordinateur (cf. section "Procédure d'exécution d'une analyse complète de l'ordinateur" à la page [42](#)).

SUPPRESSION DE L'APPLICATION

Si vous supprimez Kaspersky Internet Security, la sécurité de votre ordinateur et de vos données risque d'être menacée.

➡ Pour supprimer Kaspersky Internet Security, procédez comme suit :

1. Ouvrez le contenu du fichier d'installation de Kaspersky Internet Security.
Si vous avez acheté Kaspersky Internet Security en ligne et que vous avez téléchargé la distribution au format DMG depuis le site de Kaspersky Lab, ouvrez le fichier dmg.
2. Dans la fenêtre contenant la distribution, double-cliquez sur **Supprimer Kaspersky Internet Security**.
Le programme d'installation de Kaspersky Internet Security se lance. Suivez les étapes du programme de suppression pour supprimer Kaspersky Internet Security.
3. Dans la fenêtre **Introduction**, cliquez sur le bouton **Supprimer**.
4. Confirmez la suppression de l'application dans la fenêtre de saisie des informations d'identification de l'administrateur de l'ordinateur.
La suppression de Kaspersky Internet Security démarre.
5. Dans la fenêtre **Fin**, lisez les informations sur la fin du processus de suppression et cliquez sur le bouton **Terminer** pour quitter le programme de suppression.

Il n'est pas nécessaire de redémarrer l'ordinateur après la suppression de Kaspersky Internet Security.

INTERFACE DE L'APPLICATION

DANS CETTE SECTION

Icône de Kaspersky Internet Security	19
Fenêtre principale de l'application	20
Fenêtre de configuration de l'application.....	21
Fenêtre de configuration du Contrôle Parental	22
Fenêtre Protection bancaire	22
Fenêtres de notification et fenêtres contextuelles.....	23
Kiosque d'informations.....	25

ICONE DE KASPERSKY INTERNET SECURITY

Juste après l'installation de Kaspersky Internet Security, son icône apparaît dans la barre de menus. L'icône de l'application indique l'état de fonctionnement de l'application. Si l'icône de l'application est active, cela signifie que la protection en temps réel du système de fichiers de l'ordinateur contre les programmes malveillants est activée. L'icône de l'application inactive indique que la protection est désactivée.

L'icône de Kaspersky Internet Security se trouve toujours dans la barre de menus. Si l'une des fenêtres de l'application est ouverte, l'icône de Kaspersky Internet Security apparaît également dans le **Dock**.

Le menu contextuel de l'icône de l'application permet d'accéder aux commandes principales de Kaspersky Internet Security :

- désactivation de la protection de l'ordinateur ;
- restauration de la protection de l'ordinateur ;
- accès au Centre de protection ;
- lancement de la tâche de mise à jour ;
- lancement de l'analyse rapide ;
- accès à la fenêtre du Contrôle Parental ;
- accès à la fenêtre Protection bancaire ;
- accès à la fenêtre de configuration de l'application.

► *Pour ouvrir le menu contextuel de l'icône de Kaspersky Internet Security,*

cliquez sur l'icône de l'application dans la barre de menus.

FENETRE PRINCIPALE DE L'APPLICATION

► Pour ouvrir la fenêtre principale de l'application, procédez comme suit :

1. Cliquez sur l'icône de Kaspersky Internet Security dans la barre de menus.
Le menu contextuel de l'icône de l'application s'ouvre.
2. Sélectionnez l'option **Kaspersky Internet Security**.

Tâches de la fenêtre principale de l'application

La fenêtre principale de Kaspersky Internet Security vous permet de consulter les informations sur l'état de la protection de l'ordinateur, le fonctionnement de l'Anti-Virus Fichiers, l'Anti-Virus Internet et sur l'exécution des tâches d'analyse et de mise à jour.

De plus, la fenêtre principale de l'application permet d'exécuter les actions suivantes :

- gérer les tâches d'analyse et de mise à jour ;
- passer à la gestion des clés de l'application ;
- ouvrir la fenêtre du Centre de protection, la fenêtre de configuration de l'application, la fenêtre des rapports ;
- consulter les actualités de Kaspersky Internet Security en particulier et la protection contre les menaces informatiques en général ;
- ouvrir la fenêtre de configuration du Contrôle Parental ;
- ouvrir la fenêtre Protection bancaire ;
- ouvrir le portail My Kaspersky.

Eléments d'administration de la fenêtre principale de l'application

La fenêtre principale de l'application comprend les éléments suivants pour l'administration :

- indicateur de l'état de la protection sous la forme d'un ordinateur ;
- boutons dans la partie inférieure de la fenêtre principale de l'application ;
- panneau de navigation dans la partie supérieure de la fenêtre principale de l'application.

L'indicateur de l'état de la protection indique l'état de la protection de l'ordinateur en temps réel (cf. section "Evaluation de l'état de la protection de l'ordinateur" à la page [38](#)) :

- vert signifie que la protection de l'ordinateur est garantie au niveau requis ;
- jaune ou rouge indiquent l'existence d'un problème dans la configuration des paramètres ou dans le fonctionnement de Kaspersky Internet Security.

La partie droite de la fenêtre principale vient compléter l'indicateur de l'état de la protection de l'ordinateur avec des informations textuelles. Elle énumère également les problèmes et les menaces de sécurité qui ont été corrigés par le Centre de protection (cf. section "Utilisation du Centre de protection" à la page [40](#)). Si une analyse ou une mise à jour est en cours d'exécution à ce moment donné, la progression de celle-ci (exprimée en pour cent) apparaît également dans la partie droite de la fenêtre principale de l'application.

Les boutons de la partie inférieure de la fenêtre principale de l'application permettent de réaliser les tâches suivantes :



Ouvrir la fenêtre Mise à jour.



Passer aux tâches de recherche de virus : Analyse rapide, Analyse complète et Analyse personnalisée.



Ouvrir la fenêtre Licence (cf. section "Consultation des informations relatives à la licence" à la page [32](#)).



Ouvrir la fenêtre Protection des transactions bancaires (cf. section "Fenêtre Protection des transactions bancaires" à la page [22](#)).



Ouvrir la fenêtre de configuration du Contrôle Parental (à la page [22](#)).

La partie supérieure de la fenêtre principale de l'application contient une barre de navigation. Les boutons de la barre de navigation permettent de réaliser les opérations suivantes :



Ouvrir la fenêtre des rapports de Kaspersky Internet Security.



Ouvrir la fenêtre de configuration de l'application (à la page [21](#)).



Ouvrir l'aide électronique de Kaspersky Internet Security.



Ouvre la fenêtre contenant les informations sur les moyens d'obtenir l'assistance technique (cf. section "Contacter le Support Technique" à la page [58](#)).



Ouvrir la fenêtre du kiosque d'informations (cf. section "Kiosque d'informations" à la page [25](#)) proposant une liste d'informations. Le bouton apparaît quand Kaspersky Internet Security reçoit des informations.

FENETRE DE CONFIGURATION DE L'APPLICATION

► Pour ouvrir la fenêtre de configuration de Kaspersky Internet Security, exécutez l'une des actions suivantes :

- cliquez sur le bouton  dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)) ;
- dans le menu contextuel de l'icône de Kaspersky Internet Security (cf. section "Icône de Kaspersky Internet Security" à la page [19](#)), sélectionnez l'option **Paramètres**.

Vous pouvez utiliser les onglets suivants, situés dans la partie supérieure de la fenêtre des paramètres, pour accéder rapidement aux paramètres de l'application :

- **Protection.** Cet onglet permet de configurer les paramètres de l'Anti-Virus Fichiers, de l'Anti-Virus Internet et de la prévention des intrusions.
- **Analyse.** Cet onglet permet de configurer les paramètres d'analyse.
- **KSN.** Cet onglet permet de participer à Kaspersky Security Network ou de refuser la participation au Kaspersky Security Network.
- **Menaces.** Cet onglet permet de sélectionner la catégorie d'objets à détecter et de créer une zone de confiance.
- **Navigateurs.** Cet onglet permet d'installer le module d'analyse des liens et le clavier virtuel en tant qu'extension pour les navigateurs.
- **Mise à jour.** Cet onglet permet de configurer les paramètres de mise à jour de l'application.
- **Rapports.** Cet onglet permet de configurer les paramètres des rapports de Kaspersky Internet Security et de la quarantaine, d'activer ou de désactiver la consignation des informations de débogage dans le fichier de traçage et de configurer l'envoi automatique du rapport d'erreurs à Kaspersky Lab.
- **Apparence.** Cet onglet permet de configurer les paramètres d'affichage des fenêtres de notification Kaspersky Internet Security.

Le bouton  permet d'empêcher la modification des paramètres de fonctionnement de Kaspersky Internet Security par un utilisateur qui ne disposerait pas des privilèges d'administrateur de l'ordinateur. Le bouton se trouve dans la partie inférieure de la fenêtre des paramètres. Dans ce cas, il faudra saisir les informations d'identification de l'administrateur de l'ordinateur pour pouvoir introduire des modifications.

Le bouton  permet d'accéder à l'aide de Kaspersky Internet Security et plus exactement à la description des paramètres de la fenêtre ouverte. Vous pouvez également ouvrir l'aide pour la fenêtre actuelle de l'application, en sélectionnant l'option **Ouvrir l'aide pour cette fenêtre** dans le menu **Aide**.

FENETRE DE CONFIGURATION DU CONTROLE PARENTAL

► Pour ouvrir la fenêtre de configuration du Contrôle Parental, procédez de l'une des manières suivantes :

- dans le menu contextuel de l'icône de Kaspersky Internet Security (cf. section "Icône de Kaspersky Internet Security" à la page [19](#)), sélectionnez l'option **Contrôle parental** ;
- cliquez sur le bouton  dans la partie inférieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)).

La partie gauche de la fenêtre des paramètres du Contrôle Parental contient la liste des comptes utilisateur de l'ordinateur. Vous pouvez voir l'indicateur de fonctionnement du Contrôle Parental pour le compte utilisateur qui s'affiche à côté du nom de ce compte utilisateur. Un indicateur vert signale que le Contrôle Parental est activé. Le rouge indique que le Contrôle Parental est désactivé. Par défaut, le Contrôle Parental est désactivé pour tous les comptes utilisateur de l'ordinateur. Vous pouvez l'activer.

Si le Contrôle Parental a été activé pour un compte utilisateur, la partie droite de la fenêtre des paramètres du Contrôle Parental permet de sélectionner sous l'onglet **Paramètres** les actions de l'utilisateur sur l'ordinateur et sur Internet qui doivent être contrôlées.

Kaspersky Internet Security effectue le contrôle des actions suivantes de l'utilisateur par catégories :

- **Contrôle Internet** : contrôle des sites Internet visités et des fichiers téléchargés.
- **Contrôle du temps** : contrôle de la durée d'utilisation d'Internet.
- **Données personnelles** : contrôle de l'utilisation des données personnelles.
- **Réseaux sociaux** : contrôle de l'utilisation des réseaux sociaux.

Par défaut, le contrôle des actions de l'utilisateur est désactivé pour toutes les catégories. Vous pouvez l'activer individuellement pour chaque catégorie d'actions de l'utilisateur et accéder à une configuration plus poussée de la catégorie sélectionnée dans la partie droite de la fenêtre des paramètres du Contrôle Parental.

De même, sous l'onglet **Rapports** de la partie droite de la fenêtre des paramètres du Contrôle Parental, vous pouvez consulter les rapports sur les actions de l'utilisateur pour chaque compte utilisateur couvert par le Contrôle Parental ; et ce par catégorie.

Les utilisateurs qui ne possèdent pas les privilèges d'administrateur de l'ordinateur ne peuvent pas configurer le Contrôle Parental. Pour configurer et consulter les rapports du Contrôle Parental, il faut cliquer sur le bouton  et saisir les données du compte utilisateur administrateur de l'ordinateur.

FENETRE PROTECTION BANCAIRE

► Pour ouvrir la fenêtre Protection des transactions bancaires, procédez de l'une des manières suivantes :

- dans le menu contextuel de l'icône de Kaspersky Internet Security (cf. section "Icône de Kaspersky Internet Security" à la page [19](#)), sélectionnez l'option **Protection bancaire** ;
- cliquez sur le bouton  dans la partie inférieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)).

Le module Protection bancaire assure la protection des données de paiement et des opérations financières lors de l'utilisation des sites Internet des banques, des systèmes de paiement et des boutiques en ligne au paiement intégré (celles où vous saisissez les données de votre carte bancaire).

La fenêtre Protection bancaire permet de réaliser les opérations suivantes :

- ajouter, modifier et supprimer les données d'une banque, d'un système de paiement ou d'une boutique en ligne ;
- ouvrir le site de la banque, du système de paiement ou de la boutique en ligne au départ de la fenêtre du navigateur ;
- consulter la liste des données ajoutées.

Les boutons de la fenêtre Protection bancaire permettent de réaliser les tâches suivantes :



Ouvrir la fenêtre dans laquelle vous pouvez ajouter les données d'une banque, d'un système de paiement ou d'une boutique en ligne et sélectionner l'action que l'application exécutera lors de l'ouverture du site Internet de la banque, du système de paiement ou de la boutique en ligne ajouté.



Supprimer les données d'une banque, d'un système de paiement ou d'une boutique en ligne que vous aurez sélectionnées dans la liste.



Ouvrir le site Internet d'une banque, d'un système de paiement ou d'une boutique en ligne.



Ouvrir la fenêtre dans laquelle vous pouvez modifier les données d'une banque, d'un système de paiement ou d'une boutique en ligne que vous aurez sélectionnées dans la liste.

FENETRES DE NOTIFICATION ET FENETRES CONTEXTUELLES

Des événements présentant différents degrés de gravité se produisent lors du fonctionnement de Kaspersky Internet Security.

L'application signale les événements via des *fenêtres de notification* et des *messages contextuels*. La fenêtre de notification peut être accompagnée de notifications sonores.

DANS CETTE SECTION

Présentation des fenêtres de notification	23
Présentation des types d'événement	24
Présentation des fenêtres contextuelles	24
Désactivation des notifications	24

PRESENTATION DES FENETRES DE NOTIFICATION

Kaspersky Internet Security affiche une fenêtre de notification si l'événement nécessite que vous sélectionniez une action. Par exemple, lorsque l'application détecte un objet malveillant, l'utilisateur choisit de le supprimer ou de le réparer. La fenêtre de notification disparaît une fois que vous avez sélectionné une des actions proposées.

PRESENTATION DES TYPES D'ÉVÉNEMENT

Les événements qui apparaissent au cours du fonctionnement de Kaspersky Internet Security se divisent en trois catégories, selon leur niveau de gravité :

- **Critiques** : événements présentant un danger sérieux pour l'ordinateur (objets malveillants ou vulnérabilités détectés, problèmes dans le fonctionnement de Kaspersky Internet Security). L'apparition d'événements critiques exige une action immédiate de la part de l'utilisateur. Il est conseillé de ne pas désactiver les notifications à propos des événements critiques.
- **Importants** : événements ne nécessitant pas une action immédiate de la part de l'utilisateur mais qui peuvent s'avérer dangereux à long terme pour l'ordinateur.
- **Informatifs** : simples informations.

PRESENTATION DES FENÊTRES CONTEXTUELLES

Kaspersky Internet Security affiche des *fenêtres contextuelles* pour vous signaler les événements qui ne requièrent pas nécessairement la sélection d'une action. En fonction de la version du système d'exploitation de l'ordinateur, les messages contextuels apparaîtront sous l'icône de l'application dans la barre de menus ou dans le Centre de notification du système d'exploitation Mac OS X (pour les versions Mac OS X 10.8 et suivantes).

DESACTIVATION DES NOTIFICATIONS

Par défaut, Kaspersky Internet Security signale (cf. section "Fenêtres de notification et fenêtres contextuelles" à la page [23](#)) uniquement les événements critiques. Vous pouvez désactiver l'affichage des notifications ou sélectionner les événements pour lesquels vous souhaitez recevoir des notifications, ainsi que désactiver la notification sonore.

Que la remise des notifications soit activée ou non, les informations relatives aux événements survenus pendant le fonctionnement de Kaspersky Internet Security sont consignées dans le rapport sur le fonctionnement de l'application.

➔ *Pour désactiver la remise des notifications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Décochez la case **Afficher les notifications** du groupe **Notifications** dans l'onglet **Apparence** pour ne pas afficher les fenêtres de notification.

➔ *Pour sélectionner le type d'événement pour lequel vous ne souhaitez pas recevoir de notification, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Dans l'onglet **Apparence**, groupe **Notifications**, décochez les cases en regard des types d'événement (cf. section "Présentation des types d'événements" à la page [24](#)) au sujet desquels vous ne souhaitez pas recevoir de notification.

➡ Pour désactiver la notification sonore quand une fenêtre de notification s'affiche, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Décochez la case **Activer les notifications sonores** du groupe **Notifications** dans l'onglet **Apparence** pour ne pas afficher les fenêtres de notification.

KIOSQUE D'INFORMATIONS

Grâce au kiosque d'informations, Kaspersky Lab vous informe sur Kaspersky Internet Security en particulier et la protection contre les menaces informatiques en général.

L'application signale la diffusion de nouvelles informations à l'aide d'une icône  dans la partie supérieure de la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)). Cliquez sur l'icône pour afficher la fenêtre **Infos**.

LICENCE DE L'APPLICATION

Cette section présente les notions principales relatives à l'activation de l'application. Cette section explique le rôle du contrat de licence, les modes d'activation de l'application et le renouvellement de l'abonnement.

DANS CETTE SECTION

Présentation du Contrat de licence.....	26
Présentation de la licence.....	26
Présentation de l'abonnement.....	27
Présentation du code d'activation.....	28
Présentation de la clé.....	28
Présentation des données proposées.....	29
Consultation des informations sur la licence.....	32
Achat d'une licence.....	32
Renouvellement de la licence.....	33
Renouvellement de l'abonnement.....	33
Mise à jour de l'état de l'abonnement.....	34
Activation de Kaspersky Internet Security.....	34

PRESENTATION DU CONTRAT DE LICENCE

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement le Contrat de licence avant de commencer à utiliser l'application.

Vous acceptez les conditions du Contrat de licence en confirmant votre accord avec le texte du Contrat de licence lors de l'installation de l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application.

PRESENTATION DE LA LICENCE

La *licence* est un droit d'utilisation de l'application octroyé pour une durée définie sur la base du Contrat de licence. Un code unique d'activation de votre copie de Kaspersky Internet Security est associé à la licence.

La licence donne droit aux services suivants :

- Utilisation de l'application et de toutes ses fonctions sur un ou plusieurs périphériques.

Le nombre de périphériques sur lesquels vous pouvez utiliser l'application est défini dans les conditions du Contrat de licence.

- Contacter le Support Technique de Kaspersky Lab.
- Obtention d'autres services proposés par Kaspersky Lab ou par ses partenaires durant la validité de la licence (cf. section "Service pour les utilisateurs enregistrés" à la page [13](#)).

Pour pouvoir utiliser toutes les fonctions de l'application, vous devez acheter une licence pour l'application et l'activer.

La licence présente une durée de validité restreinte. Une fois que la durée de validité de la licence est écoulée, l'application reste fonctionnelle, mais ses fonctionnalités sont limitées (par exemple, il n'est plus possible de mettre l'application à jour ou d'utiliser le service Kaspersky Security Network). Vous pouvez continuer à utiliser tous les modules de l'application et à exécuter l'analyse antivirus mais uniquement à l'aide des bases anti-virus installées avant la date d'expiration de la licence. Pour pouvoir continuer à profiter de toutes les fonctionnalités de Kaspersky Internet Security, il faut renouveler la licence.

Il est conseillé de renouveler la licence avant sa date d'expiration afin de garantir la protection maximale contre toutes les menaces informatiques.

Avant d'acheter une licence, vous pouvez vous familiariser gratuitement avec la version d'évaluation de Kaspersky Internet Security. Les fonctions de la version d'évaluation de Kaspersky Internet Security sont disponibles pendant une courte période de familiarisation. Suite à l'expiration de cette période de familiarisation, Kaspersky Internet Security cesse de remplir ses fonctions. Pour continuer à utiliser l'application, il est nécessaire d'acheter une licence.

PRESENTATION DE L'ABONNEMENT

L'abonnement à Kaspersky Internet Security constitue une commande pour l'utilisation de l'application selon des paramètres sélectionnés (date d'expiration, nombre de périphériques protégés). Il est possible de commander un abonnement à Kaspersky Internet Security auprès d'un prestataire de services (par exemple, auprès d'un fournisseur Internet). Vous pouvez suspendre et reprendre l'abonnement, ainsi que le renouveler automatiquement ou l'arrêter. Vous pouvez gérer votre abonnement à partir de votre espace personnel, sur le site Internet du prestataire de services.

L'abonnement peut être limité (à un an par exemple) ou illimité (sans date d'expiration). Pour prolonger l'action de Kaspersky Internet Security après la date d'expiration d'un abonnement limité, vous devez le renouveler. L'abonnement illimité se renouvelle automatiquement selon les conditions en vigueur au moment du paiement au prestataire de services.

Si vous utilisez l'application selon un abonnement limité, vous bénéficierez d'une période de renouvellement à tarif préférentiel à son expiration afin de le renouveler. Toutes les fonctions de l'application demeurent opérationnelles durant cette période.

Les prestataires de services peuvent vous proposer deux types d'abonnement pour l'utilisation de Kaspersky Internet Security : abonnement pour la mise à jour ou abonnement pour la mise à jour et la protection. Si vous avez souscrit un abonnement pour les mises à jour, à l'expiration de l'abonnement et à la fin de la période de renouvellement à tarif préférentiel, Kaspersky Internet Security continue à fonctionner, mais ne procède plus à la mise à jour des bases de l'application. Si vous avez souscrit un abonnement pour les mises à jour et la protection, à l'expiration de l'abonnement et à la fin de la période de renouvellement à tarif préférentiel, Kaspersky Internet Security ne procède plus à la mise à jour des bases de l'application, il suspend également la protection de l'ordinateur et arrête de lancer les analyses.

Pour utiliser Kaspersky Internet Security sur abonnement, vous devez modifier le code d'activation fourni par le prestataire de services. Dans certains cas, le code d'activation peut s'appliquer automatiquement. Lorsque vous utilisez l'application sur abonnement, vous ne pouvez pas appliquer un autre code d'activation pour renouveler l'abonnement. Vous pouvez appliquer un autre code d'activation mais ceci uniquement après l'expiration de l'abonnement ou en cas de résiliation. Pour résilier l'abonnement, vous devez contacter le prestataire de services auprès de qui vous avez acheté Kaspersky Internet Security.

Si, lors de la souscription à l'abonnement Kaspersky Internet Security, vous possédez déjà une licence active, il faudra supprimer la clé active afin de pouvoir activer l'application selon l'abonnement. Le code d'activation ayant permis d'activer l'application peut être transféré à un autre ordinateur.

Le choix des possibilités de gestion de l'abonnement diffère selon les prestataires de services. De même, la période de renouvellement à tarif préférentiel au cours de laquelle vous pouvez prolonger votre abonnement n'est pas toujours proposée.

PRESENTATION DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence d'utilisation de Kaspersky Internet Security. Ce code est indispensable pour activer l'application.

Le code d'activation est une suite unique de 20 caractères alphanumériques (alphabet latin) au format xxxxx-xxxxx-xxxxx-xxxxx.

En fonction du mode d'achat de l'application, vous pouvez obtenir le code d'activation d'une des manières suivantes :

- Si vous avez acheté Kaspersky Internet Security en magasin, le code d'activation figure dans la documentation présente dans la boîte.
- Si vous avez acheté Kaspersky Internet Security en ligne, le code d'activation est envoyé à l'adresse de messagerie que vous avez renseignée lors de la commande.

Le décompte de la durée de validité de la licence de l'application débute à la date d'activation de l'application. Si vous avez acheté une licence qui permet d'utiliser Kaspersky Internet Security sur plusieurs périphériques, le décompte de la durée de validité de la licence débute à la date de la première utilisation du code d'activation.

En cas de perte ou de suppression accidentelle du code après l'activation de l'application, contactez le Support Technique de Kaspersky Lab pour le récupérer.

PRESENTATION DE LA CLÉ

Une *clé* est une séquence de bits qui permet d'activer, puis d'utiliser l'application conformément aux conditions du Contrat de licence. La clé est créée par les experts de Kaspersky Lab.

Pour ajouter une clé à l'application, vous devez saisir le *code d'activation*. La clé apparaît dans l'interface de l'application sous la forme d'une séquence alphanumérique unique après que vous l'avez ajoutée à l'application.

La clé peut être bloquée par Kaspersky Lab en cas de non-respect des dispositions du Contrat de licence. Si la clé est bloquée, il faudra en ajouter une autre pour pouvoir utiliser l'application.

La clé peut être une clé active ou de réserve.

La *clé active* est la clé utilisée au moment actuel pour faire fonctionner l'application. L'application ne peut avoir qu'une clé active à la fois.

La *clé de réserve* est la clé qui confirme le droit d'utilisation de l'application mais qui n'est pas utilisée actuellement. La clé de réserve devient automatiquement la clé active à l'expiration de la licence associée à la clé active actuelle. Une clé de réserve peut être ajoutée uniquement quand une clé active est présente. Il est impossible d'ajouter une clé de réserve si vous utilisez une clé par abonnement. De même, il est impossible d'ajouter une clé par abonnement en tant que clé de réserve.

La clé de la version d'évaluation peut être ajoutée uniquement en qualité de clé active. La clé de la version d'évaluation ne peut être ajoutée en qualité de clé de réserve.

PRESENTATION DES DONNEES PROPOSEES

On entend par Logiciel le logiciel et toute mise à jour, ainsi que tous les documents associés.

On entend par Titulaire des droits (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

On entend par Ordinateur(s) le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les " téléphones intelligents ", les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

On entend par Utilisateur final (vous/votre) la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, " Vous " signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme " entité ", sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limitée, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

On entend par Mise(s) à jour toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patches, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

Fichiers trace signifie des données contenant des informations concernant le fonctionnement du Logiciel ou de ses composants.

Fichiers de l'image mémoire signifie le contenu de la mémoire système des processus du Logiciel, lors de la génération.

Fichiers d'informations système signifie les données contenant des informations concernant l'Ordinateur.

Pour améliorer la protection, en acceptant le Contrat de licence, vous acceptez d'envoyer automatiquement à Kaspersky Lab des informations sur la copie de Kaspersky Lab installée sur l'ordinateur, sur la version utilisée et sur ses paramètres, ainsi que les informations relatives à l'activation.

Si vous participez à Kaspersky Security Network, ces informations sont automatiquement transmises à Kaspersky Lab lors du fonctionnement de Kaspersky Internet Security sur l'ordinateur :

- Informations relatives au système d'exploitation (SE) installé sur l'ordinateur et aux mises à jour installées.
- Informations concernant les logiciels installés par le Détenteur du droit et l'état de la protection antivirus, y compris : la version du logiciel, identificateur unique de l'ordinateur, informations sur les mises à jour.
- Informations sur tous les objets analysés et les actions d'analyse, y compris le nom de l'objet analysé, la date et l'heure de l'analyse, Référent, l'URL depuis laquelle l'objet a été téléchargé, le nom et la taille des fichiers analysés et leur chemin d'accès, la date et l'heure de la création du fichier, le nom de l'utilitaire de compression (si le fichier a été compressé), l'entropie du fichier, l'identificateur du type du fichier et son format, l'URL depuis laquelle l'objet a été téléchargé, la somme de contrôle de l'objet (MD5), le type et la valeur de la somme de contrôle supplémentaire de l'objet, les données concernant la signature numérique de l'objet (certificat) .

Pour les fichiers exécutables : signe de l'envoi des informations de service, indicateur de vérification de réputation ou indicateur de signature de fichier, nom, type, ID, type, checksum (MD5) et la taille de l'application qui a été chargée par l'objet en cours de validation, le chemin de l'application et les chemins des modèles, un signe de la liste de l'Autorun, date de l'entrée, la liste des attributs, nom de l'emballeur, informations sur la signature numérique de l'application, y compris le certificat de l'éditeur, le nom du fichier téléchargé au format MIME.

- Informations relatives aux applications et à leur module, dont les sommes de contrôle des fichiers exécutables (MD5), la taille, les attributs, la date de création, les informations de l'en-tête des fichiers PE, le nom du compacteur (si le fichier avait été compacté), le code du compte utilisateur au nom duquel le processus a été exécuté, les paramètres de la ligne de commande utilisés pour lancer le processus, les noms des fichiers et de leurs modules.

- En cas de détection de menaces ou de vulnérabilités, outre les informations concernant l'objet détectée, les informations suivantes sont fournies : identificateur, version et type de l'enregistrement dans la base de données antivirus, nom de la menace basé sur la classification du Détenteur de droit, somme de contrôle (MD5) du fichier de l'application ayant demandé l'URL dans laquelle la menace a été détectée, adresse IP (IPv4 ou IPv6) de la menace détectée, identificateur du type de trafic sur lequel la menace a été détectée, identificateur de la vulnérabilité et son niveau de menace, URL de la page Web dans laquelle la menace a été détectée, numéro du script dans la page, identificateur du danger, type et état de la vulnérabilité détectée, résultats intermédiaires de l'analyse de l'objet.
- Informations sur les attaques réseau, y compris l'adresse IP de l'ordinateur attaquant et le numéro de port de l'ordinateur de l'utilisateur cible par l'attaque réseau, l'identificateur du protocole utilisé pour effectuer l'attaque, ainsi que le nom et le type d'attaque.
- L'URL et l'adresse IP de la page Web dans laquelle un contenu malveillant ou suspect a été détecté, le nom, la taille et la somme de contrôle du fichier ayant demandé l'URL, l'identificateur et le poids de la règle utilisée pour atteindre un verdict, l'objectif de l'attaque.
- Informations concernant les modifications apportées par l'utilisateur dans la liste des sites Web protégés par le composant Protection bancaire, y compris l'URL du site Web, un indicateur signalant qu'un site Web a été ajouté, modifié ou supprimé, le mode d'exécution de Protection bancaire pour le site Web.

Les fichiers (parties de fichiers et sommes de contrôle de fichiers) pouvant être utilisés par des attaquants pour endommager l'ordinateur de l'utilisateur, y compris les objets détectés sur des liens malveillants, peuvent éventuellement être envoyés à Kaspersky Lab à des fins d'analyse.

En outre, pour éviter les incidents et analyser ceux qui ont lieu, les fichiers approuvés exécutables et non exécutables, les rapports d'activité des applications, des portions de la mémoire vive de l'ordinateur ainsi que le secteur d'amorçage du système d'exploitation peuvent éventuellement être envoyés.

Pour améliorer la qualité du produit, l'utilisateur accepte de fournir à Kaspersky Lab les informations suivantes :

- Informations sur l'utilisation de l'interface utilisateur du produit, y compris les informations sur l'ouverture des fenêtres de l'interface (y compris les identificateurs et les noms des fenêtres, ainsi que les éléments de contrôle utilisés) et le passage d'une fenêtre à l'autre, les informations motivant l'ouverture d'une fenêtre, la date et l'heure de démarrage de l'interface ainsi que les étapes de démarrage de l'interface, la durée et le type d'interaction de l'utilisateur avec l'interface, les informations relatives aux modifications de réglages et aux paramètres du produit (y compris le nom du réglage ou du paramètre, ainsi que les valeurs anciennes et nouvelles) ;
- L'ID de l'application en mode interactif.

Si une erreur apparaît lors du processus Kaspersky Internet Security, l'utilisateur peut envoyer à Kaspersky Lab un fichier contenant les informations suivantes :

- nom et identificateur du processus ;
- chemin vers le module en cours d'exécution ;
- version de l'application ;
- nombre de bits du processus (32 ou 64 bits) ;
- nom et identificateur du processus parent ;
- heure et date de la défaillance de l'application ;
- version du système d'exploitation ;
- version du rapport ;
- type d'erreur à l'origine de la défaillance de l'application ;

- informations à propos de l'erreur ;
- numéro du flux dans lequel l'erreur est apparue ;
- pile d'exécution de chaque flux au moment de la défaillance de l'application (numéro de trame, nom du module, adresse dans le code, nom de la fonction qui correspond à l'adresse) ;
- valeur du flux dans lequel l'erreur est apparue ;
- liste des modules téléchargés avec l'adresse d'où ils ont été téléchargés, sa version, l'UUID et son chemin d'accès.

En outre, les systèmes d'exploitation Mountain Lion et Yosemite demandent la transmission des informations suivantes :

- ID de l'utilisateur (UID) ;
- les statistiques de certaines invocations système d'interaction d'autres processus avec ce processus ;
- distribution de la mémoire (statistiques sur la quantité de mémoire affectée à tel ou tel domaine).

Le fichier de traçage de Kaspersky Internet Security reprend les informations suivantes :

- Les informations relatives à l'état de la protection antivirus de l'ordinateur, ainsi que les données relatives à tous les objets et actions potentiellement malveillants (dont le nom de l'objet détecté, la date et l'heure de la détection, l'URL de téléchargement, le nom et la taille des fichiers infectés et le chemin d'accès à ceux-ci, l'adresse IP de l'ordinateur attaqué et le numéro de port de l'ordinateur de l'utilisateur victime de l'attaque réseau, la séquence d'actions du programme malveillant et les URL potentiellement malveillantes) ainsi que les solutions appliquées à ceux-ci par l'application et l'utilisateur.
- Les informations relatives aux applications chargées par l'utilisateur (URL, attributs, taille du fichier, informations relatives au processus qui a téléchargé le fichier).
- Les informations relatives aux applications et aux modules exécutés (tailles, attributs, date de création, informations de l'en-tête PE, région, nom, emplacement, compacteurs).
- Les informations sur les erreurs d'utilisation de l'interface utilisateur de l'application de Kaspersky Lab installée.
- Les informations relatives aux connexions réseau, notamment l'adresse IP de l'ordinateur distant et de l'ordinateur de l'utilisateur, les numéros des ports de connexion et le protocole réseau de connexion.
- Les informations relatives aux paquets réseau reçus par l'ordinateur et transmis par ce dernier via le réseau informatique.
- Les informations relatives aux messages électroniques et IM envoyés et reçus.
- Les informations relatives aux URL consultées notamment, si la connexion a été établie via un protocole ouvert, le nom d'utilisateur et le mot de passe d'accès aux sites comportant des fichiers cookie.
- Certificat de serveur public.

Les données importées dans les fichiers de vidage reprennent toutes les informations relatives à la mémoire active des processus de l'application au moment de la création de ces fichiers.

Il est également possible d'envoyer à Kaspersky Lab pour une analyse complémentaire des fichiers complets ou tronqués dont le risque d'utilisation par les individus malintentionnés peut nuire à l'ordinateur ou aux données de l'utilisateur.

Les informations reçues sont protégées par Kaspersky Lab, conformément aux exigences réglementaires. Kaspersky Lab utilise les informations reçues uniquement pour les statistiques générales. Ces statistiques générales se créent automatiquement à partir des informations reçues et ne contiennent aucune donnée personnelle ou toute autre information confidentielle. Les informations reçues sont chiffrées et détruites au fur et à mesure qu'elles s'accumulent (deux fois par an). Les statistiques générales sont conservées sans limite de temps.

CONSULTATION DES INFORMATIONS RELATIVES A LA LICENCE

➤ *Pour consulter les informations relatives à la licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.

La fenêtre **Licence** s'ouvre.

La fenêtre **Licence** reprend les informations suivantes :

- clé active (cf. section "A propos des clés" à la page [28](#)) ;
- clé de réserve, si elle a été ajoutée ;
- l'état de la clé ou de l'abonnement ;
- nombre d'ordinateurs sur lesquels vous pouvez utiliser l'application conformément à la licence active ou à l'abonnement ;
- la date et l'heure d'expiration de la licence ;
- et le nombre de jours restants avant cette date.

Si l'application n'a pas été activée, la fenêtre **Licence** le signale. Vous pouvez activer l'application (cf. section "Activation de Kaspersky Internet Security" à la page [34](#)).

Si vous utilisez une version d'évaluation de l'application, vous pouvez acheter une licence (cf. section "Achat d'une licence" à la page [32](#)).

Si aucune clé de réserve n'a été ajoutée et que la licence associée à la clé active expire, vous pouvez la renouveler (cf. section "Renouvellement de la licence" à la page [33](#)).

Si votre abonnement à Kaspersky Internet Security a expiré et qu'il en est de même pour la période de renouvellement à tarif préférentiel, vous pouvez renouveler manuellement votre abonnement (cf. section "Renouvellement de l'abonnement" à la page [33](#)). De même, si vous utilisez l'application sur abonnement, vous pouvez mettre à jour l'état de l'abonnement (cf. section "Mise à jour de l'état de l'abonnement" à la page [34](#)).

ACHAT D'UNE LICENCE

Si vous ne possédez pas de licence d'utilisation de Kaspersky Internet Security ou que vous utilisez une licence d'évaluation, vous pouvez acheter une licence.

➤ *Pour acheter une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.

La fenêtre **Licence** s'ouvre.

3. Dans la fenêtre **Licence**, cliquez sur **Acheter**.

Une page Internet s'ouvre et présente les informations relatives à l'achat de la licence via la boutique en ligne de Kaspersky Lab, sur le portail My Kaspersky ou auprès des partenaires de la société. Si vous achetez la licence via la boutique en ligne, vous recevrez, après confirmation du paiement, le code d'activation de Kaspersky Internet Security (cf. section "A propos du code d'activation" à la page [28](#)) dans un message envoyé à l'adresse électronique indiquée sur le bon de commande.

RENOUVELLEMENT DE LA LICENCE

Vous devez renouveler la licence lorsque la durée de validité associée à la clé active est expirée et qu'aucune clé de réserve n'a été ajoutée. Une fois que la durée de validité de la licence est écoulée, l'application reste fonctionnelle, mais ses fonctionnalités sont limitées (par exemple, il n'est plus possible de mettre l'application à jour ou d'utiliser le service Kaspersky Security Network). Vous pouvez continuer à utiliser tous les modules de l'application et à exécuter l'analyse antivirus mais uniquement à l'aide des bases anti-virus installées avant la date d'expiration de la licence.

Si les bases anti-virus sont dépassées, l'ordinateur est exposé au risque d'infection.

➔ *Pour renouveler une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.
La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Renouveler**.

Une page Internet s'ouvre et présente les informations relatives au renouvellement de la licence via la boutique en ligne de Kaspersky Lab, sur le portail My Kaspersky ou auprès des partenaires de la société. Si vous renouvelez la licence via la boutique en ligne, vous recevrez, après confirmation du paiement, le code d'activation de Kaspersky Internet Security (cf. section "A propos du code d'activation" à la page [28](#)) dans un message envoyé à l'adresse électronique indiquée dans le bon de commande.

RENOUVELLEMENT DE L'ABONNEMENT

Si vous utilisez l'application par abonnement, Kaspersky Internet Security se connecte automatiquement au serveur d'activation à des intervalles définis jusqu'à la fin de l'abonnement.

Si vous utilisez l'application avec un abonnement illimité, Kaspersky Internet Security vérifie automatiquement et en arrière-plan la possibilité de renouveler ma clé sur le serveur d'activation. Si cette opération est possible, il remplace la clé antérieure par la nouvelle. C'est ainsi que l'abonnement illimité à Kaspersky Internet Security se renouvelle sans votre participation.

Si l'abonnement et la période de renouvellement à tarif préférentiel ont expiré, Kaspersky Internet Security vous notifie et arrête ses tentatives de renouvellement automatique de l'abonnement. Kaspersky Internet Security ne met plus à jour les bases de l'application (pour les abonnements pour la mise à jour) et n'assure plus la protection ou l'exécution des tâches d'analyse (pour les abonnements pour la mise à jour et la protection).

Pour renouveler l'abonnement manuellement, vous devez contacter le prestataire de services auprès de qui vous avez acheté Kaspersky Internet Security.

➔ *Pour renouveler l'abonnement, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.
La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Visiter le site Internet du service client**.

Cette page présente les informations sur les conditions de renouvellement de l'abonnement.

MISE A JOUR DE L'ETAT DE L'ABONNEMENT

Il se peut que l'état de l'abonnement ne soit pas à jour. Dans ce cas, il faut mettre à jour l'état de l'abonnement manuellement. Kaspersky Internet Security ne met plus à jour les bases anti-virus de l'application (pour les abonnements pour la mise à jour) et n'assure plus la protection ou l'exécution des tâches d'analyse (pour les abonnements pour la mise à jour et la protection) jusqu'à ce que l'abonnement soit prolongé ou renouvelé.

► Pour renouveler l'abonnement, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.
La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Mettre à jour l'état de l'abonnement**.

ACTIVATION DE KASPERSKY INTERNET SECURITY

Avant d'activer Kaspersky Internet Security, assurez-vous que la date et l'heure système de l'ordinateur correspondent à la date et à l'heure réelles.

L'activation de l'application s'effectue lors de l'ajout de la clé (cf. section "A propos de la clé" à la page [28](#)) dans l'application.

Si l'application n'est pas activée, toutes les fonctions de Kaspersky Internet Security vous sont accessibles, sauf l'obtention des mises à jour. La mise à jour des bases anti-virus peut être exécutée une seule fois seulement après l'installation de l'application.

DANS CETTE SECTION

Activation de la version d'évaluation de l'application.....	34
Activation de l'application à l'aide du code d'activation	35

ACTIVATION DE LA VERSION D'EVALUATION DE L'APPLICATION

L'activation de la version d'évaluation de Kaspersky Internet Security est possible uniquement si l'application se trouvant sur cet ordinateur n'a pas été déjà activée par une telle licence.

Il est conseillé d'activer la version d'évaluation de l'application afin de se familiariser avec ses fonctionnalités avant de décider d'acheter la licence. Les fonctions de la version d'évaluation de Kaspersky Internet Security sont disponibles pendant une courte période de familiarisation. Suite à l'expiration de cette période de familiarisation, Kaspersky Internet Security cesse de remplir ses fonctions. Une clé gratuite vous sera fournie pour activer la version d'évaluation.

Une connexion à Internet est indispensable pour activer l'application.

► Pour activer la version d'évaluation de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.
La fenêtre **Licence** s'ouvre.

3. Dans la fenêtre **Licence** qui s'ouvre, cliquez sur le bouton **Version d'essai**.
4. Dans la fenêtre **Activation de la version d'évaluation de l'application**, cliquez sur le bouton **Activer la version d'évaluation**.

Kaspersky Internet Security contacte les serveurs de Kaspersky Lab afin d'envoyer les données pour vérification. Si la vérification réussit, l'application reçoit la clé gratuite et l'installe.

5. Cliquez sur **Terminer** pour terminer l'activation de l'application.

Si l'activation de la version d'évaluation de l'application s'est déroulée avec succès, la fenêtre **Licence** s'ouvre et affiche les informations suivantes :

- état de la clé ;
- la restriction du nombre d'ordinateurs sur lesquels l'application peut être exécutée ;
- la date et l'heure d'expiration de la licence ;
- et le nombre de jours restants avant cette date.

Un message s'affiche à la fin de la durée de validité de la licence d'évaluation pour la version de Kaspersky Internet Security. Pour renouveler la licence, vous devez acheter une licence (cf. section "Achat d'une licence" à la page [32](#)).

ACTIVATION DE L'APPLICATION A L'AIDE DU CODE D'ACTIVATION

Grâce au code d'activation, l'application reçoit la clé et l'ajoute automatiquement afin de vous donner accès à toutes les fonctions de Kaspersky Security pendant la durée de validité de la licence.

Une connexion à Internet est indispensable pour activer l'application.

➔ Pour activer l'application à l'aide du code d'activation, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.
La fenêtre **Licence** s'ouvre.
3. Dans la fenêtre **Licence**, cliquez sur le bouton **Activer**.
4. Dans la fenêtre **Activation de l'application**, saisissez le code d'activation reçu à l'achat de Kaspersky Internet Security.

Le code d'activation est une suite unique de 20 caractères alphanumériques (alphabet latin) au format xxxx-xxxx-xxxx-xxxx.

Kaspersky Internet Security contacte les serveurs de Kaspersky Lab afin d'envoyer le code d'activation pour vérification de l'authenticité. Si la vérification du code d'activation réussit, l'application reçoit automatiquement la clé et l'installe.

En fonction du code d'activation octroyé, il vous faudra peut-être saisir des données dans un formulaire d'inscription ou ouvrir un compte sur le portail My Kaspersky.

Si la vérification de l'authenticité du code d'activation échoue, un message vous le signalera. Dans ce cas, demandez des informations à la société qui vous a fourni ce code d'activation.

Si l'activation de l'application s'est déroulée avec succès à l'aide du code d'activation, la fenêtre **Licence** s'ouvre et affiche les informations suivantes :

- clé ;
- l'état de la clé ou de l'abonnement ;
- la restriction du nombre d'ordinateurs sur lesquels l'application peut être exécutée ;
- la date et l'heure d'expiration de la licence ;
- et le nombre de jours restants avant cette date.

LANCEMENT ET ARRET DE L'APPLICATION

L'application est lancée automatiquement après l'installation et l'icône de Kaspersky Internet Security (cf. page [19](#)) apparaît dans la barre de menus.

◆ *Pour quitter Kaspersky Internet Security, procédez comme suit :*

1. Cliquez sur l'icône de Kaspersky Internet Security (à la page [19](#)).
2. Dans le menu contextuel qui s'ouvre, choisissez l'option **Quitter**.

Le fonctionnement de l'application s'arrête et le processus sera supprimé dans la mémoire vive de l'ordinateur.

Une fois que vous avez quitté Kaspersky Internet Security, l'ordinateur continue à fonctionner sans protection. Il risque d'être infecté et vos données sont menacées.

ETAT DE LA PROTECTION DE L'ORDINATEUR

Cette section explique comment déterminer la présence de problèmes et de menaces contre la sécurité de l'ordinateur et comment configurer le niveau de protection. Vous apprendrez également à activer ou désactiver la protection pendant l'utilisation de l'application.

L'état de la protection de votre ordinateur reflète la présence ou l'absence de menaces qui influencent le niveau général de sécurité du système d'exploitation. Dans ce cas, les menaces sont non seulement les programmes malveillants découverts, mais aussi l'utilisation de bases anti-virus dépassées, la désactivation de l'Anti-Virus Fichiers ou de l'Anti-Virus Internet ou l'expiration prochaine de la validité de la licence.

Le Centre de protection (cf. section "Utilisation du Centre de protection" à la page [40](#)) permet d'examiner les menaces existantes et de les éliminer.

DANS CETTE SECTION

Evaluation de l'état de la protection de l'ordinateur.....	38
Désactivation de la protection de l'ordinateur	39
Rétablissement de la protection de l'ordinateur.....	40
Utilisation du Centre de protection.....	40

ÉVALUATION DE L'ÉTAT DE LA PROTECTION DE L'ORDINATEUR

L'indicateur de l'état de la protection de l'ordinateur représenté par un ordinateur et situé dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)), signale les problèmes qui surviennent dans la protection. La couleur de l'indicateur change en fonction de l'état de la protection. Si une menace est présente dans le l'ordinateur, l'indicateur de couleur sera accompagné d'un message relatif aux menaces.

L'indice peut prendre une des valeurs suivantes :

- **Vert.** La protection de l'ordinateur est assurée au niveau adéquat.
Un indicateur vert signale que les bases anti-virus de l'application sont mises à jour et que l'ensemble des composants de l'application fonctionne conformément aux paramètres recommandés par les spécialistes de Kaspersky Lab. Aucun objet malveillant n'a été décelé ou les objets malveillants découverts ont été neutralisés. Le Contrôle Parental fonctionne en mode normal.
- **Jaune.** Le niveau de protection de votre ordinateur est abaissé.
Un indicateur jaune signale un problème de fonctionnement de Kaspersky Internet Security. Par exemple, l'écart par rapport au mode de fonctionnement recommandé est négligeable, les bases de l'application n'ont pas été mises à niveau pendant quelques jours.
- **Rouge.** Votre ordinateur est exposé à un risque d'infection.
Un indicateur rouge signale l'existence de problèmes graves qui pourraient entraîner l'infection de l'ordinateur ou la perte de données. Par exemple, les bases anti-virus de l'application sont sérieusement dépassées, l'application n'est pas activée ou un objet malveillant a été détecté.

Il est conseillé d'éliminer les problèmes et les menaces sur la sécurité de l'ordinateur.

DESACTIVATION DE LA PROTECTION DE L'ORDINATEUR

Kaspersky Internet Security est lancé par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. Tous les modules de la protection (Anti-virus Fichiers, Anti-virus Internet et prévention des intrusions) sont activés et fonctionnent.

Vous pouvez désactiver la protection par Kaspersky Internet Security complètement ou partiellement.

Les experts de Kaspersky Lab vous recommandent vivement de ne pas désactiver la protection offerte par les modules de protection en temps réel, car cela pourrait entraîner l'infection de votre ordinateur et la perte de données.

Les éléments suivants témoignent de la désactivation de la protection de l'ordinateur :

- icône de l'application inactive (cf. section "Icône de Kaspersky Internet Security" à la page [19](#)) dans la barre de menus ;
- couleur rouge de l'indicateur de l'état de la protection de l'ordinateur dans la fenêtre principale de l'application.

La protection de l'ordinateur est envisagée dans le contexte du fonctionnement de l'Anti-Virus Fichiers, de l'Anti-Virus Internet et de la prévention des intrusions. La désactivation ou la suspension du fonctionnement de ces composants n'a aucune influence sur l'exécution de l'analyse et de la mise à jour.

Plusieurs méthodes existent pour désactiver complètement la protection de l'ordinateur. Vous pouvez désactiver les composants de la protection sous l'onglet **Protection** de la fenêtre des paramètres de l'application.

➔ Pour désactiver la protection de l'ordinateur, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Internet Security (à la page [19](#)) dans la barre de menus et sélectionnez l'option **Désactiver la Protection** dans le menu contextuel.
- Ouvrez la fenêtre de configuration de l'application (à la page [21](#)), choisissez l'onglet **Protection** et dans le groupe **Général**, décochez la case **Activer la Protection**.

Si vous avez désactivé la protection de l'ordinateur, alors après le redémarrage de Kaspersky Internet Security, elle n'est pas réactivée automatiquement. Vous devez activer manuellement la protection de l'ordinateur (cf. section "Restauration de la protection de l'ordinateur" à la page [40](#)).

➔ Pour désactiver un module de la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Protection** de la fenêtre des paramètres, dans le groupe **<nom du composant>**, décochez la case **Activer <nom du composant>**.

Si vous avez désactivé un module de la protection, il ne se réactivera pas automatiquement après le redémarrage de Kaspersky Internet Security. Vous devez activer manuellement le module de protection (cf. section "Restauration de la protection de l'ordinateur" à la page [40](#)).

RETABLISSEMENT DE LA PROTECTION DE L'ORDINATEUR

Si la protection de l'ordinateur ou un module de la protection (Anti-Virus Fichiers, Anti-Virus Internet ou prévention des intrusions) est désactivé, la seule manière de rétablir la protection de l'ordinateur ou le fonctionnement d'un module de la protection est d'utiliser un procédé manuel à la demande de l'utilisateur. Le rétablissement automatique de la protection de l'ordinateur ou d'un module de la protection après le redémarrage du système d'exploitation ou de Kaspersky Internet Security n'a pas lieu.

► Pour activer la protection de l'ordinateur, utilisez un des moyens suivants :

- Cliquez sur l'icône de Kaspersky Internet Security (à la page [19](#)) dans la barre de menus et sélectionnez l'option **Activer la Protection** dans le menu contextuel.
- Ouvrez la fenêtre de configuration de l'application (à la page [21](#)), choisissez l'onglet **Protection** et dans le groupe **Général**, cochez la case **Activer la Protection**.

► Pour activer le module de la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Dans la fenêtre principale de l'application, cliquez sur le bouton  .
La fenêtre des paramètres de l'application s'ouvre.
3. Sous l'onglet **Protection** de la fenêtre des paramètres, dans le groupe **<nom du composant>**, cochez la case **Activer <nom du composant>**.

De même, pour activer la protection de l'ordinateur ou d'un module de la protection, vous pouvez utiliser le Centre de protection (cf. section "Centre de protection" à la page [40](#)). La désactivation de la protection de l'ordinateur ou la désactivation des composants de la protection augmente considérablement le risque d'infection de l'ordinateur. Pour cette raison, les informations sur la désactivation sont conservées dans le Centre de protection.

UTILISATION DU CENTRE DE PROTECTION

Le *Centre de protection* est une fonction de Kaspersky Internet Security qui permet d'analyser et de supprimer les problèmes et les menaces existants sur la sécurité de l'ordinateur.

► Pour ouvrir le Centre de protection,

cliquez sur le bouton **En savoir plus** dans la fenêtre principale de l'application (cf. section "Fenêtre principale de l'application" à la page [20](#)) ;

La fenêtre Centre de protection permet d'afficher la liste des problèmes et des menaces contre la sécurité de l'ordinateur existants. Pour chaque problème ou menace, des actions sont proposées pour la résolution ou l'élimination. Vous pouvez résoudre le problème, éliminer la menace immédiatement ou traiter le problème ultérieurement.

► Pour résoudre le problème ou éliminer la menace immédiatement,

cliquez sur le bouton reprenant le nom de l'action recommandée.

Par exemple, si des fichiers infectés ont été découverts sur l'ordinateur, il faut cliquer sur **Réparer**. Si les bases anti-virus sont dépassées, il faut cliquer sur **Mettre à jour**. L'application exécute l'action sélectionnée.

► Pour reporter l'élimination du problème ou de la menace,

cliquez sur le bouton **Masquer**.

Le message concernant le problème ou la menace sera masqué dans la liste. Vous pourrez revenir à l'élimination de ce problème ou de cette menace ultérieurement.

Vous ne pouvez pas reporter l'élimination des menaces sérieuses sur la sécurité de l'ordinateur. Les menaces sérieuses sont, par exemple, la présence d'objets malveillants non réparés, un échec de fonctionnement des modules de la protection ou l'endommagement des bases anti-virus de Kaspersky Internet Security.

Si vous quittez le Centre de protection sans avoir éliminé les menaces sérieuses, la couleur de l'indicateur d'état de la protection de l'ordinateur dans la fenêtre principale de l'application ne change pas.

La fenêtre Centre de protection permet également de consulter les informations relatives à la tâche de mise à jour ou aux tâches d'analyse en cours d'exécution et le cas échéant, d'arrêter ou de relancer ces tâches.

RESOLUTION DES PROBLEMES TYPES

Cette section explique comment exécuter pas à pas les principales fonctions de l'application.

DANS CETTE SECTION

Procédure d'exécution d'une analyse complète de l'ordinateur	42
Réalisation d'une analyse rapide de l'ordinateur	43
Comment rechercher d'éventuels virus dans un fichier, un répertoire ou un disque	43
Procédure d'achat d'une licence	43
Procédure de renouvellement de la licence	44
Procédure de mise à jour des bases de l'application	44
Procédure de protection contre l'interception des données saisies à l'aide du clavier traditionnel	45
Comment protéger les transactions financières et les achats en ligne sur le site Internet de la banque, le système de paiement ou les boutiques en ligne	45
Procédure de restriction de la durée de navigation de l'enfant ou de l'adolescent sur Internet	46
Restriction des consultations de sites Internet et du téléchargement de fichiers pour les enfants ou les adolescents	47
Restriction des contacts et des communications sur les réseaux sociaux pour les enfants ou les adolescents	48
Procédure d'interdiction du transfert de données personnelles pour les enfants ou les adolescents	48
Que faire si l'application a bloqué l'accès au fichier	49
Procédure de restauration d'un fichier supprimé ou réparé par l'application	50
Emplacement du rapport sur le fonctionnement de l'application	50
Que faire en cas d'affichage de fenêtres de notification et de messages contextuels	50

PROCEDURE D'EXECUTION D'UNE ANALYSE COMPLETE DE L'ORDINATEUR

La tâche d'analyse complète (créée par défaut) de l'ordinateur fait partie de Kaspersky Internet Security. Dans le cadre de cette tâche, l'application analyse tous les disques durs de l'ordinateur à la recherche de virus et d'autres programmes dangereux.

► *Pour lancer la tâche d'analyse complète de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).

2. Cliquez sur le bouton .

3. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse complète**.

La tâche d'analyse complète de l'ordinateur démarre automatiquement.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports.

REALISATION D'UNE ANALYSE RAPIDE DE L'ORDINATEUR

La tâche d'analyse rapide (créée par défaut) de l'ordinateur fait partie de Kaspersky Internet Security. Dans le cadre de cette tâche, l'application recherche la présence éventuelle de virus et autres programmes dangereux dans les secteurs critiques de l'ordinateur : dossiers contenant les fichiers du système d'exploitation et les bibliothèques système dont l'infection par des programmes malveillants pourrait endommager le système d'exploitation de l'ordinateur.

► Pour lancer la tâche d'analyse rapide de l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton .
3. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse rapide**.

La tâche d'analyse rapide de l'ordinateur démarre automatiquement.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports.

COMMENT RECHERCHER D'EVENTUELS VIRUS DANS UN FICHIER, UN REPERTOIRE OU UN DISQUE

Si vous devez rechercher la présence éventuelle de virus et d'autres programmes dangereux dans un objet distinct (un des disques durs, un dossier ou un fichier en particulier ou un périphérique amovible), vous pouvez utiliser la tâche préconfigurée **Analyse personnalisée**.

► Pour rechercher la présence éventuelle de virus ou d'autres programmes dangereux dans un objet distinct, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton .
3. Dans la fenêtre **Analyse** qui s'ouvre, sélectionnez la tâche  **Analyse personnalisée**.

La liste déroulante de sélection de la zone d'analyse s'ouvre.

4. Dans la liste qui s'ouvre, choisissez l'option qui vous convient le mieux (**fichiers ou dossiers, Tous les disques**, etc.) ou déplacez les fichiers et les dossiers sur la fenêtre.

L'analyse démarre automatiquement dans la zone indiquée.

Pour lancer l'analyse, vous pouvez également faire glisser le fichier et le dossier sur l'icône de l'application dans le **Dock** ou dans la fenêtre principale de l'application (cf. page [20](#)) ouverte.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports.

PROCEDURE D'ACHAT D'UNE LICENCE

Si vous avez installé Kaspersky Internet Security sans licence, vous pouvez acheter une licence après l'installation de l'application. Lors de l'achat d'une licence, vous recevez le code requis pour activer l'application (cf. section "Activation de Kaspersky Internet Security" à la page [34](#)).

➤ *Pour acheter une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.

La fenêtre **Licence** s'ouvre.

3. Dans la fenêtre **Licence**, cliquez sur **Acheter**.

Le portail My Kaspersky ou la page de la boutique en ligne de Kaspersky Lab ou de notre partenaire s'ouvre et vous permet d'acheter une licence.

PROCEDURE DE RENOUELEMENT DE LA LICENCE

Quand la durée de validité de la licence utilisée pour activer Kaspersky Internet Security approche de son échéance, vous pouvez la renouveler. Lors du renouvellement de la licence, vous obtenez le code d'activation qui permet d'activer l'application (cf. section "Activation de Kaspersky Internet Security" à la page [34](#)).

➤ *Pour renouveler une licence, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure droite de la fenêtre principale de l'application.

La fenêtre **Licence** s'ouvre.

3. Dans la fenêtre **Licence**, cliquez sur le bouton **Renouveler**.

Le portail My Kaspersky ou la page de la boutique en ligne de Kaspersky Lab ou de notre partenaire s'ouvre et vous permet de renouveler la licence.

PROCEDURE DE MISE A JOUR DES BASES DE L'APPLICATION

Kaspersky Lab actualise les bases anti-virus de Kaspersky Internet Security via des serveurs de mises à jour. *Serveurs de mises à jour de Kaspersky Lab* : serveurs HTTP de Kaspersky Lab présentant des mises à jour régulières des bases de Kaspersky Internet Security.

Pour réussir le téléchargement des mises à jour depuis les serveurs, la connexion de l'ordinateur à Internet est requise.

Par défaut, Kaspersky Internet Security recherche périodiquement la présence de mises à jour sur les serveurs de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Internet Security les télécharge en arrière-plan et les installe sur l'ordinateur.

➤ *Pour lancer la mise à jour de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton .
3. Dans la fenêtre **Mise à jour** qui s'ouvre, cliquez sur **Mettre à jour**.

Les résultats de l'exécution de la tâche sont présentés dans la fenêtre des rapports.

PROCEDURE DE PROTECTION CONTRE L'INTERCEPTION DES DONNEES SAISIES A L'AIDE DU CLAVIER TRADITIONNEL

Les individus malintentionnés peuvent intercepter vos données lorsque vous les saisissez à l'aide du clavier de l'ordinateur. Ils peuvent ainsi obtenir les données de votre carte de paiement lorsque vous les saisissez sur la page d'une boutique en ligne. Le clavier virtuel permet d'éviter l'interception des données saisies.

Kaspersky Internet Security protège la saisie des données à l'aide d'un clavier virtuel que vous pouvez installer dans les navigateurs Safari, Firefox et Google Chrome.

Le clavier virtuel ne peut protéger vos données si le site Internet sur lequel vous saisissez ces données a été compromis. En effet, dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

Le clavier virtuel possède les caractéristiques suivantes :

- Il faut appuyer sur les touches du clavier à l'aide de la souris.
- A la différence du clavier ordinaire, le clavier virtuel ne vous permet pas d'appuyer sur plusieurs touches en même temps. Par conséquent, pour saisir un caractère tapé sur un clavier normal à l'aide de la combinaison de touches **ALT** et/ou **SHIFT**, il faut d'abord appuyer sur la première touche (par exemple **ALT**), puis sur la touche illustrant le caractère requis.
- Sur le clavier virtuel, la langue de saisie peut être modifiée à l'aide de la touche située dans le coin inférieur gauche. Vous pouvez appuyer sur cette touche et saisir la langue souhaitée dans la liste déroulante.

Par défaut, le clavier virtuel s'affiche automatiquement quand un champ de saisie a été sélectionné dans une fenêtre du navigateur.

➔ *Pour ouvrir le clavier virtuel,*

cliquez sur le bouton  dans la barre d'outils du navigateur.

COMMENT PROTEGER LES TRANSACTIONS FINANCIERES ET LES ACHATS EN LIGNE SUR LE SITE INTERNET DE LA BANQUE, LE SYSTEME DE PAIEMENT OU LES BOUTIQUES EN LIGNE

Pour que l'application Kaspersky Internet Security commence à protéger vos opérations financières ou vos achats en ligne, il faut ajouter les sites de la banque, du système de paiement ou de la boutique en ligne à la liste des sites Internet protégés par l'application.

➔ *Pour ajouter cette banque, ce système de paiement ou cette boutique en ligne à la liste des sites protégés par Kaspersky Internet Security, réalisez les opérations suivantes dans la fenêtre Protection bancaire :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).
2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre principale de l'application.

La fenêtre **Protection bancaire** s'ouvre.

3. Cliquez sur le bouton **+**.

Ouvre la fenêtre de saisie des données du site que vous ajoutez et dans laquelle il faut définir l'action que l'application exécutera à l'ouverture du site.

4. Saisissez l'adresse de la banque, du système de paiement ou de la boutique en ligne dans le champ **Adresse du site Internet**.

Vous ne pouvez ajouter que des sites qui utilisent une connexion HTTPS.

5. Saisissez le nom de la banque, du système de paiement ou de la boutique en ligne dans le champ **Nom**.
6. Choisissez l'option **Utiliser le mode protégé (vérifier l'authenticité du site Internet)**.

L'application activera le mode protégé dès que vous ouvrirez ce site Internet. Dans ce mode, Kaspersky Security Network analyse l'authenticité des sites Internet des banques, des systèmes de paiement et des boutiques en ligne. Il analyse également les certificats qui permettent d'établir les connexions sécurisées.

7. Cliquez sur le bouton **Ajouter**.

- *Pour ajouter cette banque, ce système de paiement ou cette boutique en ligne à la liste des sites protégés par Kaspersky Internet Security, réalisez les opérations suivantes dans la fenêtre du navigateur :*

1. Ouvrez dans le navigateur le site de la banque, du système de paiement ou de la boutique en ligne que vous souhaitez ajouter.

Vous ne pouvez ajouter que des sites qui utilisent une connexion HTTPS.

Un message de Kaspersky Internet Security apparaît dans le navigateur. Il permet d'activer le mode de fonctionnement protégé du navigateur pour ce site. Dans ce mode, Kaspersky Security Network analyse l'authenticité des sites Internet des banques, des systèmes de paiement et des boutiques en ligne. Il analyse également les certificats qui permettent d'établir les connexions sécurisées.

2. Cliquez sur le bouton **Utiliser le mode protégé**.

PROCEDURE DE RESTRICTION DE LA DUREE DE NAVIGATION DE L'ENFANT OU DE L'ADOLESCENT SUR INTERNET

Trop de temps passé sur l'ordinateur peut nuire à la santé des enfants et des adolescents. Si vous devez limiter la durée d'utilisation d'Internet, vous pouvez utiliser la catégorie Contrôle du temps du composant Contrôle parental.

- *Pour limiter la durée de navigation de l'utilisateur sur Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du Contrôle Parental (à la page [22](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le compte utilisateur pour lequel vous souhaitez limiter la durée d'utilisation d'Internet.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Activer le Contrôle Parental**.
4. Dans la partie droite de la fenêtre, sous l'onglet **Paramètres**, sélectionnez la catégorie d'actions **Contrôle du temps**. Si la fonction Contrôle du temps est désactivée, il faut l'activer.
5. Dans le groupe **Utilisation d'Internet par jour**, cochez la case **Durée d'utilisation d'Internet maximum**.

6. A l'aide du curseur, sélectionnez le nombre d'heures par jour pendant lequel la navigation sur Internet sera autorisée.
7. Dans le groupe **Utilisation d'Internet à certaines heures**, cochez la case **Autoriser l'utilisation d'Internet selon les jours de la semaine**.
8. Définissez les restrictions sur l'horaire d'utilisation d'Internet pendant les jours ouvrés et les week-ends.

Le rapport sur la navigation de l'utilisateur sur Internet aux périodes autorisées ou non est accessible sous l'onglet **Rapports** de la fenêtre des paramètres du Contrôle Parental.

RESTRICTION DES CONSULTATIONS DE SITES INTERNET ET DU TELECHARGEMENT DE FICHIERS POUR LES ENFANTS OU LES ADOLESCENTS

Pour garantir la sécurité des enfants et des adolescents se servant de l'ordinateur, vous pouvez restreindre les actions suivantes :

- La visite de sites Internet dont le contenu peut provoquer une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites d'enchères).
- L'accès à des sites Web réservés aux adultes (contenu pornographique, contenu extrême faisant l'apologie des armes, de la drogue, de la violence, etc.).
- le téléchargement de certains types de fichiers.

Vous pouvez utiliser la catégorie Contrôle Internet du Contrôle Parental.

➡ *Pour limiter l'accès à certains sites et le téléchargement de fichiers depuis Internet, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du Contrôle Parental (à la page [22](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le compte utilisateur pour lequel vous souhaitez limiter l'accès aux sites Internet et le téléchargement de fichiers depuis Internet.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Activer le Contrôle Parental**.
4. Dans la partie droite de la fenêtre, sous l'onglet **Paramètres**, sélectionnez la catégorie d'actions **Contrôle Internet**. Si la fonction Contrôle Internet est désactivée, il faut l'activer.
5. Cochez la case **Contrôle Internet** ainsi que les cases des catégories de sites Internet dont l'accès doit être bloqué dans la liste en dessous.
6. Cochez la case **Le Contrôle des fichiers téléchargés** et les cases correspondant aux catégories de fichier dont le téléchargement est autorisé.

Le cas échéant, vous pouvez autoriser l'accès à certains sites Internet qui appartiennent à une catégorie interdite ou interdire l'accès à certains sites en composant une liste d'exclusions.

Le rapport sur les tentatives d'accès aux sites bloqués et de téléchargement de catégories de fichier interdites est accessible sous l'onglet **Rapports** de la fenêtre des paramètres du Contrôle Parental.

RESTRICTION DES CONTACTS ET DES COMMUNICATIONS SUR LES RESEAUX SOCIAUX POUR LES ENFANTS OU LES ADOLESCENTS

Le contrôle des contacts et des communications des enfants et des adolescents sur les réseaux sociaux tels que Facebook, Myspace et Twitter permet d'éviter des contacts avec des inconnus qui se présentent sous les traits de copains pour obtenir des informations confidentielles sur le mineur. Si vous devez limiter les contacts et les communications des utilisateurs dans les réseaux sociaux, vous pouvez utiliser la catégorie Réseaux sociaux du Contrôle parental.

➔ *Pour limiter les contacts et les échanges sur les réseaux sociaux, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du Contrôle Parental (à la page [22](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le compte utilisateur pour lequel vous souhaitez limiter les échanges sur les réseaux sociaux.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Activer le Contrôle Parental**.
4. Dans la partie droite de la fenêtre, sous l'onglet **Paramètres**, sélectionnez la catégorie d'actions **Réseaux sociaux**. Si le contrôle des réseaux sociaux est désactivé, il faut l'activer.
5. Composez la liste des contacts autorisés et interdits. Pour ce faire, cliquez sur le bouton et saisissez dans le champ de la colonne **ID** l'identificateur du contact sur les réseaux sociaux et dans la colonne **Nom d'utilisateur**, son nom réel.

L'identificateur du contact sur les réseaux sociaux peut être consulté dans l'onglet **Rapports** pour la catégorie d'actions de l'utilisateur **Réseaux sociaux**.

Après l'ajout d'un contact dans la liste, le Contrôle parental interdit les échanges avec ce contact sur les réseaux sociaux.

6. Si vous souhaitez autoriser temporairement la communication avec un contact, sélectionnez-le dans la liste et décochez la case dans la colonne **Bloqué**.

La communication avec ce contact sera autorisée tant que la case ne sera pas à nouveau cochée.

Si l'échange de messages avec un contact est interdit, tous les messages envoyés à ce contact ou par celui-ci seront bloqués par le Contrôle Parental.

L'onglet **Rapports** de la fenêtre des paramètres du Contrôle Parental comporte les informations suivantes :

- informations sur les messages envoyés au contact interdit ou reçus de celui-ci ;
- informations sur la présence de données personnelles dans les messages ;
- texte des messages avec chaque contact.

PROCEDURE D'INTERDICTION DU TRANSFERT DE DONNEES PERSONNELLES POUR LES ENFANTS OU LES ADOLESCENTS

Kaspersky Internet Security permet de diminuer les risques liés à l'utilisation de l'ordinateur et d'Internet. Vous pouvez interdire le transfert de données contenant des informations personnelles via les réseaux sociaux ou lors de l'envoi de données sur un site Internet grâce à la catégorie Données personnelles du Contrôle parental.

➤ *Pour interdire le transfert de données personnelles, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du Contrôle Parental (à la page [22](#)).
2. Dans la partie gauche de la fenêtre, sélectionnez le compte utilisateur pour lequel vous souhaitez interdire le transfert de données personnelles.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Activer le Contrôle Parental**.
4. Dans la partie droite de la fenêtre, sous l'onglet **Paramètres**, sélectionnez la catégorie d'actions **Données personnelles**. Si le contrôle des données personnelles est désactivé, il faut l'activer.
5. Créez la liste des données personnelles. Pour ce faire, cliquez sur le bouton et saisissez les données dans le champ des colonnes **Description** et **Données**. Par exemple, vous pouvez créer des enregistrements pour un numéro de carte bancaire, une adresse privée ou un numéro de téléphone.

Après l'ajout des données personnelles dans la liste, le Contrôle parental interdit leur transfert sur les réseaux sociaux ou les sites Internet.

Kaspersky Internet Security bloque toutes les tentatives de transfert de données ajoutées à la liste. L'onglet **Rapports** de la fenêtre des paramètres du Contrôle Parental comporte les informations sur les messages bloqués.

QUE FAIRE SI L'APPLICATION A BLOQUE L'ACCES AU FICHER

Kaspersky Internet Security bloque l'accès aux fichiers ou programmes infectés ou potentiellement infectés. Si un fichier est infecté, il est indispensable de le réparer pour y accéder.

➤ *Pour réparer les objets détectés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).

2. Cliquez sur le bouton .

La fenêtre des rapports de Kaspersky Internet Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports, choisissez **Objets détectés**.

La liste des objets détectés et de leur état sera affichée dans le groupe **Actifs** de la partie droite de la fenêtre. Pour développer la liste des objets, cliquez sur le bouton ►.

4. Réparez tous les objets infectés détectés ou un d'entre eux :

- Si vous souhaitez réparer tous les objets infectés détectés, cliquez sur le bouton **Tout réparer**.

L'application commencera la réparation des objets détectés. Une fenêtre de notification apparaît lors de la réparation pour que vous puissiez sélectionner l'action à exécuter sur l'objet. Si, après la sélection des actions à réaliser sur les objets, vous cochez la case **Appliquer à tous les cas similaires** dans la fenêtre de notification, l'action sélectionnée sera appliquée à tous les fichiers de ce type.

- Si vous souhaitez réparer un seul objet infecté détecté, sélectionnez-le dans la liste, puis cliquez sur le bouton **Réparer**.

L'application commencera la réparation de l'objet sélectionné. Une fenêtre de notification apparaît lors de la réparation pour que vous puissiez sélectionner l'action à exécuter sur l'objet.

Si vous êtes convaincu que les fichiers bloqués par l'Anti-Virus Fichiers ne présentent aucun danger, ajoutez-les à la zone de confiance.

PROCEDURE DE RESTAURATION D'UN FICHIER SUPPRIME OU REPARÉ PAR L'APPLICATION

Il est déconseillé, sauf urgence, de restaurer les fichiers supprimés et réparés car ils pourraient constituer une menace pour votre ordinateur.

Il n'est pas toujours possible de préserver l'intégrité des fichiers infectés lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de le restaurer à partir de sa copie de sauvegarde.

➔ *Pour restaurer un fichier supprimé ou modifié lors de la réparation, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).

2. Cliquez sur le bouton .

La fenêtre des rapports de Kaspersky Internet Security s'ouvre.

3. Dans la partie gauche de la fenêtre des rapports, sélectionnez **Quarantaine**.

La partie droite de la fenêtre présente le contenu de la quarantaine sous forme de liste des copies de sauvegarde des objets.

4. Sélectionnez la copie de sauvegarde du fichier nécessaire dans la liste et cliquez sur le bouton **Restaurer**. Confirmez l'action dans la fenêtre qui s'ouvre.

Le fichier sera restauré dans l'emplacement d'origine avec le même nom qu'avant la réparation ou la suppression. Si l'emplacement d'origine contient un fichier portant le même nom (cette situation est possible en cas de restauration d'un fichier dont la copie avait déjà été créée avant la réparation), un avertissement apparaîtra à l'écran. Vous pouvez modifier l'emplacement du fichier restauré ainsi que son nom.

Nous recommandons d'analyser les fichiers tout de suite après la restauration. Il sera possible de le réparer avec les bases anti-virus les plus récentes tout en préservant son intégrité.

EMPLACEMENT DU RAPPORT SUR LE FONCTIONNEMENT DE L'APPLICATION

Les informations relatives aux événements survenus pendant l'utilisation de l'Anti-Virus Fichiers, de l'Anti-Virus Internet, de la prévention des intrusions pendant l'exécution des tâches d'analyse ou de mise à jour apparaissent dans la fenêtre des rapports.

➔ *Pour ouvrir la fenêtre des rapports,*

ouvrez la fenêtre principale de l'application (à la page [20](#)) et cliquez sur le bouton .

QUE FAIRE EN CAS D'AFFICHAGE DE FENETRES DE NOTIFICATION ET DE MESSAGES CONTEXTUELS

Les notifications de l'application (cf. section "Fenêtres de notifications et fenêtres contextuelles" à la page [23](#)) sous la forme de fenêtres de notification signalent les événements survenus pendant le fonctionnement de l'application et qui requièrent votre attention.

Quand un tel message apparaît, il faut sélectionner une des actions proposées. L'action optimale est celle qui est recommandée par les experts de Kaspersky Lab par défaut.

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Internet Security à l'aide de la ligne de commande.

La syntaxe de la ligne de commande est la suivante :

```
kav <commande> [paramètres]
```

Vous pouvez envoyer les <commandes> suivantes :

- **help** : aide sur la syntaxe de la commande, affichage d'une liste de commandes ;
- **scan** : analyse des objets à la recherche de programmes malveillants ;
- **update** : lancement de la mise à jour de l'application ;
- **rollback** : retour à l'état antérieur à la dernière mise à jour de Kaspersky Internet Security (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **start** : lancement du composant ou de la tâche ;
- **stop** : arrêt du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **status** : apparition à l'écran de l'état actuel du composant ou de la tâche ;
- **statistics** : apparition à l'écran des statistiques de fonctionnement du composant ou de la tâche ;
- **export** : exportation des paramètres du composant ou de la tâche ;
- **import** : importation des paramètres du composant ou de la tâche (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **addkey** : activation de l'application à l'aide du fichier clé (l'exécution de cette instruction requiert les privilèges d'administrateur) ;
- **exit** : quitte l'application (l'exécution de cette instruction requiert les privilèges d'administrateur).

Chaque commande possède sa propre sélection de paramètres.

DANS CETTE SECTION

Consultation de l'aide.....	52
Recherche de virus.....	52
Mise à jour de l'application.....	54
Annulation de la dernière mise à jour.....	55
Lancement/arrêt d'un composant ou d'une tâche.....	55
Statistiques du fonctionnement du composant ou de la tâche.....	56
Exportation des paramètres de protection.....	56
Importation des paramètres de protection.....	57
Arrêt de l'application.....	57
Codes de retour de la ligne de commande.....	57

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
kav [ -? | help ]
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
kav <commande> -?
```

```
kav help <commande>
```

RECHERCHE DE VIRUS

La ligne de commande pour le lancement de la recherche d'éventuels virus dans un secteur quelconque ressemble à ceci :

```
kav scan [<zone d'analyse>] [<action>] [<types de fichiers>] [<exclusions>]
[<paramètres du rapport>] [< paramètres complémentaires >]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande (cf. section "Lancement/arrêt du fonctionnement du composant ou de la tâche" à la page [55](#)). Dans ce cas, la tâche est réalisée selon les paramètres définis dans l'interface de Kaspersky Internet Security.

Description des paramètres

<zone d'analyse> : ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace :

<files> : liste des chemins d'accès aux fichiers et/ou dossiers à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques :

- si le nom de l'objet ou le chemin d'accès contient un espace ou un caractère spécial (\$, &, @, etc.), il doit être repris entre guillemets ou le caractère doit être précédé d'une barre oblique inverse ;
- lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.

-all : analyse complète de l'ordinateur ;

-remdrives : tous les disques amovibles ;

-fixdrives : tous les disques durs ;

-netdrives : tous les disques réseau ;

-@:<filelist.lst> : chemin d'accès au fichier contenant une liste d'objets et de dossiers à soumettre à l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. Seuls les chemins absolus au fichier sont admis.

Si la zone d'analyse n'est pas définie, Kaspersky Internet Security lance la tâche Analyse personnalisée avec les paramètres définis dans l'interface de l'application.

<action> : le paramètre définit les actions à réaliser sur les objets malveillants détectés lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **-i8**. Les valeurs suivantes sont possibles :

-i0 : ne réaliser aucune action sur l'objet, conserver uniquement les informations le concernant dans le rapport ;

-i1 : réparer les objets infectés, si la réparation est impossible, les ignorer ;

-i2 : réparer les objets infectés, si la réparation est impossible, les supprimer ; ne pas supprimer les objets infectés des conteneurs, sauf les conteneurs avec un en-tête exécutable (archives sfx) ;

-i3 : réparer les objets infectés, si la réparation est impossible, les supprimer ; supprimer complètement les conteneurs s'il est impossible de supprimer les fichiers infectés qu'ils contiennent ;

-i4 : supprimer les objets infectés ; supprimer complètement les conteneurs s'il est impossible de supprimer les fichiers infectés qu'ils contiennent ;

-i8 : confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté (cette action est utilisée par défaut) ;

-i9 : confirmer l'action auprès de l'utilisateur à la fin de l'analyse.

Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Par défaut, si le paramètre n'est pas défini, seuls seront analysés les objets pouvant être infectés en fonction du contenu. Les valeurs suivantes sont possibles :

-fe : analyser uniquement les fichiers qui peuvent être infectés selon l'extension ;

-fi : analyser uniquement les fichiers qui peuvent être infectés selon le contenu (par défaut) ;

-fa : analyser tous les fichiers.

<exclusions> : ce paramètre définit les objets qui sont exclus de l'analyse. Il est possible d'utiliser plusieurs paramètres de la liste suivante, à condition de les séparer par un espace :

-e:a : ne pas analyser les archives ;

-e:b : ne pas analyser les bases de messagerie ;

-e:m : ne pas analyser les messages électroniques au format texte ;

-e:<mask> : ne pas analyser les objets selon le masque ;

-e:<seconds> : ignorer les objets dont l'analyse dure plus que la valeur définie en secondes ;

-es:<size> : ignorer les objets dont la taille dépasse la valeur définie en mégaoctets.

<paramètres du rapport> : ce paramètre définit le format du rapport de l'analyse anti-virus. Les chemins relatifs et absolus au fichier pour l'enregistrement du rapport sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

-r:<report_file> : consigner uniquement les événements importants dans le fichier du rapport indiqué ;

-ra:<report_file> : consigner tous les événements dans le fichier du rapport.

<paramètres complémentaires> : paramètres qui définissent l'utilisation des technologies de l'analyse antivirus et l'utilisation du fichier de configuration :

-iSwift=<on|off> : activer / désactiver l'utilisation de la technologie iSwift ;

-c:<settings_file> : ce paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les valeurs définies dans l'interface utilisateur de l'application sont utilisées en plus des valeurs déjà indiquées dans la ligne de commande.

Exemple :

Lancer l'analyse des dossiers ~/Documents, /Applications et du fichier my test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_settings.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

Exemple de fichier de configuration :

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

MISE A JOUR DE L'APPLICATION

La commande de mise à jour de l'application possède la syntaxe suivante :

```
kav update [<source_de_la_mise_à_jour>] [-app=<on|off>] [<paramètres_de_rapport>]
[<paramètres_complémentaires>]
```

Description des paramètres

<source_des_mises_à_jour> : serveur HTTP, répertoire réseau ou local utilisé pour le téléchargement des mises à jour. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.

-app=<on|off> : active/désactive la mise à jour des modules de l'application.

<paramètres du rapport> : ce paramètre définit le format du rapport de l'analyse anti-virus. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport.

<paramètres complémentaires> : paramètre qui définit l'utilisation du fichier de configuration des paramètres.

-c:<nom_du_fichier_de_configuration> : ce paramètre définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par l'application pour la mise à jour. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.

Exemple :

Actualiser les bases de l'application depuis la source par défaut et consigner tous les événements dans le rapport :

```
kav update -ra:avbases_upd.txt
```

Mettre à jour les modules de Kaspersky Internet Security en utilisant les paramètres du fichier de configuration updateapp.ini :

```
kav update -app=on -c:updateapp.ini
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
kav rollback [<paramètres_du_rapport>]
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<paramètres du rapport> : le paramètre définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport.

Exemple :

```
kav rollback -ra:rollback.txt
```

LANCEMENT/ARRET D'UN COMPOSANT OU D'UNE TACHE

Syntaxe de la commande start :

```
kav start <profil|nom_de_la_tâche> [<paramètres_du_rapport>]
```

Syntaxe de la commande stop :

```
kav stop <profil|nom_de_la_tâche>
```

L'exécution de l'instruction stop requiert les privilèges d'administrateur.

Description des paramètres

<paramètres du rapport> : ce paramètre définit le format du rapport de l'analyse anti-virus. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements. Les valeurs suivantes sont possibles :

-r:<report_file> : consigner uniquement les événements importants dans le fichier indiqué ;

-ra:<report_file> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

<profil|nom_de_la_tâche> : peut contenir une des valeurs suivantes :

file_monitoring (fm) : Anti-Virus Fichiers ;

web_monitoring (wm) : Anti-Virus Internet ;

scan_my_computer (full) : tâche d'analyse complète de l'ordinateur ;

scan_objects : tâche d'analyse personnalisée ;

scan_critical_areas (quick) : tâche d'analyse rapide de l'ordinateur ;

updater : tâche de mise à jour ;

rollback : tâche d'annulation de mise à jour.

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemple :

Pour activer l'Anti-Virus Fichiers, saisissez dans la ligne de commande :

```
kav start fm
```

Pour arrêter la tâche d'analyse complète, saisissez dans la ligne de commande :

```
kav stop scan_my_computer
```

STATISTIQUES DU FONCTIONNEMENT DU COMPOSANT OU DE LA TÂCHE

Syntaxe de la commande status :

```
kav status [<profil|nom_de_la_tâche>]
```

Syntaxe de la commande statistics :

```
kav statistics <profil|nom_de_la_tâche>
```

Description des paramètres

<profil|nom_de_la_tâche> désigne une des valeurs reprises pour l'instruction start / stop (cf. section "Lancement/arrêt d'un composant ou d'une tâche" à la page [55](#)).

Si la commande status est lancée sans paramètre **<profil|nom_de_la_tâche>** défini, l'application affichera l'état actuel de toutes ses tâches et composants. La valeur du paramètre **<profil|nom_de_la_tâche>** de la commande statistics doit être obligatoirement définie.

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav export <profil|nom_de_la_tâche> <nom_du_fichier>
```

Description des paramètres

<profil|nom_de_la_tâche> désigne une des valeurs reprises pour l'instruction start / stop (cf. section "Lancement/arrêt d'un composant ou d'une tâche" à la page [55](#)).

<nom_du_fichier> : chemin d'accès au fichier dans lequel les paramètres de l'application sont exportés. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple :

```
kav export fm fm_settings.txt - format texte
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
kav import <nom_du_fichier>
```

L'exécution de cette commande requiert les privilèges d'administrateur.

Description des paramètres

<nom_du_fichier> : chemin d'accès au fichier contenant les paramètres de l'application à importer. Vous pouvez indiquer un chemin relatif ou absolu.

Exemple:

```
kav import settings.dat
```

ARRET DE L'APPLICATION

Syntaxe de la commande :

```
kav exit
```

L'exécution de cette commande requiert les privilèges d'administrateur.

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches reprennent les codes généraux et les codes spécifiques à un type de tâche en particulier.

Codes de retour généraux :

- 0 – opération réussie ;
- 1 – valeur de paramètre invalide ;
- 2 – erreur inconnue ;
- 3 – erreur d'exécution de la tâche ;
- 4 – annulation de l'exécution de la tâche.

Codes de retour des tâches d'analyse antivirus :

- 101 – tous les objets malveillants ont été traités ;
- 102 – des objets malveillants ont été détectés.

CONTACTER LE SUPPORT TECHNIQUE

Cette section décrit les modes de support technique et les conditions nécessaires pour bénéficier du Support technique.

DANS CETTE SECTION

Modes d'obtention du support technique.....	58
Support technique par téléphone.....	58
Support technique via le portail My Kaspersky.....	59
Utilisation du fichier de traçage.....	59
Création d'un fichier de traçage.....	60
Envoi des fichiers comportant des informations sur l'erreur à Kaspersky Lab.....	60

MODES D'OBTENTION DU SUPPORT TECHNIQUE

➔ Pour consulter les informations sur les moyens d'obtenir une assistance technique pour Kaspersky Internet Security,

ouvrez la fenêtre principale de l'application (à la page [20](#)) et cliquez sur le bouton .

Si vous n'avez pas trouvé de solution à votre problème dans la documentation de l'application ni dans aucune des sources d'information sur l'application, nous vous conseillons de contacter le Support Technique de Kaspersky Lab. Les experts du Support technique répondront à toutes vos questions concernant l'installation et l'utilisation de l'application.

Avant de contacter le Support Technique, veuillez lire les règles d'octroi de l'assistance technique (<http://support.kaspersky.com/fr/support/rules>).

Vous pouvez contacter les experts du Support Technique par un des moyens suivants :

- Appeler par téléphone. Ce moyen permet d'obtenir une consultation par téléphone avec des experts du Support Technique russophone ou international.
- Soumettre une demande depuis l'Espace personnel sur le site Internet du Support Technique <https://my.kaspersky.com/>. Ce moyen permet de contacter les experts du Support Technique via un formulaire de demande.

L'assistance technique est fournie uniquement aux utilisateurs de l'application qui ont acheté une licence. L'assistance technique pour les utilisateurs d'une version d'évaluation n'est pas prévue.

SUPPORT TECHNIQUE PAR TELEPHONE

En cas de problème urgent, vous pouvez contacter les experts du support technique de Kaspersky Lab (<http://support.kaspersky.com/fr/b2c>).

Avant de contacter le Service de Support Technique, veuillez prendre connaissance des Conditions d'accès au Support Technique (<http://support.kaspersky.com/fr/support/rules>). Ces règles précisent les heures auxquelles vous pouvez contacter le Support Technique de Kaspersky Lab ainsi que les données à fournir à l'expert pour qu'il puisse vous venir en aide.

SUPPORT TECHNIQUE VIA LE PORTAIL MY KASPERSKY

Le portail My Kaspersky constitue votre unique ressource en ligne pour la gestion de la protection de l'ensemble de vos périphériques et de vos licences Kaspersky Lab.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (<https://my.kaspersky.com/fr/registration>).

Le portail My Kaspersky permet de réaliser les opérations suivantes :

- soumettre des demandes au Support Technique et au laboratoire des virus de Kaspersky Lab ;
- communiquer avec le Support Technique sans envoyer de courrier électronique ;
- suivre l'état de vos demandes en temps réel ;
- consulter l'historique complet de vos demandes adressées au Support Technique ;
- recevoir une copie du fichier clé en cas de perte ou suppression éventuelle.

Requête électronique adressée au Support Technique

Vous pouvez soumettre une demande électronique au Support Technique en russe, en anglais, en allemand, en français et en espagnol.

Lors de la soumission d'une demande, fournissez les renseignements suivants :

- type de demande ;
- nom et numéro de la version de l'application ;
- texte de la demande.

Demande électronique envoyée au Laboratoire des virus de Kaspersky Lab

Certaines demandes doivent être soumises au Laboratoire des virus et non au Support Technique.

Vous pouvez transmettre les types de demandes suivants au laboratoire d'étude des virus :

- Si vous pensez que le fichier ou la ressource Web contient un virus mais que Kaspersky Internet Security ne détecte aucune menace. Les experts du Laboratoire d'étude des virus analysent le fichier ou l'adresse Internet et, en cas de détection d'un virus inconnu jusque-là, ils ajoutent les informations le concernant à la base de données accessible lors de la mise à jour des applications antivirus de Kaspersky Lab.
- Si Kaspersky Internet Security identifie un fichier ou une ressource Web comme porteur d'un virus mais que vous êtes sûr que ce n'est pas le cas.

UTILISATION DU FICHIER DE TRAÇAGE

Après avoir communiqué votre problème aux experts du Support Technique de Kaspersky Lab, ces derniers peuvent vous demander de créer un rapport contenant les informations sur le fonctionnement de Kaspersky Internet Security et de leur envoyer ce document. Les experts du Support Technique de Kaspersky Lab peuvent également vous demander de créer *un fichier de traçage*. Le fichier de traçage permet de suivre pas à pas le processus d'exécution des commandes de l'application et de découvrir à quelle étape se produit une erreur.

CREATION D'UN FICHIER DE TRAÇAGE

➤ Pour créer un fichier de traçage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).

2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Rapports** de la fenêtre des paramètres de l'application, dans le groupe **Traçage**, cochez la case **Activer le traçage**.

4. Relancez Kaspersky Internet Security pour lancer le processus de traçage.

Utilisez le traçage uniquement sous la direction d'un spécialiste du Support Technique de Kaspersky Lab.

Les fichiers de traçage peuvent occuper beaucoup d'espace sur le disque. Après avoir terminé le travail avec les fichiers de traçage, il est recommandé de désactiver leur création en décochant la case **Activer le traçage** sous l'onglet **Rapports** de la fenêtre des paramètres de l'application. Il est ensuite nécessaire de relancer Kaspersky Internet Security.

ENVOI DES FICHIERS COMPORTANT DES INFORMATIONS SUR L'ERREUR A KASPERSKY LAB

Kaspersky Internet Security permet d'enregistrer et d'envoyer automatiquement à Kaspersky Lab des informations sur l'état de l'application lorsque des erreurs surviennent.

➤ Pour activer l'envoi automatique des fichiers d'information sur les erreurs à Kaspersky Lab, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application (cf. page [20](#)).

2. Dans la fenêtre principale de l'application, cliquez sur le bouton .

La fenêtre des paramètres de l'application s'ouvre.

3. Sous l'onglet **Rapports** de la fenêtre des paramètres de l'application, dans le groupe **Rapport d'erreurs**, cochez la case **Envoyer le rapport automatiquement**.

Vous pouvez également activer l'envoi automatique de fichiers d'information sur l'erreur à Kaspersky Lab dans la fenêtre de notification sur l'erreur de lancement de l'application.

GLOSSAIRE

A

ACTIVATION DE L'APPLICATION

L'application devient entièrement fonctionnelle. L'activation est exécutée par l'utilisateur pendant ou après l'installation de l'application. Pour activer l'application, l'utilisateur doit posséder le code d'activation ou le fichier clé.

ANALYSEUR HEURISTIQUE

La technologie de détection des menaces dont les informations ne sont pas inscrites dans les bases de Kaspersky Lab. L'analyseur heuristique permet de découvrir les objets dont le comportement dans le système d'exploitation évoque celui d'une menace. Les objets détectés à l'aide de l'analyseur heuristique sont reconnus comme des objets potentiellement infectés. Par exemple, l'objet contenant les suites des commandes propres aux objets infectés (ouverture des fichiers, enregistrement dans le fichier) peut être reconnu comme l'objet potentiellement infecté.

B

BASE ANTIVIRUS

Bases de données contenant les informations relatives aux menaces informatiques connues de Kaspersky Lab au moment de la publication des bases. Les entrées des bases antivirus permettent de détecter le code malveillant dans les objets analysés. Les Bases antivirus sont composées par les experts de Kaspersky Lab et sont mises à jour toutes les heures.

BLOCAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté ou modifié.

C

CLE ACTIVE

La clé utilisée au moment actuel pour faire fonctionner l'application.

CLE DE RESERVE

La clé qui confirme le droit d'utilisation de l'application mais qui n'est pas utilisée actuellement.

E

ETAT DE PROTECTION

État actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

F

FAUX-POSITIFS

Situation qui se présente lorsqu'un objet sain est considéré par l'application de Kaspersky Lab comme étant infecté car son code évoque celui d'un virus.

L**LES SERVEURS DE MISE A JOUR DE KASPERSKY LAB**

Serveurs HTTP de Kaspersky Lab sur lesquels les applications de Kaspersky Lab récupèrent les mises à jour des bases et des modules de l'application.

M**MISE A JOUR**

La fonction de l'application de Kaspersky Lab qui permet de maintenir la protection de l'ordinateur dans l'état actuel. Pendant la mise à jour, l'application copie les mises à jour des bases et des modules de l'application à partir des serveurs de mises à jour de Kaspersky Lab sur l'ordinateur et les installe et les applique automatiquement.

O**OBJET INFECTE**

Objet dont un segment de code correspond parfaitement à un segment de code d'un programme dangereux connu. Les experts de Kaspersky Lab ne conseillent pas de travailler avec tels objets.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient un segment modifié de code d'un programme dangereux connu ou objet dont le comportement évoque un tel programme.

P**PHISHING**

Type d'escroquerie sur Internet dont l'objectif est d'obtenir un accès aux données privées de l'utilisateur.

PROTECTION

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

Q**QUARANTAINE**

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression. L'application de Kaspersky Lab place également en quarantaine les objets potentiellement infectés détectés. Les objets en quarantaine sont enregistrés sous forme cryptée pour éviter leur action sur l'ordinateur.

R**RESTAURATION**

Déplacement d'un objet original depuis le dossier de quarantaine vers l'emplacement où il était avant sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

REPARATION D'OBJETS

Le mode de traitement des objets infectés qui débouche sur la restauration complète ou partielle des données. Il n'est pas possible de réparer tous les objets infectés.

KASPERSKY LAB

Kaspersky Lab est un éditeur de renommée mondiale spécialisé dans les systèmes de protection contre les menaces informatiques : virus et autres programmes malveillants, courrier indésirable, attaques de réseau et attaques de pirates.

En 2008, Kaspersky Lab a fait son entrée dans le Top 4 des leaders mondiaux du marché des solutions de sécurité informatique pour les utilisateurs finaux (classement « IDC Worldwide Endpoint Security Revenue by Vendor »). Selon les résultats d'une étude réalisée par KomKon TGI-Russia 2009, Kaspersky Lab est l'éditeur de système de protection préféré des utilisateurs particuliers en Russie.

Kaspersky Lab a vu le jour en Russie en 1997. Aujourd'hui, Kaspersky Lab est devenu un groupe international de sociétés dont le siège principal est basé à Moscou. La société compte cinq filiales régionales qui gèrent les activités de la société en Russie, en Europe de l'Ouest et de l'Est, au Moyen Orient, en Afrique, en Amérique du Nord et du Sud, au Japon, en Chine et dans d'autres pays de la région Asie-Pacifique. La société emploie plus de 2 000 experts qualifiés.

PRODUITS. Les produits développés par Kaspersky Lab protègent aussi bien les ordinateurs des particuliers que les ordinateurs des réseaux d'entreprise.

La gamme de logiciels pour particuliers reprend des applications antivirus pour ordinateurs de bureau et ordinateurs portables, ainsi que des applications pour la protection des tablettes, des smartphones et autres appareils nomades.

La société propose des applications et des services pour la protection des postes de travail, des serveurs de fichiers et Internet, des passerelles de messagerie et des pare-feu. L'utilisation de ces solutions combinée à des outils d'administration centralisés permet de mettre en place et d'exploiter une protection efficace automatisée de l'organisation contre les menaces informatiques. Les logiciels de Kaspersky Lab ont obtenu les certificats des plus grands laboratoires d'essai. Ils sont compatibles avec les applications de nombreux éditeurs et sont optimisés pour de nombreuses plateformes matérielles.

Les experts de la lutte antivirus de Kaspersky Lab travaillent 24h/24. Chaque jour, ils trouvent des centaines de nouvelles menaces informatiques, développent les outils d'identification et de neutralisation de ces menaces et les ajoutent aux bases utilisées par les applications de Kaspersky Lab. *Les bases anti-virus de Kaspersky Lab sont actualisées toutes les heures, tandis que les bases antispam sont actualisées toutes les 5 minutes.*

TECHNOLOGIES. Kaspersky Lab est à l'origine de nombreuses technologies sans lesquelles il est impossible d'imaginer un logiciel antivirus moderne. Ce n'est donc pas un hasard si le moteur logiciel de Kaspersky Anti-Virus est intégré aux logiciels de plusieurs autres éditeurs : citons notamment SafeNet (É-U), Alt-N Technologies (É-U), Blue Coat Systems (É-U), Check Point Software Technologies (Israël), Clearswift (R-U), CommuniGate Systems (É-U), Critical Path (Irlande), D-Link (Taïwan), M86 Security (É-U), GFI (Malte), IBM (É-U), Juniper Networks (É-U), LANDesk (É-U), Microsoft (É-U), NETASQ (France), NETGEAR (É-U), Parallels (E-U), SonicWALL (USA), WatchGuard Technologies (É-U), ZYXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

REALISATIONS. Au cours de ces années de lutte contre les menaces informatiques, Kaspersky Lab a décroché des centaines de récompenses. Ainsi, en 2010, Kaspersky Anti-Virus a obtenu plusieurs hautes distinctions Advanced+ à l'issue de tests réalisés par le célèbre laboratoire antivirus autrichien AV-Comparatives. Mais la récompense la plus importante de Kaspersky Lab, c'est la fidélité de ses utilisateurs à travers le monde. Les produits et les technologies de la société protègent plus de 300 millions d'utilisateurs. Elle compte également plus de 200 000 entreprises parmi ses clients.

Site Web de Kaspersky Lab :

<http://www.kaspersky.com/fr>

Encyclopédie des virus :

<http://www.securelist.com>

Laboratoire d'étude des virus :

newvirus@kaspersky.com (uniquement pour l'envoi de fichiers potentiellement infectés sous forme d'archive)

Forum Internet de Kaspersky Lab :

<http://forum.kaspersky.com/index.php?showforum=129>

INFORMATIONS SUR LE CODE TIERS

Les informations relatives au code tiers sont reprises dans le fichier legal_notices.txt
file:///Library/Application%20Support/Kaspersky%20Lab/KAV/Doc/legal_notices.txt qui se trouve dans le dossier
d'installation de l'application.

NOTIFICATIONS SUR LES MARQUES DE COMMERCE

Les marques déposées et les marques de services appartiennent à leurs propriétaires respectifs.

Mac, Mac OS, OS X et Safari sont des marques déposées d'Apple Inc.

Google Chrome est une marque déposée de Google Inc.

Firefox est une marque déposée de Mozilla Foundation.

Myspace est une marque déposée de Myspace LLC.

INDEX

A

Abonnement.....	33, 34
Activation de l'application.....	34
version d'évaluation.....	34
l'aide du code d'activation	35
Analyse.....	42, 43

B

Banque électronique.....	45
Bases de l'application	44

C

Centre de protection	38, 40
Clé.....	28
Code d'activation	28
Configuration matérielle et logicielle	13
Contrat de licence.....	26
Contrôle Parental.....	22, 46, 47, 48

F

Fenêtre principale de l'application	20
---	----

K

Kaspersky Lab.....	63
--------------------	----

L

Lancement	
application	37
tâche de recherche de virus.....	42, 43
Lancement de la tâche de mise à jour	44
Le clavier virtuel	45
Licence	26
achat	32, 43
information.....	32
renouveler.....	33, 44

M

Mise à jour de l'application	44
My Kaspersky.....	16

N

Notifications.....	23, 50
--------------------	--------

P

Protection.....	39, 40
-----------------	--------

Q

Quarantaine	50
-------------------	----

R

Rapports	50
Restauration de l'objet	50