

Kaspersky Internet Security

**KASPERSKY** **lab**

**Manuel de l'utilisateur**

VERSION DE L'APPLICATION : 14.0

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que ce document vous aidera dans votre travail et répondra à la plupart des problèmes émergents.

Attention ! Ce document demeure la propriété de Kaspersky Lab ZAO (ci-après, 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, intégrale ou partielle, est passible de poursuites civiles, administratives ou judiciaires, conformément aux lois applicables.

La copie sous un format quelconque et la diffusion, y compris la traduction, de n'importe quel document ne sont admises que par 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 avertissement préalable. La version la plus récente de ce document est accessible sur le site de Kaspersky Lab à l'adresse <http://www.kaspersky.com/fr/docs>.

Kaspersky Lab ne peut être tenu 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. Kaspersky Lab n'assume pas non plus de responsabilité en cas de dommages liés à l'utilisation de ces textes.

Ce document fait référence aux autres noms et aux marques déposés qui appartiennent à leurs propriétaires respectifs.

Date d'édition : 03/06/2013

© 2013 Kaspersky Lab ZAO. Tous droits réservés.

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

# TABLE DES MATIERES

PRESENTATION DU GUIDE .....	6
Dans ce document.....	6
Conventions.....	7
SOURCES D'INFORMATIONS SUR L'APPLICATION .....	9
Sources d'informations pour les recherches indépendantes .....	9
Discussion sur les logiciels de Kaspersky Lab dans le forum.....	10
Contacter le service vente .....	10
Contacter le service de localisation et de rédaction de la documentation technique .....	10
KASPERSKY INTERNET SECURITY.....	11
Nouveautés .....	11
Distribution.....	12
Fonctions principales de l'application .....	12
Service pour les utilisateurs.....	14
Configurations logicielles et matérielles.....	14
INSTALLATION ET SUPPRESSION DE L'APPLICATION .....	16
Procédure standard de l'installation.....	16
Etape 1. Recherche d'une version plus récente de l'application .....	17
Etape 2. Début d'installation de l'application .....	17
Etape 3. Consultation du contrat de licence.....	17
Etape 4. Disposition sur Kaspersky Security Network .....	17
Etape 5. Installation .....	18
Etape 6. Fin de l'installation .....	18
Etape 7. Activation de l'application.....	18
Etape 8. Enregistrement de l'utilisateur.....	19
Etape 9. Fin de l'activation .....	19
Mise à jour d'une version antérieure de l'application .....	19
Etape 1. Recherche d'une version plus récente de l'application .....	20
Etape 2. Début d'installation de l'application .....	21
Etape 3. Consultation du contrat de licence.....	21
Etape 4. Disposition sur Kaspersky Security Network .....	21
Etape 5. Installation .....	21
Etape 6. Fin de l'installation .....	22
Suppression de l'application .....	22
Etape 1. Saisie du mot de passe pour supprimer l'application.....	23
Etape 2. Enregistrement de données pour une réutilisation .....	23
Etape 3. Confirmation de la suppression de l'application.....	24
Etape 4. Suppression de l'application. Fin de la suppression .....	24
LICENCE DE L'APPLICATION .....	25
A propos du contrat de licence .....	25
A propos de la licence .....	25
A propos du code d'activation.....	26
A propos de l'abonnement.....	26
A propos des données.....	27

RESOLUTION DES PROBLEMES TYPES.....	29
Activation de l'application .....	30
Achat d'une licence et renouvellement de sa durée de validité .....	31
Traitement des notifications de l'application .....	31
Analyse de l'état de protection de l'ordinateur et suppression des problèmes de sécurité .....	32
Mise à jour des bases et des modules de l'application .....	33
Analyse complète de l'ordinateur sur la présence de virus.....	34
Analyse du fichier, du dossier, du disque ou d'un autre objet sur la présence de virus .....	34
Analyse de l'ordinateur pour la présence de vulnérabilités.....	36
Analyse des zones importantes de l'ordinateur pour la présence de virus .....	36
Analyse des objets potentiellement infectés .....	36
Restauration de l'objet supprimé ou réparé par l'application .....	37
Restauration du système d'exploitation après l'infection .....	38
Configuration de l'Antivirus Courrier .....	40
Blocage du courrier indésirable (spam).....	40
Traitement des applications inconnues .....	41
Vérification de la réputation des applications .....	41
Contrôle des actions de l'application sur l'ordinateur et dans le réseau.....	42
Utilisation du mode des Applications sécurisées .....	44
Protection des données personnelles contre le vol .....	46
Clavier virtuel .....	47
Protection de saisie des données depuis le clavier.....	50
Configuration de la Protection bancaire .....	51
Suppression des traces d'activité.....	52
Vérification de la sécurité du site Internet.....	54
Utilisation du Contrôle Parental .....	55
Contrôle d'utilisation de l'ordinateur .....	56
Contrôle d'utilisation d'Internet.....	57
Contrôle du lancement des jeux et des applications .....	59
Contrôle des communications via les réseaux sociaux.....	60
Contrôle du contenu de la correspondance .....	61
Consultation du rapport sur les actions de l'utilisateur .....	62
Utilisation du Mode Jeux pour travailler en mode plein écran.....	63
Création et utilisation du disque de dépannage.....	63
Création d'un disque de dépannage .....	63
Démarrage de l'ordinateur à l'aide du disque de dépannage.....	65
Protection de l'accès aux paramètres de Kaspersky Internet Security à l'aide du mot de passe.....	66
Suspension et restauration de la protection de l'ordinateur .....	67
Restauration des paramètres standards du fonctionnement de l'application.....	67
Consultation du rapport sur l'utilisation de l'application .....	70
Utilisation de Kaspersky Gadget.....	70
Participation au Kaspersky Security Network (KSN) .....	71
Activation et désactivation de la participation à Kaspersky Security Network.....	72
Vérification de la connexion à Kaspersky Security Network .....	72
Participation au programme "Protège ton ami".....	73
Entrée dans votre profil dans le programme "Protège ton ami" .....	74
Comment partager le lien sur Kaspersky Internet Security avec les amis .....	75
Echange des points sur le code d'activation offert .....	76

CONTACTER LE SUPPORT TECHNIQUE .....	78
Modes d'obtention du Support Technique .....	78
Support Technique par téléphone .....	78
Obtention du Support Technique via Mon Espace Personnel .....	78
Utilisation du fichier de traçage et du script AVZ .....	79
Création d'un rapport sur l'état du système .....	80
Envoi des fichiers de données .....	80
Exécution du script AVZ.....	81
GLOSSAIRE .....	83
KASPERSKY LAB.....	89
INFORMATIONS SUR LE CODE TIERS .....	90
NOTICE SUR LES MARQUES DE COMMERCE .....	90
INDEX .....	91

# PRESENTATION DU GUIDE

Ce document est le manuel de l'utilisateur de Kaspersky Internet Security.

Pour une utilisation réussie de l'application, la possession des connaissances de base sur l'utilisation de l'ordinateur est requise : connaissance de l'interface du système d'exploitation utilisé, maîtrise des principales tâches, maîtrise du courrier électronique et d'Internet.

Ce guide poursuit les objectifs suivants :

- Aider à installer Kaspersky Internet Security, activer et utiliser l'application.
- Offrir un accès rapide aux informations pour répondre aux questions liées à l'application.
- Présenter les sources complémentaires d'informations sur l'application et les modes d'obtention du Support Technique.

## DANS CETTE SECTION

---

Dans ce document .....	<a href="#">6</a>
Conventions .....	<a href="#">7</a>

## DANS CE DOCUMENT

Ce document contient les sections suivantes.

### Sources d'informations sur l'application

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de l'application.

### Kaspersky Internet Security

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

### Installation et suppression de l'application

Cette section explique, étape par étape, comment installer et désinstaller l'application.

### 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 la durée de validité de la licence.

### Résolution des problèmes types

Cette section explique, étape par étape, comment exécuter les principales tâches que l'utilisateur peut accomplir à l'aide de l'application.

## Contacteur le Support Technique

Cette section contient des informations sur les méthodes de contact du Support Technique de Kaspersky Lab.

## Glossaire

Cette section contient une liste des termes qui apparaissent dans ce document et leur définition.

## Kaspersky Lab

Cette section contient des informations sur Kaspersky Lab ZAO.

## Informations sur le code tiers

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

## Notice sur les marques de commerce

Cette section cite les marques commerciales d'autres propriétaires cités dans le document.

## Index

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

# CONVENTIONS

Le texte du document est suivi des éléments de sens sur lesquels nous attirons votre attention : avertissements, conseils, exemples.

Les conventions sont utilisées pour identifier les éléments de sens. Les conventions et les exemples de leur utilisation sont repris dans le tableau ci-dessous.

Tableau 1. Conventions

EXEMPLE DU TEXTE	DESCRIPTION DE LA CONVENTION
N'oubliez pas que...	Les avertissements apparaissent en rouge et sont encadrés. Les avertissements contiennent les informations sur les actions indésirables potentielles qui peuvent amener à la perte des informations ou à la perturbation du fonctionnement du matériel ou du système d'exploitation.
Il est conseillé d'utiliser...	Les remarques sont encadrées. Les remarques peuvent contenir des conseils utiles, des recommandations, des valeurs importantes de paramètres ou des cas particuliers importants dans le fonctionnement de l'application.
<b>Exemple :</b> ...	Les exemples sont présentés sur un fond jaune sous le titre "Exemple".

EXEMPLE DU TEXTE	DESCRIPTION DE LA CONVENTION
<p>La <i>mise à jour</i>, c'est ...</p> <p>L'événement <i>Bases dépassées</i> survient.</p>	<p>Les éléments de sens suivants sont en italique :</p> <ul style="list-style-type: none"> <li>• nouveaux termes ;</li> <li>• noms des états et des événements de l'application.</li> </ul>
<p>Appuyez sur la touche <b>ENTER</b>.</p> <p>Appuyez sur la combinaison des touches <b>ALT+F4</b>.</p>	<p>Les noms des touches du clavier sont en caractères mi-gras et en lettres majuscules.</p> <p>Deux noms de touche unis par le caractère "+" représentent une combinaison de touches. Il faut appuyer simultanément sur ces touches.</p>
<p>Cliquez sur le bouton <b>Activer</b>.</p>	<p>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.</p>
<p>➡ <i>Pour planifier une tâche, procédez comme suit :</i></p>	<p>Les phrases d'introduction des instructions sont en italique et ont l'icône "flèche".</p>
<p>Dans la ligne de commande, saisissez le texte help</p> <p>Les informations suivantes s'affichent :</p> <p>Indiquez la date au format JJ:MM:AA.</p>	<p>Les types suivants du texte apparaissent dans un style spécial :</p> <ul style="list-style-type: none"> <li>• texte de la ligne de commande ;</li> <li>• texte des messages affichés sur l'écran par l'application ;</li> <li>• données à saisir par l'utilisateur.</li> </ul>
<p>&lt;Nom d'utilisateur&gt;</p>	<p>Les variables sont écrites entre chevrons. La valeur correspondant à la variable remplace cette variable. Par ailleurs, les parenthèses angulaires sont omises.</p>

# SOURCES D'INFORMATIONS SUR L'APPLICATION

Cette section contient la description des sources d'informations sur l'application et les renseignements sur les sites Internet que vous pouvez consulter pour discuter du fonctionnement de 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 les recherches indépendantes .....	<a href="#">9</a>
Discussion sur les logiciels de Kaspersky Lab dans le forum .....	<a href="#">10</a>
Contacteur le service vente.....	<a href="#">10</a>
Contacteur le service de localisation et de rédaction de la documentation technique.....	<a href="#">10</a>

## SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser les sources suivantes pour rechercher les informations sur l'application :

- page du site de Kaspersky Lab ;
- page sur le site Internet du Support Technique (Base des connaissances) ;
- aide électronique ;
- la documentation.

Si vous ne parvenez pas à résoudre vous-même le problème, il est conseillé de contacter le Support Technique de Kaspersky Lab (cf. section "Assistance technique par téléphone" à la page [78](#)).

Une connexion Internet est requise pour utiliser les sources d'informations sur le site Internet de Kaspersky Lab.

### Page sur le site Internet de Kaspersky Lab

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

La page (<http://www.kaspersky.com/fr/internet-security>) fournit des informations générales sur l'application, ses possibilités et ses particularités.

La page contient le lien sur la boutique en ligne. Le lien permet d'acheter l'application ou de renouveler le droit d'utilisation de l'application.

### Page sur le site Internet du service du Support Technique (Base des connaissances)

La Base des connaissances est une section du site Internet du Support Technique contenant les recommandations pour travailler avec les applications de Kaspersky Lab. La Base de connaissance est composée des articles d'aide regroupés selon les thèmes.

La page de l'application dans la Base des connaissances (<http://support.kaspersky.com/fr/kis2014>) permet de trouver les articles qui proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application.

Les articles peuvent répondre à des questions en rapport non seulement avec Kaspersky Internet Security, mais également avec d'autres applications de Kaspersky Lab. De plus, ils peuvent fournir des informations sur le Support Technique en général.

## Aide électronique

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

L'aide contextuelle contient les informations sur chaque fenêtre de l'application : la liste et la description des paramètres et la liste des tâches à effectuer.

L'aide complète contient les détails sur la gestion de la protection, la configuration des paramètres de l'application et l'exécution des tâches principales pour l'utilisateur.

## Documentation

Le manuel de l'utilisateur contient les informations sur l'installation, sur l'activation, sur la configuration des paramètres, ainsi que les informations pour travailler avec l'application. Le document décrit l'interface graphique et décrit l'exécution des tâches les plus fréquentes dans l'utilisation de l'application.

# DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM

Si votre question n'est pas urgente, vous pouvez la soumettre aux experts de Kaspersky Lab et aux autres utilisateurs de nos applications dans notre forum (<http://forum.kaspersky.com/index.php?showforum=105>).

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

## CONTACTER LE SERVICE VENTE

Si vous avez des questions sur la sélection, sur l'achat ou sur la prolongation de la durée d'utilisation de l'application, vous pouvez contacter nos experts du service vente à l'aide d'un des moyens suivants :

- En appelant notre service clientèle Français (détails sur <http://www.kaspersky.com/fr/about/contactinfo>).
- En envoyant un message avec votre question à l'adresse électronique [sales@kaspersky.com](mailto:sales@kaspersky.com).

La réponse sera formalisée en Français ou en anglais suivant votre demande.

## CONTACTER LE SERVICE DE LOCALISATION ET DE REDACTION DE LA DOCUMENTATION TECHNIQUE

Pour contacter le Groupe de rédaction de la documentation, vous pouvez envoyer un message par courrier électronique [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com). En tant que sujet du message, il faut indiquer "Kaspersky Help Feedback: Kaspersky Internet Security".

# KASPERSKY INTERNET SECURITY

Cette section décrit les possibilités de l'application et offre une brève description des fonctionnalités et des modules. Vous y découvrirez le contenu de la distribution et les services offerts aux utilisateurs enregistrés. La section fournit des informations sur la configuration matérielle et logicielle requise pour l'installation de l'application.

## DANS CETTE SECTION

---

Nouveautés .....	<a href="#">11</a>
Distribution .....	<a href="#">12</a>
Fonctionnalités principales de l'application .....	<a href="#">12</a>
Service pour les utilisateurs .....	<a href="#">14</a>
Configurations logicielle et matérielle .....	<a href="#">14</a>

## NOUVEAUTES

Les nouvelles possibilités suivantes sont présentes dans Kaspersky Internet Security :

- Pour augmenter la sécurité d'utilisation des applications, le mode des Applications sécurisées a été ajouté. Quand le mode des Applications sécurisées est activé, Kaspersky Internet Security détermine automatiquement les applications sûres et autorise le lancement des applications sécurisées uniquement.
- La fonctionnalité de la Protection bancaire a été améliorée : maintenant il est possible de sélectionner le navigateur Internet à ouvrir les sites des banques et des systèmes de paiement. La liste des sites Internet populaires est aussi complétée pour exécuter les opérations financières dans lesquels la Protection bancaire est activée automatiquement.
- La fonctionnalité du Contrôle Parental est améliorée : la possibilité de configuration flexible des autorisations pour lancer les jeux et les applications est ajoutée. Les modèles préinstallés des paramètres du Contrôle Parental qui correspondent à l'âge des utilisateurs contrôlés sont ajoutés.
- La configuration de Kaspersky Internet Security a été simplifiée. Maintenant, uniquement les paramètres de l'application utilisés plus souvent sont accessibles à la configuration.
- La prise en charge des dernières versions des navigateurs Internet populaires est ajoutée : maintenant les modules de protection (par exemple, le module d'analyse des liens, la Protection bancaire) prennent en charge les navigateurs Internet Mozilla™ FireFox™ (versions 16.x, 17.x, 18.x, 19.x), Internet Explorer® (versions 8, 9, 10), Google Chrome™ (versions 22.x, 23.x, 24.x, 25.x, 26.x).
- La fonction de protection contre les programmes malveillants de blocage de l'écran est ajoutée. Vous pouvez débloquer l'écran à l'aide de la combinaison de touches définie. La fonction de protection contre les programmes de blocage de l'écran détectera et neutralisera la menace.
- L'efficacité de protection contre le phishing est augmentée : la fonctionnalité du module Anti-Phishing a été améliorée et actualisée.
- La rapidité de l'application est augmentée et la consommation des ressources de l'ordinateur est optimisée.
- Le mode d'activité limitée lors de l'inaction de l'ordinateur est ajouté. Maintenant pendant l'inaction de l'ordinateur, Kaspersky Internet Security consomme moins de ressources ce qui amène à l'économie de la consommation d'énergie lors de l'utilisation de la batterie.

- Le temps de lancement de l'application est réduit considérablement.
- La rapidité de l'interface graphique de l'application est augmentée et le temps de réaction sur l'action de l'utilisateur est réduit.
- La présentation des rapports sur l'utilisation de l'application est améliorée. Maintenant, les rapports sont devenus plus simples et claires.
- La possibilité de participer au programme "Protège ton ami" a été ajoutée. Vous pouvez maintenant partager le lien sur Kaspersky Internet Security avec les amis et recevoir des codes d'activation offerts.

## 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 :

- pochette cachetée contenant le cédérom d'installation où sont enregistrés les fichiers de l'application et la documentation de l'application ;
- bref manuel de l'utilisateur contenant le code d'activation de l'application ;
- Contrat de licence reprenant les conditions d'utilisation de l'application.

Ces éléments peuvent varier en fonction du pays 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, y compris le code d'activation, vous seront envoyées par courrier électronique après le paiement.

Pour en savoir plus sur les modes d'achat et de distribution, contactez notre le Service Ventes [sales@kaspersky.com](mailto:sales@kaspersky.com).

## FONCTIONS PRINCIPALES DE L'APPLICATION

Kaspersky Internet Security protège votre ordinateur contre les menaces connues et nouvelles, les attaques réseau et les escroqueries, les messages non sollicités et d'autres données indésirables. Pour remplir les fonctions liées à la protection complète, Kaspersky Internet Security propose différents fonctions et modules de protection.

### Protection de l'ordinateur

Les *modules de la protection* ont été développés pour protéger les ordinateurs contre les menaces connues ou non, les attaques réseau, les escroqueries, les messages non sollicités et les informations indésirables. Chaque type de menace est pris en charge par un module particulier (cf. la description des modules ci-après). Les modules peuvent être activés, désactivés et configurés indépendamment les uns des autres.

En plus de la protection en temps réel réalisée par des modules de la protection, il est recommandé d'*analyser* périodiquement votre ordinateur pour détecter d'éventuels virus. Cette opération s'impose pour exclure la possibilité de propager des programmes malveillants qui n'auraient pas été détectés par les modules de la protection en raison, par exemple, d'un niveau de protection faible ou pour toute autre raison.

La *mise à jour* des bases et des modules de l'application utilisés dans le fonctionnement de l'application est requise pour que Kaspersky Internet Security garantisse l'actualité de la protection.

Certaines tâches spécifiques, qui requièrent l'exécution épisodique (par exemple, l'élimination des traces d'activité de l'utilisateur dans le système), sont exécutées à l'aide des *outils et Assistants complémentaires*.

Les modules suivants assurent la protection en temps réel de votre ordinateur.

Vous trouverez ci-après une description du fonctionnement des modules de protection selon le mode de fonctionnement de Kaspersky Internet Security recommandé par les experts de Kaspersky Lab (à savoir, selon les paramètres par défaut).

#### Antivirus Fichiers

L'Antivirus Fichiers permet d'éviter l'infection du système de fichiers de l'ordinateur. Le module est lancé au démarrage du système d'exploitation. Il se trouve en permanence dans la mémoire vive de l'ordinateur et il analyse tous les fichiers ouverts, enregistrés et exécutés sur l'ordinateur et sur tous les disques montés. Kaspersky Internet Security intercepte chaque requête adressée à un fichier et recherche la présence éventuelle de virus connus dans ce dernier. La suite de l'utilisation du fichier est possible uniquement si le fichier est sain ou s'il a pu être réparé par l'application. Si le fichier ne peut être réparé pour une raison quelconque, il sera supprimé. Avec cela, la copie du fichier sera placée en quarantaine.

#### Antivirus Courrier

L'Antivirus Courrier analyse le courrier entrant et sortant sur votre ordinateur. Tout message sera remis à son destinataire uniquement s'il ne contient aucun objet dangereux.

#### Antivirus Internet

L'Antivirus Internet intercepte et bloque l'exécution de scripts situés sur des sites Internet si ces scripts constituent une menace pour la sécurité de l'ordinateur. L'Antivirus Internet contrôle également tout le trafic Internet et bloque l'accès aux sites dangereux.

#### Antivirus IM ("Chat")

L'Antivirus IM ("Chat") garantit la sécurité de l'utilisation des messageries instantanées. Le module protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée. L'Antivirus IM ("Chat") vous protège pendant l'utilisation de nombreux clients de messagerie instantanée.

#### Contrôle des Applications

Le module Contrôle des Applications enregistre les actions réalisées par les applications dans le système et régleme l'activité des applications sur la base des groupes dans lesquels le module a placé cette application. Il existe un ensemble de règles défini pour chaque groupe. Ces règles définissent l'accès des applications à diverses ressources du système d'exploitation.

#### Pare-feu

Le Pare-feu vous protège pendant l'utilisation des réseaux locaux et d'Internet. Le module filtre toute activité réseau selon des règles de deux types : *règles pour les applications* et *règles pour les paquets*.

#### Surveillance du réseau

La Surveillance du réseau a été mise au point pour observer en temps réel l'activité réseau.

#### Prévention des intrusions

La Prévention des intrusions est lancée au démarrage du système d'exploitation et surveille l'activité du trafic entrant caractéristique des attaques réseau. Dès qu'il décèle une tentative d'attaque contre votre ordinateur, Kaspersky Internet Security bloque toute activité réseau de l'ordinateur qui vous attaque.

### Anti-Spam

L'Anti-Spam s'intègre au client de messagerie de votre ordinateur et recherche la présence éventuelle de messages non sollicités dans tout le courrier entrant. Tous les messages non sollicités reçoivent un en-tête spécial. Vous pouvez configurer les actions de l'Anti-Spam sur les messages non sollicités (par exemple, suppression automatique, placement dans un dossier spécial).

### Anti-phishing

L'Anti-Phishing permet de déterminer si une adresse Internet quelconque figure dans la liste des URL de phishing. Ce module est intégré à l'Antivirus Internet, à l'Anti-Spam et à l'Antivirus IM ("chat").

### Anti-bannière

L'Anti-bannière bloque les bannières qui apparaissent sur les sites Internet et dans l'interface des applications.

### Protection bancaire

La Protection bancaire assure la protection des données confidentielles lors de l'utilisation des services des banques en ligne et des systèmes de paiements et prévient aussi le vol des instruments de paiement lors des paiements en ligne.

### Contrôle Parental

Les fonctions du Contrôle Parental visent à protéger les enfants et les adolescents des menaces qu'ils pourraient croiser sur l'ordinateur et sur Internet.

Le Contrôle Parental permet de définir des restrictions souples de l'accès aux ressources Internet et aux applications en fonction de l'âge des utilisateurs. Outre cela, le Contrôle Parental permet de consulter des statistiques sur les actions des utilisateurs soumis aux contrôles.

## SERVICE POUR LES UTILISATEURS

Quand vous achetez une licence d'utilisation de l'application, vous pouvez obtenir les services suivants pendant la durée de validité de la licence :

- mise à jour des bases et nouvelles versions de l'application ;
- support par téléphone et par courrier électronique sur toutes les questions en rapport avec l'installation, la configuration et l'utilisation de l'application ;
- notification sur la sortie de nouvelles applications de Kaspersky Lab et sur l'émergence de nouveaux virus ou le déclenchement d'épidémies de virus. Pour bénéficier de ce service, vous devez être abonné à la diffusion d'informations de Kaspersky Lab ZAO sur le site Internet du Support Technique.

Aucun support ne sera apporté sur l'utilisation du système d'exploitation ou des logiciels tiers.

## CONFIGURATIONS LOGICIELLES ET MATERIELLES

Afin de garantir un fonctionnement de Kaspersky Internet Security, votre ordinateur doit répondre au minimum à la configuration suivante :

Recommandations d'ordre général :

- 480 Mo d'espace disponible sur le disque dur (dont 380 Mo pour le disque système).
- CD-/DVD-ROM (pour l'installation depuis un cédérom).

- Connexion à Internet (pour l'activation de l'application et la mise à jour des bases ou modules de l'application).
- Internet Explorer 8.0 ou suivant.
- Microsoft® Windows® Installer 3.0 ou suivantes.
- Microsoft .NET Framework 4.

Exigences pour les systèmes d'exploitation Microsoft Windows XP Home Edition (Service Pack 3 ou suivant), Microsoft Windows XP Professional (Service Pack 3 ou suivant), Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou suivant) :

- Processeur Intel® Pentium® 800 MHz 32 bits (x86)/64 bits (x64) ou supérieur (ou analogue compatible) ;
- 512 Mo de mémoire vive disponible.

Exigences pour les systèmes d'exploitation Microsoft Windows Vista® Home Basic (Service Pack 1 ou suivant), Microsoft Windows Vista Home Premium (Service Pack 1 ou suivant), Microsoft Windows Vista Business (Service Pack 1 ou suivant), Microsoft Windows Vista Enterprise (Service Pack 1 ou suivant), Microsoft Windows Vista Ultimate (Service Pack 1 ou suivant), Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate, Microsoft Windows 8, Microsoft Windows 8 Pro, Microsoft Windows 8 Enterprise :

- Processeur Intel Pentium 1 GHz 32 bits (x86)/ 64 bits (x64) ou supérieur (ou analogue compatible) ;
- 1 Go de mémoire vive disponible (pour les systèmes d'exploitation de 32 bits), 2 Go de mémoire vive disponible (pour les systèmes d'exploitation de 64 bits).

# INSTALLATION ET SUPPRESSION DE L'APPLICATION

Cette section explique, étape par étape, comment installer et désinstaller l'application.

## DANS CETTE SECTION

Procédure d'installation standard .....	<a href="#">16</a>
Mise à jour d'une version antérieure de l'application .....	<a href="#">19</a>
Suppression de l'application .....	<a href="#">22</a>

## PROCEDURE STANDARD DE L'INSTALLATION

L'installation de Kaspersky Internet Security s'opère en mode interactif à l'aide d'un Assistant d'installation.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour arrêter le fonctionnement de l'Assistant à toute étape d'installation, il faut fermer la fenêtre de l'Assistant.

Si l'application doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés est défini par les conditions du Contrat de licence), la procédure d'installation sera identique sur tous les ordinateurs.

➤ *Pour installer Kaspersky Internet Security sur votre ordinateur,*

exécutez le fichier d'installation (fichier avec extension exe) présent sur le CD-ROM de l'application.

Pour installer Kaspersky Internet Security, vous pouvez utiliser le distributif obtenu via Internet. Avec cela, l'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

## DANS CETTE SECTION

Etape 1. Recherche d'une version plus récente de l'application .....	<a href="#">17</a>
Etape 2. Début d'installation de l'application .....	<a href="#">17</a>
Etape 3. Consultation du contrat de licence .....	<a href="#">17</a>
Etape 4. Disposition sur Kaspersky Security Network.....	<a href="#">17</a>
Etape 5. Installation.....	<a href="#">18</a>
Etape 6. Fin de l'installation .....	<a href="#">18</a>
Etape 7. Activation de l'application.....	<a href="#">18</a>
Etape 8. Enregistrement de l'utilisateur.....	<a href="#">19</a>
Etape 9. Fin de l'activation .....	<a href="#">19</a>

## ETAPE 1. RECHERCHE D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation, l'Assistant d'installation vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si l'Assistant d'installation ne détecte pas, sur le serveur des mises à jour, une version plus récente de l'application, il lancera l'installation de la version actuelle.

Si l'Assistant d'installation détecte, sur les serveurs des mises à jour, une version plus récente de Kaspersky Internet Security, il vous proposera de la télécharger et de l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application, afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur d'une manière plus efficace. Si vous refusez l'installation de la nouvelle version, l'Assistant lancera l'installation de la version actuelle de l'application. Si vous acceptez l'installation de la nouvelle version, l'Assistant d'installation copiera les fichiers du distributif sur votre ordinateur et lancera l'installation de la nouvelle version. Pour plus d'informations, concernant l'installation de la nouvelle version de l'application, veuillez lire la documentation correspondante.

## ETAPE 2. DEBUT D'INSTALLATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'installer l'application.

Afin de poursuivre l'installation, cliquez sur **Installer**.

Selon le type d'installation et la langue de localisation, à cette étape l'Assistant d'installation vous propose de prendre connaissance du Contrat de licence conclu entre vous et Kaspersky Lab et vous propose également de participer au programme Kaspersky Security Network.

## ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation s'affiche pour certaines langues de localisation lors de l'installation de Kaspersky Internet Security depuis le distributif obtenu par Internet.

Au cours de cette étape, vous devez prendre connaissance du Contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le Contrat et si vous en acceptez toutes les dispositions, cliquez sur **Accepter**. L'installation de l'application se poursuivra.

Si le Contrat de licence n'est pas accepté, l'installation de l'application n'est pas réalisée.

## ETAPE 4. DISPOSITION SUR KASPERSKY SECURITY NETWORK

Cette étape de l'Assistant d'installation vous propose de participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez la Disposition relative à Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cliquez sur le bouton **Accepter** dans la fenêtre de l'Assistant.

Si vous ne voulez pas participer à Kaspersky Security Network, cliquez sur le bouton **Refuser**.

Après avoir accepté ou refusé la participation à Kaspersky Security Network, l'installation de l'application se poursuivra.

## ÉTAPE 5. INSTALLATION

Pour certaines versions de Kaspersky Internet Security, diffusées selon l'abonnement, il faut saisir le mot de passe offert par le service client avant l'installation.

Après la saisie du mot de passe, l'installation de l'application commence.

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

Une fois l'installation terminée, l'Assistant passe automatiquement à l'étape suivante.

Pendant l'installation, Kaspersky Internet Security réalise une suite de vérifications. Suite à ces analyses, les problèmes suivants peuvent être détectés :

- **Non-conformité du système d'exploitation aux exigences logicielles.** Pendant l'installation, l'Assistant analyse le respect des conditions suivantes :
  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) aux exigences logicielles ;
  - présence des programmes nécessaires ;
  - présence d'espace libre sur le disque, nécessaire à l'installation.

Si une des conditions énumérées n'est pas remplie, une notification apparaîtra.

- **Présence des programmes incompatibles sur l'ordinateur.** Si des applications incompatibles sont détectées, une liste s'affichera à l'écran et vous pourrez les supprimer. Les applications que Kaspersky Internet Security ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système sera requis. Ensuite, l'installation de Kaspersky Internet Security se poursuivra automatiquement.
- **Présence d'applications malveillantes sur l'ordinateur.** Lors de la détection d'applications malveillantes sur l'ordinateur, qui empêchent l'installation des applications antivirus, l'Assistant d'installation proposera de télécharger un outil spécial pour éliminer l'infection – l'*utilitaire Kaspersky Virus Removal Tool*.

Si vous acceptez l'installation de l'utilitaire, l'Assistant le téléchargera depuis les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, il vous proposera de le télécharger vous-même en cliquant sur le lien proposé.

## ÉTAPE 6. FIN DE L'INSTALLATION

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application. Pour commencer à utiliser Kaspersky Internet Security immédiatement, assurez-vous que la case **Lancer Kaspersky Internet Security 2012** est cochée, puis cliquez sur le bouton **Terminer**.

Si avant la fin de l'Assistant vous avez décoché la case **Lancer Kaspersky Internet Security**, l'application devra être lancée manuellement.

Dans certains cas, le redémarrage du système d'exploitation peut être requis pour terminer l'installation.

## ÉTAPE 7. ACTIVATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'activer l'application.

L'*activation* est une procédure d'activation de la version complète pour une durée de validité définie.

Si vous avez acheté une licence pour utiliser Kaspersky Internet Security et vous avez téléchargé l'application via boutique en ligne, l'activation de l'application peut être exécutée automatiquement pendant l'installation.

Vous pouvez choisir parmi les options suivantes pour activer Kaspersky Internet Security :

- **Activer l'application.** Sélectionnez cette option et saisissez le code d'activation si vous avez acheté une licence sur l'utilisation de l'application.

Si vous saisissez le code d'activation de Kaspersky Anti-Virus, la procédure de permutation sur Kaspersky Anti-Virus sera lancée à la fin de l'activation.

- **Activer la version d'évaluation de l'application.** Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter une licence. Vous allez pouvoir utiliser l'application en mode de pleine fonctionnalité pendant la durée de validité limitée par les conditions d'utilisation d'évaluation. Après la date d'expiration de la licence, vous ne pourrez plus activer la version d'évaluation.

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

## ETAPE 8. ENREGISTREMENT DE L'UTILISATEUR

Cette étape n'est pas disponible dans toutes les versions de Kaspersky Internet Security.

Les utilisateurs enregistrés obtiennent la possibilité d'envoyer des requêtes au Service du Support technique et au Laboratoire d'étude des virus via Mon Espace Personnel sur le site Internet de Kaspersky Lab, la possibilité d'administrer aisément les codes d'activation, ainsi que les informations opératoires sur les nouveaux produits et les offres spéciales.

Si vous acceptez de vous enregistrer, saisissez les données requises dans les champs correspondants pour envoyer vos données d'enregistrement à Kaspersky Lab, puis cliquez sur le bouton **Suivant**.

Dans certains cas, l'enregistrement de l'utilisateur est nécessaire pour utiliser l'application.

## ETAPE 9. FIN DE L'ACTIVATION

L'Assistant vous signale la réussite de l'activation de Kaspersky Internet Security. Outre cela, la fenêtre reprend les informations sur la licence valide : fin de validité de la licence et nombre d'ordinateurs couverts par cette licence.

En cas d'abonnement, les informations sur l'état de l'abonnement sont fournies à la place de la date d'expiration de la durée de validité de la licence.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

## MISE A JOUR D'UNE VERSION ANTERIEURE DE L'APPLICATION

### Installation de la nouvelle version de Kaspersky Internet Security par-dessus de la version précédente de Kaspersky Internet Security

Si votre ordinateur possède déjà Kaspersky Internet Security d'une des versions précédentes, vous pouvez l'actualiser jusqu'à la nouvelle version de Kaspersky Internet Security. Lors de la présence de la licence active sur l'utilisation de Kaspersky Internet Security des versions précédentes, vous devrez activer l'application : l'Assistant d'installation reçoit automatiquement les informations sur la licence sur l'utilisation de la version précédente de Kaspersky Internet Security et l'appliquera pendant l'installation de la nouvelle version de Kaspersky Internet Security.

## Installation de la nouvelle version de Kaspersky Internet Security par-dessus de la version précédente de Kaspersky Anti-Virus

Si vous installez la nouvelle version de Kaspersky Internet Security sur un ordinateur déjà équipé de Kaspersky Anti-Virus d'une des versions précédentes avec la licence valide, l'Assistant d'activation vous proposera de sélectionner l'option des actions suivantes :

- Poursuivre l'utilisation de Kaspersky Anti-Virus sous la licence valide. Dans ce cas, l'Assistant de mutation sera lancé à l'issue duquel la nouvelle version de Kaspersky Anti-Virus sera installé sur votre ordinateur. Vous pouvez utiliser Kaspersky Anti-Virus pendant la durée de validité de la licence sur l'utilisation de Kaspersky Anti-Virus de la version précédente.
- Poursuivre l'installation de la nouvelle version de Kaspersky Internet Security. Dans ce cas, l'application sera installée et activée conformément au scénario standard.

L'installation de Kaspersky Internet Security s'opère en mode interactif à l'aide d'un Assistant d'installation.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour arrêter le fonctionnement de l'Assistant à toute étape d'installation, il faut fermer la fenêtre de l'Assistant.

Si l'application doit protéger plus d'un ordinateur (le nombre maximal d'ordinateurs protégés est défini par les conditions du Contrat de licence), la procédure d'installation sera identique sur tous les ordinateurs.

➡ *Pour installer Kaspersky Internet Security sur votre ordinateur,*

exécutez le fichier d'installation (fichier avec extension exe) présent sur le CD-ROM de l'application.

Pour installer Kaspersky Internet Security, vous pouvez utiliser le distributif obtenu via Internet. Avec cela, l'Assistant d'installation affiche quelques étapes complémentaires d'installation pour certaines langues de localisation.

### DANS CETTE SECTION

Etape 1. Recherche d'une version plus récente de l'application .....	<a href="#">20</a>
Etape 2. Début d'installation de l'application .....	<a href="#">21</a>
Etape 3. Consultation du contrat de licence .....	<a href="#">21</a>
Etape 4. Disposition sur Kaspersky Security Network.....	<a href="#">21</a>
Etape 5. Installation.....	<a href="#">21</a>
Etape 6. Fin de l'installation .....	<a href="#">22</a>

## ETAPE 1. RECHERCHE D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation, l'Assistant d'installation vérifie la présence d'une version de l'application plus récente sur les serveurs de mises à jour de Kaspersky Lab.

Si l'Assistant d'installation ne détecte pas, sur le serveur des mises à jour, une version plus récente de l'application, il lancera l'installation de la version actuelle.

Si l'Assistant d'installation détecte, sur les serveurs des mises à jour, une version plus récente de Kaspersky Internet Security, il vous proposera de la télécharger et de l'installer sur votre ordinateur. Il est conseillé d'installer une nouvelle version de l'application, afin de bénéficier des nouvelles améliorations. Ces améliorations permettent de protéger votre ordinateur d'une manière plus efficace. Si vous refusez l'installation de la nouvelle version, l'Assistant lancera l'installation de la version actuelle de l'application. Si vous acceptez l'installation de la nouvelle version, l'Assistant d'installation copiera les fichiers du distributif sur votre ordinateur et lancera l'installation de la nouvelle version. Pour plus d'informations, concernant l'installation de la nouvelle version de l'application, veuillez lire la documentation correspondante.

## ETAPE 2. DEBUT D'INSTALLATION DE L'APPLICATION

A cette étape, l'Assistant d'installation vous propose d'installer l'application.

Afin de poursuivre l'installation, cliquez sur **Installer**.

Selon le type d'installation et la langue de localisation, à cette étape l'Assistant d'installation vous propose de prendre connaissance du Contrat de licence conclu entre vous et Kaspersky Lab et vous propose également de participer au programme Kaspersky Security Network.

## ETAPE 3. CONSULTATION DU CONTRAT DE LICENCE

Cette étape de l'Assistant d'installation s'affiche pour certaines langues de localisation lors de l'installation de Kaspersky Internet Security depuis le distributif obtenu par Internet.

Au cours de cette étape, vous devez prendre connaissance du Contrat de licence conclu entre vous et Kaspersky Lab.

Lisez attentivement le Contrat et si vous en acceptez toutes les dispositions, cliquez sur **Accepter**. L'installation de l'application se poursuivra.

Si le Contrat de licence n'est pas accepté, l'installation de l'application n'est pas réalisée.

## ETAPE 4. DISPOSITION SUR KASPERSKY SECURITY NETWORK

Cette étape de l'Assistant d'installation vous propose de participer au programme Kaspersky Security Network. La participation au programme implique l'envoi à Kaspersky Lab, Ltd. d'informations sur les nouvelles menaces découvertes sur l'ordinateur, sur les applications exécutées, sur les applications signées et les informations relatives au système. Vos données personnelles ne sont ni recueillies, ni traitées, ni enregistrées.

Lisez la Disposition relative à Kaspersky Security Network. Si vous êtes d'accord avec tous les points, cliquez sur le bouton **Accepter** dans la fenêtre de l'Assistant.

Si vous ne voulez pas participer à Kaspersky Security Network, cliquez sur le bouton **Refuser**.

Après avoir accepté ou refusé la participation à Kaspersky Security Network, l'installation de l'application se poursuivra.

## ETAPE 5. INSTALLATION

Pour certaines versions de Kaspersky Internet Security, diffusées selon l'abonnement, il faut saisir le mot de passe offert par le service client avant l'installation.

Après la saisie du mot de passe, l'installation de l'application commence.

L'installation de l'application peut durer un certain temps. Attendez jusqu'à la fin avant de passer à l'étape suivante.

Une fois l'installation terminée, l'Assistant passe automatiquement à l'étape suivante.

Pendant l'installation, Kaspersky Internet Security réalise une suite de vérifications. Suite à ces analyses, les problèmes suivants peuvent être détectés :

- **Non-conformité du système d'exploitation aux exigences logicielles.** Pendant l'installation, l'Assistant analyse le respect des conditions suivantes :
  - correspondance du système d'exploitation et des paquets des mises à jour (Service Pack) aux exigences logicielles ;
  - présence des programmes nécessaires ;
  - présence d'espace libre sur le disque, nécessaire à l'installation.

Si une des conditions énumérées n'est pas remplie, une notification apparaîtra.

- **Présence des programmes incompatibles sur l'ordinateur.** Si des applications incompatibles sont détectées, une liste s'affichera à l'écran et vous pourrez les supprimer. Les applications que Kaspersky Internet Security ne peut supprimer automatiquement doivent être supprimées manuellement. Au cours de la suppression des applications incompatibles, le redémarrage du système sera requis. Ensuite, l'installation de Kaspersky Internet Security se poursuivra automatiquement.
- **Présence d'applications malveillantes sur l'ordinateur.** Lors de la détection d'applications malveillantes sur l'ordinateur, qui empêchent l'installation des applications antivirus, l'Assistant d'installation proposera de télécharger un outil spécial pour éliminer l'infection – l'*utilitaire Kaspersky Virus Removal Tool*.

Si vous acceptez l'installation de l'utilitaire, l'Assistant le téléchargera depuis les serveurs de Kaspersky Lab. Ensuite, l'installation de l'utilitaire sera lancée automatiquement. Si l'Assistant ne parvient pas à télécharger l'utilitaire, il vous proposera de le télécharger vous-même en cliquant sur le lien proposé.

## ETAPE 6. FIN DE L'INSTALLATION

Cette fenêtre de l'Assistant vous signale la fin de l'installation de l'application.

A l'issue de l'installation, il faut redémarrer le système d'exploitation.

Si la case **Lancer Kaspersky Internet Security** est cochée, l'application sera lancée automatiquement après le redémarrage.

Si avant la fin de l'Assistant vous avez décoché la case **Lancer Kaspersky Internet Security**, l'application devra être lancée manuellement.

## SUPPRESSION DE L'APPLICATION

Suite à la suppression de Kaspersky Internet Security, l'ordinateur et vos données personnelles ne seront plus protégés !

La suppression de Kaspersky Internet Security s'effectue à l'aide de l'Assistant d'installation.

➤ Pour lancer l'Assistant,

ouvrez le menu **Démarrer** et sélectionnez l'option **Toutes les applications** → **Kaspersky Internet Security** → **Supprimer Kaspersky Internet Security**.

**DANS CETTE SECTION**

Etape 1. Saisie du mot de passe pour supprimer l'application .....	<a href="#">23</a>
Etape 2. Enregistrement de données pour une réutilisation.....	<a href="#">23</a>
Etape 3. Confirmation de la suppression de l'application .....	<a href="#">24</a>
Etape 4. Suppression de l'application. Fin de la suppression .....	<a href="#">24</a>

## ETAPE 1. SAISIE DU MOT DE PASSE POUR SUPPRIMER L'APPLICATION

Pour supprimer Kaspersky Internet Security, il faut saisir le mot de passe d'accès aux paramètres de l'application. Si pour des raisons quelconques vous ne pouvez pas indiquer le mot de passe, la suppression de l'application ne sera pas possible.

Cette étape s'affiche uniquement si le mot de passe de suppression de l'application a été établi.

## ETAPE 2. ENREGISTREMENT DE DONNEES POUR UNE REUTILISATION

A cette étape vous pouvez indiquer les données de l'application que vous voulez enregistrer pour une utilisation ultérieure lors de la réinstallation de l'application (par exemple, lors de l'installation de la version plus récente).

Par défaut, l'application propose d'enregistrer les informations sur la licence.

➔ *Pour enregistrer les données en vue d'une utilisation ultérieure, cochez les cases en regard des données à enregistrer :*

- **Information de licence** : données permettant de ne pas activer ultérieurement l'application à installer, mais d'utiliser automatiquement la licence déjà valide, à condition qu'elle soit toujours valable au moment de l'installation.
- **Fichiers de quarantaine** : fichiers analysés par l'application et placés en quarantaine.

Lors de la suppression de Kaspersky Internet Security de l'ordinateur, les fichiers en quarantaine ne seront pas disponibles. Pour agir sur ces fichiers, il faut installer Kaspersky Internet Security.

- **Paramètres d'utilisation de l'application** : valeurs des paramètres de fonctionnement de l'application. Ces paramètres sont définis au cours de la configuration de l'application.

**Kaspersky Lab ne garantit pas la prise en charge des paramètres de la version antérieure de l'application. Une fois que vous avez installé une version plus récente de l'application, il est conseillé de vérifier si elle a été correctement configurée.**

Vous pouvez aussi exporter les paramètres de protection à l'aide d'une ligne de commande, en utilisant la commande :

```
avp.com EXPORT <nom_du_fichier>
```

- **Données iChecker** : fichiers contenant les informations sur les objets déjà soumis à l'analyse à l'aide de la technologie iChecker.
- **Bases de l'Anti-Spam** : bases contenant les modèles des messages non sollicités reçus et enregistrés.

## ETAPE 3. CONFIRMATION DE LA SUPPRESSION DE L'APPLICATION

Dans la mesure où la suppression de l'application met en danger la protection de l'ordinateur et de vos données personnelles, vous devez confirmer la suppression de l'application. Pour ce faire, cliquez sur le bouton **Supprimer**.

## ETAPE 4. SUPPRESSION DE L'APPLICATION. FIN DE LA SUPPRESSION

Cette étape de l'Assistant correspond à la suppression de l'application de l'ordinateur. Attendez la fin du processus de suppression.

Après la suppression de Kaspersky Internet Security, vous pouvez indiquer les causes de suppression de l'application sur le site Internet de Kaspersky Lab. Pour ce faire, il faut passer sur le site Internet de Kaspersky Lab à l'aide du bouton **Remplir le formulaire**.

La suppression requiert le redémarrage du système d'exploitation. Si vous décidez de reporter le redémarrage, la fin de la procédure de suppression sera reportée jusqu'au moment où le système d'exploitation sera redémarré ou quand l'ordinateur sera éteint et allumé de nouveau.

# 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 la durée de validité de la licence.

## DANS CETTE SECTION

A propos du contrat de licence.....	<a href="#">25</a>
A propos de la licence.....	<a href="#">25</a>
A propos du code d'activation.....	<a href="#">26</a>
A propos de l'abonnement.....	<a href="#">26</a>
A propos des données.....	<a href="#">27</a>

## A PROPOS DU CONTRAT DE LICENCE

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

**Veuillez lire attentivement les conditions du Contrat de licence avant d'utiliser l'application.**

Vous êtes réputé avoir accepté les conditions du Contrat de licence lorsque vous avez décidé d'installer l'application. Si vous n'êtes pas d'accord avec les termes du Contrat de licence, vous devez interrompre l'installation de l'application ou ne pas utiliser l'application.

## A PROPOS DE LA LICENCE

La *licence* est un droit d'utilisation de l'application, limité dans le temps et octroyé dans le cadre du Contrat de licence. La licence est associée à un code d'activation unique de votre copie de Kaspersky Internet Security.

La licence vous donne droit aux types de service suivants :

- Utilisation de l'application sur un ou plusieurs périphériques.

Le nombre d'appareils sur lequel vous pouvez utiliser l'application est défini par les termes du Contrat de licence.

- Contacter le Support Technique de Kaspersky Lab.
- Accès aux autres services offerts par Kaspersky Lab ou ses partenaires pendant la durée de validité de la licence (cf. section "Services pour les utilisateurs" à la page [14](#)).

Pour utiliser l'application, vous devez acheter une licence pour l'utilisation de l'application.

La licence présente une durée de validité limitée. A l'expiration de la durée de validité de la licence, l'application continue à fonctionner, mais en mode de fonctionnalité limitée (par exemple, la mise à jour et l'utilisation de Kaspersky Security Network ne sont pas disponibles). Vous pouvez toujours utiliser tous les modules de l'application et soumettre l'ordinateur à une analyse antivirus de toutes les autres applications présentant une menace, mais uniquement à l'aide des bases installées avant l'expiration de la licence. Pour pouvoir continuer à utiliser toutes les fonctionnalités de Kaspersky Internet Security, il faut renouveler la validité de la licence.

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

Avant d'acheter une licence, vous pouvez vous familiariser gratuitement à la version d'essai de Kaspersky Internet Security. La version d'évaluation de Kaspersky Internet Security exécute ses fonctions pendant une courte durée de présentation. Après la fin de la période de présentation, Kaspersky Internet Security met fin à l'exécution de ses fonctions. En fonction du mode d'acquisition de l'application, vous pouvez obtenir le code d'activation de l'une. Pour pouvoir continuer à utiliser l'application, il faut acheter une licence.

## A PROPOS DU CODE D'ACTIVATION

Le *code d'activation* est un code que vous obtenez après avoir acheté une licence pour 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'acquisition de l'application, vous pouvez obtenir le code d'activation de l'une des manières suivantes :

- Si vous avez acheté Kaspersky Internet Security en magasin, le code d'activation figure dans la documentation ou sur la boîte contenant le cédérom d'installation.
- Si vous avez acheté Kaspersky Internet Security en ligne, le code d'activation est envoyé par courriel à l'adresse électronique que vous avez indiquée lors de la commande.
- Si vous participez au programme "Protège ton ami" (cf. section "Participation au programme "Protège ton ami" à la page [73](#)), vous pouvez recevoir le code d'activation offert en échange des points.

Le décompte de la durée de validité de la licence débute à partir du jour où l'application a été activée. Si vous avez acheté une licence autorisant l'utilisation de Kaspersky Internet Security sur plusieurs appareils, le décompte de la durée de validité débute à partir du jour de la première utilisation du code d'activation.

En cas de perte ou de suppression accidentelle du code après l'activation de l'application, vous devez envoyer une demande au Support Technique de Kaspersky Lab à <http://www.kaspersky.com/fr/support> pour le récupérer.

## A PROPOS DE L'ABONNEMENT

L'*abonnement à Kaspersky Internet Security* est une commande pour l'utilisation de l'application avec les paramètres sélectionnés (date de fin, nombre de périphériques protégés). L'abonnement à Kaspersky Internet Security peut être commandé auprès du service client (par exemple, auprès du fournisseur d'accès). Vous pouvez suspendre ou reprendre l'abonnement, le renouveler en mode automatique et le refuser. Il est possible de gérer l'abonnement via votre espace personnel sur le site Internet du service client.

Les services clients peuvent offrir deux types d'abonnement sur l'utilisation de Kaspersky Internet Security : l'abonnement sur le renouvellement ou l'abonnement sur la mise à jour et la protection.

L'abonnement peut être limité (par exemple, pour un an) ou illimité (sans date d'expiration). Pour poursuivre l'utilisation de Kaspersky Internet Security après la fin de l'abonnement limitée, il faut le renouveler de façon indépendante. L'abonnement illimité est renouvelé automatiquement si le prépaiement au service client est effectué en temps et en heure.

Pour les abonnements à durée déterminée, il existe une période de grâce après l'expiration de l'abonnement au cours de laquelle l'utilisateur aura la possibilité de reconduire l'abonnement tout en continuant à bénéficier des fonctionnalités de l'application.

Si l'abonnement n'est pas reconduit à l'issue de cette période de grâce, Kaspersky Internet Security n'actualisera plus les bases de l'application (pour l'abonnement aux mises à jour) et il arrêtera également la protection de l'ordinateur et les tâches d'analyse (pour l'abonnement aux mises à jour et à la protection).

Pour utiliser Kaspersky Internet Security par abonnement, il faut appliquer le code d'activation offert par le service client. Dans certains cas, le code d'activation peut être téléchargé ou appliqué automatiquement. Si vous utilisez l'application par abonnement, vous ne pouvez pas utiliser un autre code d'activation pour prolonger la licence. Cela sera possible uniquement après l'expiration de l'abonnement.

Si au moment de l'enregistrement de l'abonnement, Kaspersky Internet Security est déjà utilisé avec une licence active, après l'enregistrement de l'abonnement, Kaspersky Internet Security sera utilisé selon ce dernier. Le code d'activation, à l'aide duquel l'application a été activée auparavant, peut être appliqué sur un autre ordinateur.

Pour résilier l'abonnement, il faut contacter le service client chez qui vous avez acheté Kaspersky Internet Security.

Les actions qui peuvent être réalisées vis-à-vis de l'abonnement dépendent du service client. De plus, il se peut qu'il n'existe pas de période de grâce au cours de laquelle le renouvellement de l'abonnement est toujours possible.

## A PROPOS DES DONNEES

Pour augmenter le niveau de protection opératoire, en acceptant les conditions du Contrat de licence, vous acceptez de présenter les informations suivantes en mode automatique à Kaspersky Lab :

- les informations sur les sommes de contrôle des fichiers traités (MD5) ;
- les informations pour définir la réputation des URL ;
- les statistiques d'utilisation des notifications de produit ;
- les données statistiques pour la protection contre le courrier indésirable ;
- les données sur l'activation et sur la version utilisée de Kaspersky Internet Security ;
- les informations sur les types des menaces détectées ;
- les informations sur les certificats numériques utilisés et les informations nécessaires pour vérifier leur authenticité ;
- les données relatives au fonctionnement de l'application et les informations relatives à la licence indispensables pour configurer l'affichage du contenu des sites de confiance.

Si l'ordinateur est équipé d'un module TPM (Trusted Platform Module), alors vous acceptez de présenter à Kaspersky Lab le rapport TPM sur le démarrage du système d'exploitation de l'ordinateur et les informations nécessaires pour vérifier l'authenticité du rapport. Lors de l'apparition d'une erreur d'installation de Kaspersky Internet Security, vous acceptez de présenter en mode automatique à Kaspersky Lab les informations sur le code de l'erreur, sur le distributeur utilisé et sur l'ordinateur.

Lors de la participation au programme Kaspersky Security Network (cf. section "Participation au Kaspersky Security Network (KSN)" à la page [71](#)), Kaspersky Lab reçoit automatiquement les informations suivantes, obtenues dans le cadre du fonctionnement de Kaspersky Internet Security sur l'ordinateur :

- les informations sur le logiciel et le matériel installé ;
- les informations sur l'état de la protection antivirus de l'ordinateur, ainsi que sur tous les objets potentiellement infectés et les décisions prises vis-à-vis de ces objets ;
- les informations sur les programmes téléchargés et lancés ;
- les informations relatives à la licence de la version installée de Kaspersky Internet Security ;
- les informations sur les erreurs et sur l'utilisation de l'interface utilisateur de Kaspersky Internet Security ;
- les informations relatives à l'application, y compris sa version, les informations relatives aux fichiers des modules chargés et à la version des bases de l'application utilisées ;

- les statistiques des mises à jour et des connexions avec les serveurs de Kaspersky Lab ;
- les informations relatives à l'utilisation de la connexion sans fil de l'ordinateur ;
- statistiques sur le temps consacré par les modules de l'application à l'analyse des objets ;
- statistiques sur les retards lors du lancement des applications installées liées à l'utilisation de Kaspersky Internet Security ;
- les fichiers qui pourraient être utilisés par des individus malintentionnés pour nuire à l'ordinateur ou à ses composants, dont les fichiers détectés après avoir cliqué sur un lien malveillant.

Les informations à transférer à Kaspersky Lab seront conservées 30 jours maximum à partir de leur création sur l'ordinateur. Cette conservation a lieu dans la sauvegarde interne protégée. Le volume maximal de données conservées s'élève à 30 Mo.

Ainsi, les fichiers (ou leurs composants) par rapport auxquels le risque de leur utilisation par des individus malintentionnés pour nuire à l'ordinateur ou aux données existants, peuvent être envoyés à Kaspersky Lab pour une analyse complémentaire.

Les informations obtenues sont protégées par Kaspersky Lab conformément aux exigences établies par la loi. Kaspersky Lab utilise les informations obtenues uniquement sous forme de statistiques. Les données générales des statistiques sont automatiquement formées à partir des informations d'origine obtenues et ne contiennent pas de données personnelles ou d'autres informations confidentielles. Les informations d'origine obtenues sont enregistrées sous forme cryptée et sont supprimées au gré de leur accumulation (deux fois par an). Les données des statistiques générales sont conservées de manière illimitée.

# RESOLUTION DES PROBLEMES TYPES

Cette section explique, étape par étape, comment exécuter les principales tâches que l'utilisateur peut accomplir à l'aide de l'application.

## DANS CETTE SECTION

---

Activation de l'application .....	<a href="#">30</a>
Achat d'une licence et renouvellement de sa durée de validité .....	<a href="#">31</a>
Traitement des notifications de l'application .....	<a href="#">31</a>
Analyse de l'état de protection de l'ordinateur et suppression des problèmes de sécurité.....	<a href="#">32</a>
Mise à jour des bases et des modules de l'application.....	<a href="#">33</a>
Analyse complète de l'ordinateur sur la présence de virus .....	<a href="#">34</a>
Analyse du fichier, du dossier, du disque ou d'un autre objet sur la présence de virus.....	<a href="#">34</a>
Analyse de l'ordinateur pour la présence des vulnérabilités.....	<a href="#">36</a>
Analyse des zones importantes de l'ordinateur pour la présence de virus.....	<a href="#">36</a>
Analyse des objets potentiellement infectés.....	<a href="#">36</a>
Restauration de l'objet supprimé ou réparé par l'application.....	<a href="#">37</a>
Restauration du système d'exploitation après l'infection .....	<a href="#">38</a>
Configuration de l'Antivirus Courrier .....	<a href="#">40</a>
Blocage du courrier indésirable (spam).....	<a href="#">40</a>
Traitement des applications inconnues .....	<a href="#">41</a>
Protection des données personnelles contre le vol .....	<a href="#">46</a>
Vérification de la sécurité d'un site Internet.....	<a href="#">54</a>
Utilisation du Contrôle Parental .....	<a href="#">55</a>
Utilisation du Mode Jeux pour travailler en mode plein écran .....	<a href="#">63</a>
Création et utilisation du disque de dépannage .....	<a href="#">63</a>
Protection de l'accès aux paramètres de Kaspersky Internet Security à l'aide du mot de passe .....	<a href="#">66</a>
Suspension et restauration de la protection de l'ordinateur.....	<a href="#">67</a>
Restauration des paramètres standards du fonctionnement de l'application .....	<a href="#">67</a>
Consultation du rapport sur l'utilisation de l'application .....	<a href="#">70</a>
Utilisation de Kaspersky Gadget .....	<a href="#">70</a>
Participation au Kaspersky Security Network (KSN) .....	<a href="#">71</a>
Participation au programme "Protège ton ami" .....	<a href="#">73</a>

## ACTIVATION DE L'APPLICATION

Pour pouvoir profiter des fonctions de l'application et des services complémentaires associés à celle-ci, il faut activer l'application (cf. section "A propos du code d'activation" à la page [26](#)).

Si vous n'avez pas activé l'application pendant l'installation, vous pouvez le faire plus tard. Les notifications de Kaspersky Internet Security dans la zone de notifications de la barre des tâches vous rappelleront qu'il faut activer l'application. L'activation de Kaspersky Internet Security s'effectue à l'aide de l'Assistant d'activation.

► Pour démarrer l'Assistant d'activation de Kaspersky Internet Security, exécutez l'une des actions suivantes :

- Passez au lien **Activer** dans la fenêtre de notification de Kaspersky Internet Security dans la zone de notifications de la barre des tâches.
- Passez au lien **Licence** situé dans la partie inférieure de la fenêtre principale de l'application. Dans la fenêtre **Licence** qui s'ouvre, cliquez sur le bouton **Activer l'application**.

Lorsque l'Assistant d'activation de l'application fonctionne, certains paramètres doivent être indiqués.

### Etape 1. Saisie du code d'activation

Saisissez le code d'activation dans le champ correspondant, puis cliquez sur **Activer**.

### Etape 2. Demande d'activation

Si la requête sur l'activation réussit, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Saisie des données d'enregistrement

Cette étape n'est pas disponible dans toutes les versions de Kaspersky Internet Security.

Les utilisateurs enregistrés possèdent les possibilités suivantes :

- envoyer les requêtes au Service du Support technique et au Laboratoire d'étude des virus via Mon Espace Personnel sur le site Internet de Kaspersky Lab ;
- gérer les codes d'activation ;
- recevoir les informations sur des nouveaux produits et sur les offres spéciales de Kaspersky Lab.

Saisissez vos données pour l'enregistrement, puis cliquez sur le bouton **Suivant**.

### Etape 4. Activation

Si l'activation de l'application a réussi, l'Assistant passe automatiquement à la fenêtre suivante.

### Etape 5. Fin de l'Assistant

La fenêtre de l'Assistant affiche les informations relatives aux résultats de l'activation.

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

## ACHAT D'UNE LICENCE ET RENOUELEMENT DE SA DUREE DE VALIDITE

Si vous avez installé Kaspersky Internet Security sans avoir acheté une licence par avance, vous pourrez acheter celle-ci après l'installation de l'application. A l'achat d'une licence, vous recevez le code d'activation requis pour activer l'application (cf. section "Activation de l'application" à la page [30](#)).

Quand la durée de validité d'une licence est sur le point d'expirer, vous pouvez la renouveler. Pour ce faire, vous pouvez ajouter un code d'activation de réserve à l'application avant l'expiration de la licence. A l'issue de la période de validité de la licence, Kaspersky Internet Security est activé automatiquement à l'aide du code d'activation de réserve.

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

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Saisissez le code d'activation/Licence**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Licence**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Acheter le code d'activation**.

La page de la boutique en ligne où vous pouvez acheter la licence s'ouvre.

➤ *Pour ajouter un code d'activation de réserve, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Saisissez le code d'activation/Licence**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Licence**.
3. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Activer l'application**.

La fenêtre de l'Assistant d'activation de l'application s'ouvre.

4. Saisissez le code d'activation dans les champs correspondants, puis cliquez sur **Activer**.

Kaspersky Internet Security envoie les données au serveur d'activation pour vérification. Si la vérification réussit, l'Assistant passe automatiquement à l'étape suivante.

5. A la fin de l'Assistant, cliquez sur **Terminer**.

## TRAITEMENT DES NOTIFICATIONS DE L'APPLICATION

Les notifications de l'application qui apparaissent dans la zone de notification de la barre des tâches signalent les événements survenus pendant l'utilisation de l'application et qui requièrent votre attention. En fonction de la gravité de l'événement, les notifications peuvent appartenir aux catégories suivantes :

- **Critiques** : signalent des événements d'une importance capitale pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet malveillant ou d'une activité dangereuse dans le système). Fenêtre des notifications et des messages contextuels critiques : en rouge.
- **Importants** : signalent des événements potentiellement importants pour assurer la protection de l'ordinateur (par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système). Fenêtre des notifications et des messages contextuels importants : en jaune.
- **Informatifs** : signalent des événements qui ne sont pas critiques pour assurer la protection de l'ordinateur. Fenêtre des notifications et des messages contextuels informatifs : en vert.

Quand un tel message apparaît, il faut sélectionner une des actions proposées dans la notification. La version optimale, à savoir celle recommandée par les experts de Kaspersky Lab, est choisie par défaut. La notification peut être fermée automatiquement lors du redémarrage de l'ordinateur, lors de la fermeture de Kaspersky Internet Security ou dans le mode Connected Standby dans Windows 8. Lors de la fermeture automatique de la notification, Kaspersky Internet Security exécutera l'action recommandée par défaut.

Les notifications n'apparaissent pas au cours de la première heure de fonctionnement de l'application si l'ordinateur a été achetée avec une version préinstallée de Kaspersky Internet Security (livraison OEM). L'application traite les objets détectés selon les actions recommandées. Les résultats du traitement sont consignés dans un rapport.

## **ANALYSE DE L'ETAT DE PROTECTION DE L'ORDINATEUR ET SUPPRESSION DES PROBLEMES DE SECURITE**

L'indicateur situé dans la partie gauche de la fenêtre principale de l'application (cf. ill. ci-après) signale les problèmes qui pourraient survenir dans la protection de l'ordinateur. La couleur de l'indicateur (représente l'image du moniteur) change en fonction de l'état de la protection de l'ordinateur : le vert indique que l'ordinateur est protégé, le jaune signale un problème dans la protection et le rouge indique une menace sérieuse pour la sécurité de l'ordinateur. Il est conseillé d'éliminer immédiatement les problèmes et les menaces sur la sécurité.



*Illustration 1. Indicateur d'état de la protection*

En cliquant sur l'indicateur dans la fenêtre principale de l'application, vous pouvez ouvrir la fenêtre **Problèmes de sécurité** (cf. ill. ci-après) qui affiche des informations détaillées sur l'état de la protection de l'ordinateur et qui propose diverses solutions pour supprimer les problèmes et les menaces.

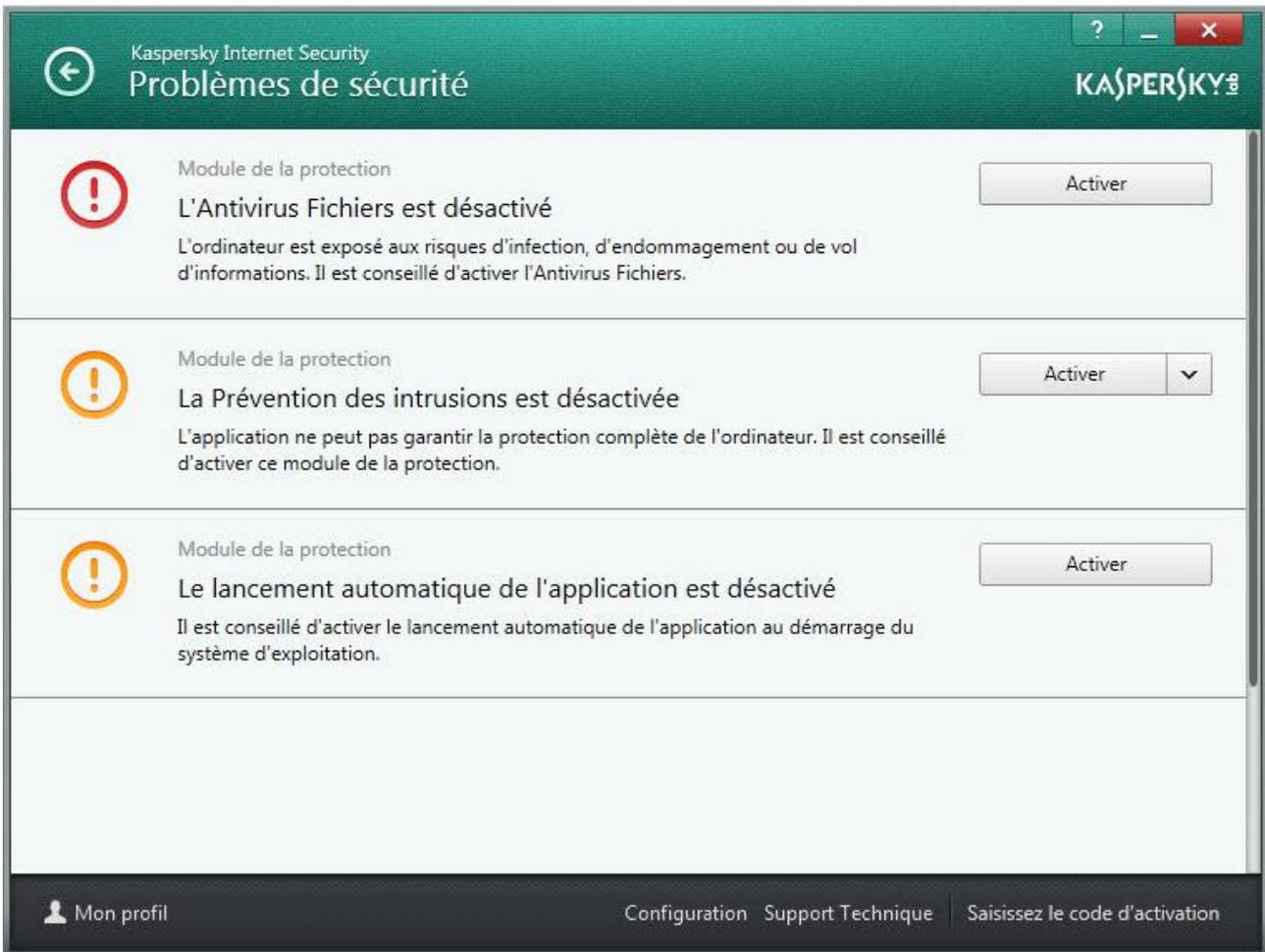


Illustration 2. Fenêtre **Problèmes de sécurité**

Les problèmes dans la protection sont regroupés selon les catégories auxquelles ils appartiennent. Des actions que vous pouvez exécuter sont proposées à titre de résolution de chaque problème.

## MISE A JOUR DES BASES ET DES MODULES DE L'APPLICATION

Kaspersky Internet Security vérifie automatiquement la présence des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Internet Security les télécharge et les installe en arrière-plan. Vous pouvez lancer la mise à jour de Kaspersky Internet Security à tout moment depuis la fenêtre principale de l'application ou depuis le menu contextuel de l'icône de l'application dans la zone des notifications de la barre des tâches.

Le téléchargement des mises à jour depuis les serveurs de Kaspersky Lab requiert une connexion Internet.

Lors du travail dans le système d'exploitation Microsoft Windows 8, le téléchargement des mises à jour ne se passe pas si la connexion à haut débit à Internet est utilisée et la restriction du trafic est configurée dans l'application avec ce type de connexion. Pour exécuter le téléchargement des mises à jour, il faut désactiver manuellement la restriction dans la sous-section **Réseau** de la fenêtre de configuration de l'application.

- *Pour lancer la mise à jour depuis le menu contextuel de l'icône de l'application dans la zone de notifications de la barre des tâches,*

choisissez l'option **Mise à jour** dans le menu contextuel de l'icône de l'application.

- *Pour lancer la mise à jour depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Mise à jour**.

La section **Mise à jour** apparaît.

2. Dans la section **Mise à jour**, cliquez sur le bouton **Mettre à jour**.

## ANALYSE COMPLETE DE L'ORDINATEUR SUR LA PRESENCE DE VIRUS

Pendant l'analyse complète, Kaspersky Internet Security analyse par défaut les objets suivants :

- mémoire système ;
- objets téléchargés au démarrage du système d'exploitation ;
- sauvegarde ;
- disques durs et amovibles.

Il est conseillé de réaliser une analyse complète directement après l'installation de Kaspersky Internet Security sur l'ordinateur.

- *Pour lancer l'analyse complète depuis la fenêtre principale de l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.

La section **Analyse** apparaît.

2. Sélectionnez la section **Analyse complète** dans la partie droite de la fenêtre.

La section **Analyse complète** apparaît.

3. Cliquez sur le bouton **Lancer l'analyse**.

Kaspersky Internet Security initialise l'analyse complète de l'ordinateur.

## ANALYSE DU FICHIER, DU DOSSIER, DU DISQUE OU D'UN AUTRE OBJET SUR LA PRESENCE DE VIRUS

Pour analyser un objet distinct, utilisez une des méthodes suivantes :

- au départ du menu contextuel de l'objet ;
- au départ de la fenêtre principale de l'application ;
- via le gadget Kaspersky Internet Security (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

➤ Pour lancer la recherche d'éventuels virus depuis le menu contextuel de l'objet, procédez comme suit :

1. Ouvrez la fenêtre de l'Assistant de Microsoft Windows et accédez au dossier contenant l'objet à analyser.
2. Ouvrez le menu contextuel de l'objet en cliquant avec le bouton droit de la souris (cf. ill. ci-après) et sélectionnez l'option **Rechercher d'éventuels virus**.

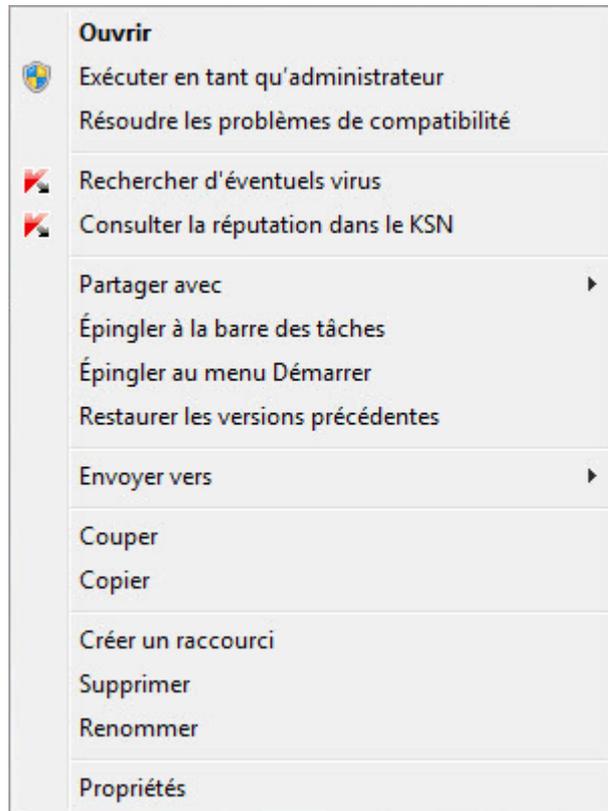


Illustration 3. Menu contextuel du fichier exécutable dans Microsoft Windows

➤ Pour lancer la recherche d'éventuels virus dans un objet depuis la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.
2. Passez à la section **Analyse personnalisée** dans la partie droite de la fenêtre.
3. Indiquez les objets à analyser d'une des méthodes suivantes :
  - Déplacez les objet dans la fenêtre **Analyse personnalisée** ;
  - Cliquez sur le bouton **Ajouter** et indiquez l'objet dans la fenêtre ouverte de la sélection du fichier ou du dossier.
4. Cliquez sur le bouton **Lancer l'analyse**.

La fenêtre **Gestionnaire des tâches** s'ouvre. Cette fenêtre affichera les informations sur le processus d'analyse.

➤ Pour rechercher la présence éventuelle de virus à l'aide du gadget,

déplacez l'objet sur le gadget.

## ANALYSE DE L'ORDINATEUR POUR LA PRESENCE DE VULNERABILITES

Une *vulnérabilité* est un endroit non protégé dans le code que des individus malintentionnés peuvent utiliser à leur fin, par exemple copier les données utilisées par l'application au code non protégé. La recherche de vulnérabilités sur votre ordinateur permet d'identifier les "points faibles" de la protection de votre ordinateur. Il est conseillé de supprimer les vulnérabilités découvertes.

► Pour lancer la recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton  et sélectionnez la section **Outils**.

La section **Outil** apparaît.

3. Dans le groupe **Recherche de vulnérabilités**, cliquez sur le bouton **Exécuter**.

Kaspersky Internet Security commence à rechercher la présence éventuelle de vulnérabilités sur votre ordinateur.

## ANALYSE DES ZONES IMPORTANTES DE L'ORDINATEUR POUR LA PRESENCE DE VIRUS

L'analyse rapide désigne l'analyse des objets suivants :

- objets chargés au démarrage du système d'exploitation ;
- mémoire système ;
- des secteurs d'amorçage du disque.

► Pour lancer l'analyse rapide depuis la fenêtre principale de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et dans la partie inférieure de la fenêtre, sélectionnez la section **Analyse**.

La section **Analyse** apparaît.

2. Ouvrez la section **Analyse rapide** dans la partie droite de la fenêtre.

La section **Analyse rapide** apparaît.

3. Cliquez sur le bouton **Lancer l'analyse**.

Kaspersky Internet Security lance l'analyse.

## ANALYSE DES OBJETS POTENTIELLEMENT INFECTES

Si vous pensez que l'objet est infecté par un virus, analysez-le à l'aide de Kaspersky Internet Security.

Si l'application, suite à l'analyse, signale que l'objet est sain, mais que vous pensez que ce n'est pas le cas, vous pouvez envoyer l'objet au *Laboratoire d'étude des virus*. Les experts du laboratoire d'étude des virus étudieront l'objet pour voir s'il est vraiment infecté par un virus et ajouteront sur le champ la description du nouveau virus aux bases qui seront chargées par l'application lors de la mise à jour.

➤ *Pour envoyer le fichier au laboratoire d'étude des virus, procédez comme suit :*

1. Ouvrez la page d'envoi de requêtes au Laboratoire d'étude des virus (<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>).
2. Suivez les instructions affichées sur la page pour envoyer votre demande.

## RESTAURATION DE L'OBJET SUPPRIME OU REPARE PAR L'APPLICATION

**Kaspersky Lab déconseille la restauration des fichiers supprimés ou réparés car ils peuvent constituer une menace pour votre ordinateur.**

La restauration d'un objet supprimé ou réparé s'opère sur la base de sa copie de sauvegarde créée par l'application lors de l'analyse.

Kaspersky Internet Security n'exécute pas de réparation des applications de la Boutique Windows. Si une telle application est considérée comme dangereuse à l'issue de l'analyse, elle sera supprimée de l'ordinateur.

Lors de la suppression des applications de la Boutique Windows, Kaspersky Internet Security ne crée pas de copies de sauvegarde. Pour restaurer de tels objets, il faut utiliser les outils de restauration du système d'exploitation (pour plus d'informations, veuillez consulter la documentation du système d'exploitation de votre ordinateur) ou actualiser les applications via Boutique Windows.

➤ *Pour restaurer un fichier supprimé ou réparé par l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Quarantaine**.

3. Dans la fenêtre ouverte **Quarantaine**, sélectionnez le fichier requis dans la liste et cliquez sur le bouton **Restaurer** (cf. ill. ci-après).

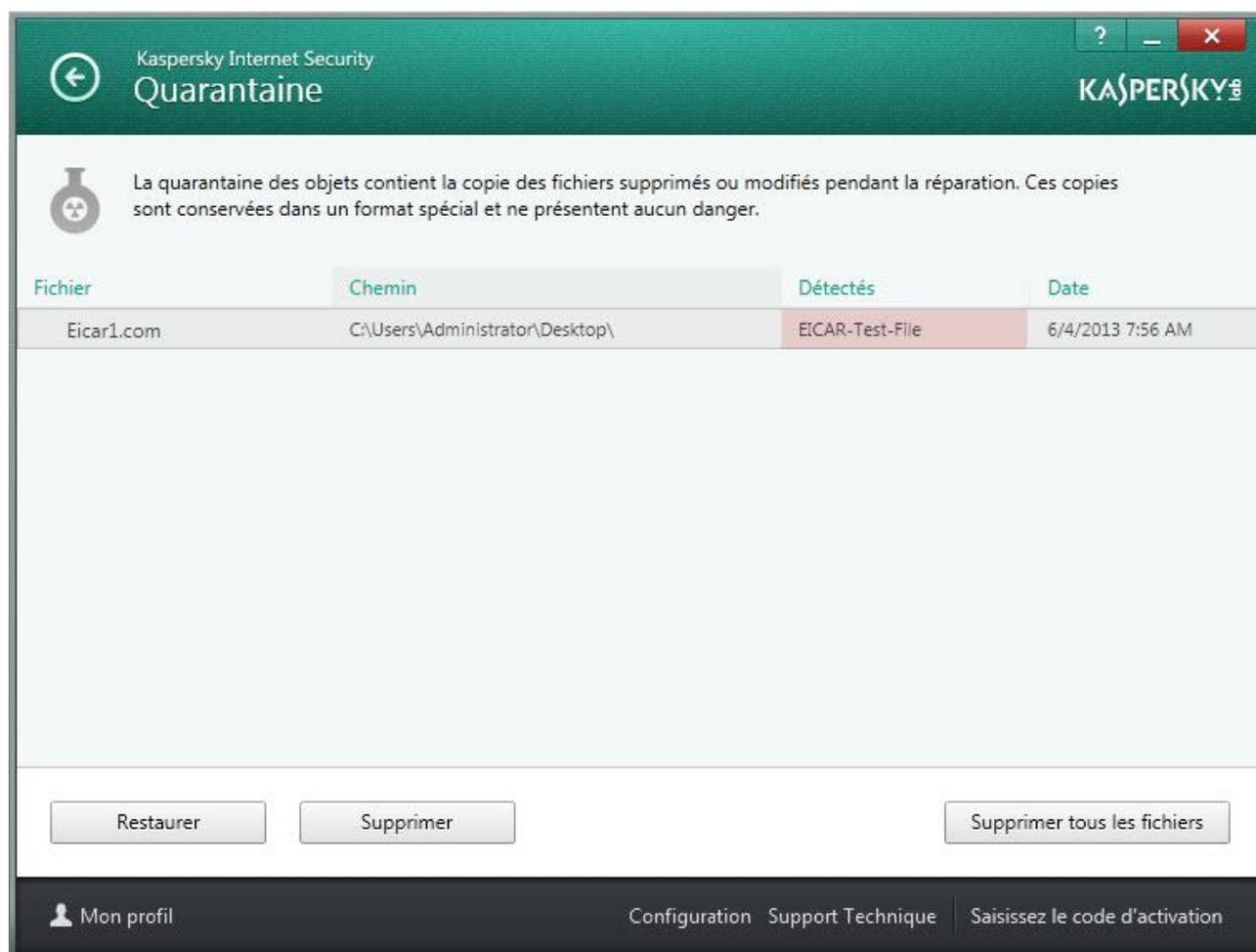


Illustration 4. Fenêtre **Quarantaine**

## RESTAURATION DU SYSTEME D'EXPLOITATION APRES L'INFECTION

Si vous soupçonnez que le système d'exploitation de votre ordinateur a été endommagé ou modifié suite aux actions des programmes malveillants ou suite à l'échec de système, utilisez l'*Assistant de restauration après une infection*, qui élimine les traces des objets malveillants dans le système. Les experts de Kaspersky Lab conseillent également de lancer l'Assistant après la réparation de l'ordinateur afin de confirmer que toutes les menaces et les dommages ont été supprimés.

L'Assistant vérifie si le système a été modifié d'une manière ou d'une autre : blocage de l'accès à l'environnement réseau, modification des extensions de fichiers de format connu, blocage du panneau d'administration, etc. Les causes de ces dégâts sont multiples. Il peut s'agir de l'activité de programmes malveillants, d'une mauvaise configuration du système, de pannes du système ou de l'utilisation d'applications d'optimisation du système qui ne fonctionnent pas correctement.

Après l'étude, l'Assistant analyse les informations recueillies afin d'identifier les dommages dans le système qui requièrent une intervention immédiate. La liste des actions à exécuter pour supprimer l'infection est générée sur la base des résultats de l'analyse. L'Assistant regroupe les actions en catégorie selon la gravité des problèmes identifiés.

➤ Pour lancer l'Assistant de restauration après une infection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans la fenêtre ouverte dans le groupe **Restauration du système**, cliquez sur le bouton **Exécuter**.

La fenêtre de l'Assistant de restauration après une infection s'ouvre.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Lancement de la restauration du système

Assurez-vous que l'option **Exécuter la recherche des problèmes liés à l'activité d'un logiciel malveillant** est sélectionnée dans la fenêtre de l'Assistant, puis cliquez sur le bouton **Suivant**.

### Etape 2. Recherche des problèmes

L'Assistant recherche les problèmes et les dégâts potentiels qu'il faut supprimer. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

### Etape 3. Sélection d'actions pour la résolution des problèmes

Tous les problèmes identifiés à l'étape précédente sont regroupés en fonction du danger qu'ils présentent. Pour chaque groupe de corruptions, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution contribuera à l'élimination des problèmes. Trois groupes d'actions ont été désignés :

- Les *actions vivement recommandées* permettent de supprimer les corruptions qui constituent un problème sérieux. Il est conseillé d'exécuter toutes les actions de ce groupe.
- Les *actions recommandées* visent à supprimer les corruptions qui peuvent présenter un danger. L'exécution des actions de ce groupe est également recommandée.
- Les *actions complémentaires* sont prévues pour supprimer les corruptions du système qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur.

Pour voir les actions reprises dans le groupe, cliquez sur le signe + situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

**Il est vivement déconseillé de décocher les cases sélectionnées par défaut car vous pourriez mettre en danger la sécurité de l'ordinateur.**

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

### Etape 4. Suppression des problèmes

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des problèmes peut durer un certain temps. Une fois la suppression des problèmes terminée, l'Assistant passe automatiquement à l'étape suivante.

## Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# CONFIGURATION DE L'ANTIVIRUS COURRIER

Kaspersky Internet Security permet d'analyser les messages du courrier électronique sur la présence des objets dangereux à l'aide de l'Antivirus Courrier. L'Antivirus Courrier est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI et NNTP (y compris les messages envoyés via des connexions sécurisées (SSL) via les protocoles POP3, SMTP et IMAP).

L'Antivirus Courrier analyse par défaut aussi bien les messages entrants que les messages sortants. En cas de nécessité, vous pouvez activer l'analyse des messages entrants uniquement.

➔ *Pour configurer l'Antivirus Courrier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre.
3. Dans la partie gauche de la fenêtre, dans la section **Protection**, sélectionnez le module **Antivirus Courrier**.

Cette fenêtre affiche les paramètres de l'Antivirus Courrier.

4. Confirmez que le bouton d'activation de l'Antivirus Courrier dans la partie supérieure de la fenêtre est bien en position **Activé**.
5. Sélectionnez le niveau de protection :
  - **Recommandé**. A ce niveau, l'Antivirus Courrier analyse le courrier entrant et sortant ainsi que les archives jointes.
  - **Faible**. A ce niveau, l'Antivirus Courrier analyse uniquement le courrier entrant, mais pas les archives jointes.
  - **Elevé**. A ce niveau, l'Antivirus Courrier analyse le courrier entrant et sortant ainsi que les archives jointes. Si vous choisissez le niveau élevé, l'analyse heuristique opère une analyse en profondeur.
6. Dans la liste déroulante **Action en cas de découverte d'une menace**, sélectionnez l'action que l'Antivirus Courrier exécutera en cas de découverte d'un objet infecté (par exemple, réparer).

Si aucune menace n'a été détectée dans le message ou si les objets infectés ont été réparés, le message peut être utilisé. Si l'objet infecté ne peut pas être réparé, l'Antivirus Courrier donne un autre nom ou supprime l'objet du message et place dans le sujet du message la notification que le message a été traité par Kaspersky Internet Security. Dans le cas de suppression de l'objet, Kaspersky Internet Security crée sa copie de sauvegarde et place en quarantaine (cf. section "Restauration de l'objet supprimé ou réparé par l'application" à la page [37](#)).

## BLOPAGE DU COURRIER INDESIRABLE (SPAM)

Si vous recevez un volume important de courrier indésirable, activez le module Anti-Spam et définissez le niveau de protection recommandé.

➔ *Pour activer l'Anti-Spam et définir le niveau de protection recommandé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre pour accéder à la section **Configuration**.

3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez le module **Anti-Spam**.  
La fenêtre reprend les paramètres de l'Anti-Spam.
5. Activez l'Anti-Spam à l'aide du bouton dans la partie droite de la fenêtre.
6. Assurez-vous que le niveau **Recommandé** est défini dans le groupe **Niveau de protection**.

## TRAITEMENT DES APPLICATIONS INCONNUES

Grâce à Kaspersky Internet Security, vous pouvez réduire les risques liés à l'utilisation d'applications inconnues (par exemple, risques d'infection par des virus ou modification non sollicitée des paramètres du système d'exploitation).

Kaspersky Internet Security inclut les modules et les outils qui permettent de vérifier la réputation de l'application et de contrôler l'activité de l'application sur votre ordinateur.

### DANS CETTE SECTION

Vérification de la réputation des applications .....	<a href="#">41</a>
Contrôle des actions de l'application sur l'ordinateur et dans le réseau .....	<a href="#">42</a>
Utilisation du mode des Applications sécurisées.....	<a href="#">44</a>

## VERIFICATION DE LA REPUTATION DES APPLICATIONS

Kaspersky Internet Security permet de vérifier la réputation des applications auprès des utilisateurs dans le monde entier. La réputation de l'application reprend les indices suivants :

- nom de l'éditeur ;
- informations sur la signature numérique (disponible en présence de la signature numérique) ;
- informations sur le groupe dans lequel l'application a été placée par le Contrôle des Applications ou par la majorité des utilisateurs de Kaspersky Security Network ;
- nombre d'utilisateurs de Kaspersky Security Network qui utilisent l'application (disponible si l'application est classée dans le groupe De confiance dans la base Kaspersky Security Network) ;
- heure à laquelle l'application est devenue connue dans Kaspersky Security Network ;
- pays dans lesquels l'application est la plus répandue.

La vérification de la réputation des applications est disponible uniquement si vous avez accepté de participer au Kaspersky Security Network.

► Pour connaître la réputation d'une application,

ouvrez le menu contextuel du fichier exécutable de l'application et sélectionnez l'option **Consulter la réputation dans le KSN** (cf. ill. ci-après).

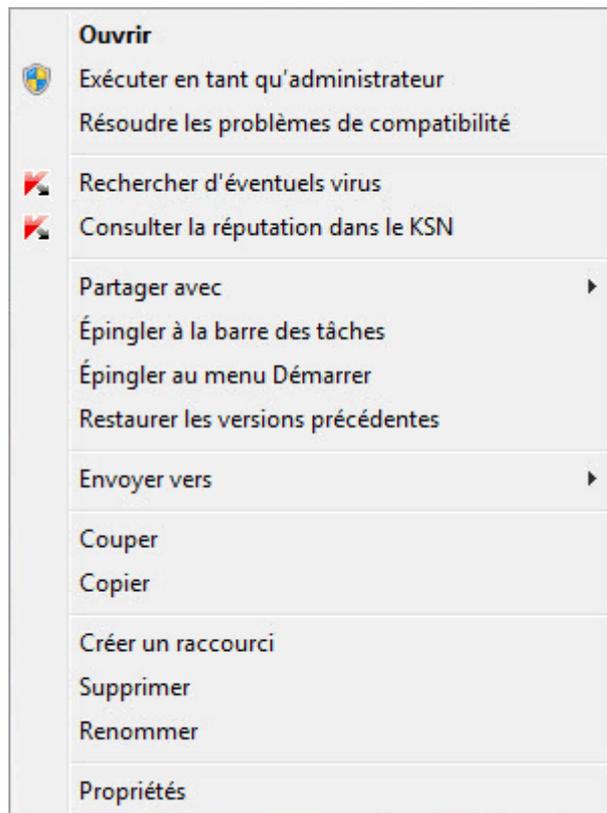


Illustration 5. Menu contextuel du fichier exécutable dans Microsoft Windows

Une fenêtre reprenant les données sur la réputation de l'application dans le KSN s'ouvre.

## VOIR EGALEMENT

Participation au Kaspersky Security Network (KSN) ..... [71](#)

## CONTROLE DES ACTIONS DE L'APPLICATION SUR L'ORDINATEUR ET DANS LE RESEAU

Le Contrôle des Applications prévient l'exécution des actions dangereuses pour le système, et il assure aussi le contrôle d'accès aux ressources du système d'exploitation et de vos données personnelles.

Le Contrôle des Applications surveille les actions en exécution dans le système par les applications installées sur les ordinateurs, et il les règle sur la base des règles. Ces règles réglementent l'activité potentiellement dangereuse, y compris l'accès des applications aux ressources protégées (par exemple, aux fichiers, dossiers, clés du registre, adresses réseau, etc.).

Lors de l'utilisation des systèmes d'exploitation de 64 bits, les privilèges des applications sur l'exécution des actions suivantes ne sont pas disponibles à la configuration :

- accès direct à la mémoire physique ;
- administration des pilotes de l'imprimante ;

- création du service ;
- ouverture du service pour la lecture ;
- ouverture du service pour la modification ;
- modification de la configuration du service ;
- administration du service ;
- lancement du service ;
- suppression du service ;
- accès aux données internes du navigateur ;
- accès aux objets critiques du système ;
- accès au stockage des mots de passe ;
- installation des privilèges du débogueur ;
- utilisation des interfaces logicielles du système ;
- utilisation des interfaces logicielles du système (DNS).

Lors de l'utilisation de Microsoft Windows 8 de 64 bits, les privilèges des applications sur l'exécution des actions suivantes ne sont pas disponibles à la configuration :

- envoi des messages de fenêtre aux autres processus ;
- opérations suspectes ;
- installation des intercepteurs ;
- interception des événements entrants du flux ;
- création des images de l'écran.

Le module Pare-feu contrôle l'activité réseau des applications.

Au premier lancement de l'application sur l'ordinateur, le Contrôle des Applications analyse sa sécurité et place dans un des groupes (De confiance, Douteuses, Restrictions élevées ou Restrictions faibles). Le groupe définit les règles que Kaspersky Internet Security appliquera pour contrôler l'activité de cette application.

Vous pouvez modifier manuellement les règles de contrôle des actions pour l'application sur l'ordinateur.

► *Pour modifier manuellement la règle de contrôle pour l'application, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton  et sélectionnez la section **Contrôle des Applications**.

La section **Contrôle des Applications** apparaît dans la fenêtre.

3. Dans le groupe **Applications**, passez par le lien **Administration des applications**.

La section **Administration des applications** apparaît dans la fenêtre.

4. Cliquez sur l'application nécessaire dans la liste.

La fenêtre **Règles pour l'application** s'ouvre.

5. Définissez les règles de contrôle de l'application :

- Pour configurer les règles d'accès de l'application aux ressources du système d'exploitation, procédez comme suit :
  - a. Sous l'onglet **Fichiers et base de registres**, sélectionnez la catégorie nécessaire des ressources.
  - b. D'un clic droit de la souris dans la colonne avec l'action possible sur la ressource (**Lecture, Ecriture, Suppression** ou **Création**), ouvrez le menu contextuel et y sélectionnez la valeur nécessaire (**Autoriser, Interdire** ou **Confirmer l'action**).
- Pour configurer les privilèges de l'application sur l'exécution des actions différentes dans le système d'exploitation, procédez comme suit :
  - a. Sélectionnez la catégorie nécessaire des privilèges sous l'onglet **Privilèges**.
  - b. D'un clic droit de la souris dans la colonne **Autorisation**, ouvrez le menu contextuel et y sélectionnez la valeur nécessaire (**Autoriser, Interdire** ou **Confirmer l'action**).
- Pour configurer les privilèges de l'application sur l'exécution des actions différentes dans le réseau, procédez comme suit :
  - a. Sous l'onglet **Règles réseau**, cliquez sur le bouton **Ajouter**.  
La fenêtre **Règle réseau** s'ouvre.
  - b. Dans la fenêtre ouverte, définissez les paramètres nécessaires, puis cliquez sur le bouton **OK**.
  - c. Pour définir la priorité de la nouvelle règle, déplacez-la vers le haut ou vers le bas de la liste à l'aide des boutons **Haut** et **Bas**.
- Pour désactiver certaines actions de l'analyse par le Contrôle des Applications, cochez les cases pour les actions à ne pas contrôler sous l'onglet **Exclusions**.

Toutes les exclusions créées dans les règles des applications sont accessibles dans la fenêtre de configuration de l'application, dans le groupe **Menaces et exclusions**.

Le Contrôle des Applications va surveiller et limiter les actions conformément aux paramètres configurés.

## UTILISATION DU MODE DES APPLICATIONS SECURISEES

Kaspersky Internet Security offre la possibilité de créer sur l'ordinateur un environnement protégé (mode des Applications sécurisées), où le lancement uniquement des applications avec l'état des applications de confiance est autorisé. Le mode des Applications sécurisées vous convient si vous utilisez l'ensemble permanent des programmes répandus et vous n'avez pas besoin de télécharger et de lancer souvent des nouveaux fichiers inconnus depuis Internet. Lors de l'utilisation du mode des Applications sécurisées, Kaspersky Internet Security bloque le lancement de toutes les applications qui ne sont pas des applications de confiance pour des raisons quelconques (par exemple, les informations sur l'application depuis KSN, la confiance au programme d'installation et à la source depuis laquelle l'application est téléchargée).

Le mode des Applications sécurisées peut être absent ou peut être inaccessible dans la version actuelle de Kaspersky Internet Security. La présence dans Kaspersky Internet Security du mode des Applications sécurisées dépend aussi de votre région et du fournisseur. Précisez la présence du mode des Applications sécurisées lors de l'achat de l'application.

Si la présence du mode des Applications sécurisées est prévue dans votre version de Kaspersky Internet Security, mais le mode des Applications sécurisées est inaccessible actuellement, il peut devenir accessible après la mise à jour (cf. section "Mise à jour des bases et des modules de l'application" à la page 33) de l'application.

Le mode des Applications sécurisées peut être aussi inaccessible si les fichiers systèmes sont situés dans les sections du disque dur avec le système de fichier différent de NTFS.

Avant d'activer le mode des Applications sécurisées, Kaspersky Internet Security effectue l'analyse du système d'exploitation et des applications installées sur votre ordinateur. Si suite à l'analyse, un logiciel qui n'est pas un logiciel de confiance a été détecté, il n'est pas conseillé d'activer le mode des Applications sécurisées. Le blocage du lancement des applications méfiantes peut nuire à votre travail. Vous pouvez autoriser à la main le lancement des applications dont vous faites confiance et puis activer le mode des Applications sécurisées.

L'analyse du système d'exploitation et des applications installées est exécutée au premier lancement du mode des Applications sécurisées. L'analyse peut prendre un long temps (jusqu'à plusieurs heures). L'analyse peut être exécutée en arrière-plan.

Pour utiliser le mode des Applications sécurisées, il faut activer les modules de protection Contrôle Parental, Antivirus Fichiers et Surveillance du système. Lors de l'arrêt d'un de ces composants, le mode des Applications sécurisées est désactivé.

En cas de nécessité, vous pouvez désactiver le mode des Applications sécurisées à tout moment.

➔ Pour activer le mode des Applications sécurisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie inférieure de la fenêtre, cliquez sur le bouton  et sélectionnez la section **Contrôle des Applications**.

La section **Contrôle des Applications** apparaît dans la fenêtre.

3. Dans le groupe **Le mode des Applications sécurisées est désactivé**, utilisez le lien **Activer** dans la partie inférieure de la fenêtre.

Si les modules de protection nécessaires sont désactivés, la fenêtre **Activer le mode des Applications sécurisées** s'ouvre. Cette fenêtre contient les informations sur les modules de protection à activer pour utiliser le mode des Applications sécurisées.

4. Cliquez sur le bouton **Poursuivre**.

L'analyse des fichiers systèmes et des applications installées commence. Les informations sur le processus d'analyse s'affiche dans la fenêtre ouverte **Analyse des applications installées**.

Attendez la fin de l'analyse des applications installées. Vous pouvez réduire la fenêtre **Analyse des applications installées**. Avec cela, l'analyse est exécutée en arrière-plan. Les informations sur le processus d'exécution de l'analyse des applications installées s'affiche à l'aide du lien **Exécution de l'analyse des applications installées (<N> %)** dans la fenêtre **Contrôle des Applications**.

5. Consultez les informations sur les résultats d'analyse dans la fenêtre **L'analyse des applications installées est terminée**.

Si durant les processus d'analyse les fichiers systèmes, sur lesquels il n'y a pas assez d'informations, ont été détectés, il est déconseillé d'activer le mode des Applications sécurisées. Il est aussi déconseillé d'activer le mode des Applications sécurisées si un grand nombre d'applications, sur lesquelles il n'y a pas assez d'informations pour que Kaspersky Internet Security les considère comme totalement sûres, a été détecté. Prenez d'une façon indépendante une décision sur l'utilisation du mode des Applications sécurisées.

- Utilisez le lien **Autoriser l'exécution des fichiers système inconnus et continuer**.

Vous pouvez consulter les informations sur les fichiers systèmes méfiants, en utilisant le lien **Passer à la liste des fichiers système inconnu**. La liste des fichiers systèmes méfiants s'affiche dans la fenêtre **Fichiers systèmes inconnus**. Vous pouvez aussi annuler l'utilisation du mode des Applications sécurisées, en cliquant sur le bouton **Ne pas activer le mode des Applications sécurisées**.

- Cliquez sur le bouton **Activer le mode des Applications sécurisées**.

Le mode des Applications sécurisées sera activé. Kaspersky Internet Security bloque le lancement de toutes les applications qui ne sont pas des applications de confiance. Le passage à la fenêtre du Contrôle des Applications sera exécuté.

➔ *Pour activer le mode des Applications sécurisées, procédez comme suit :*

- Ouvrez la fenêtre principale de l'application.

- Dans la partie inférieure de la fenêtre, cliquez sur le bouton  et sélectionnez la section **Contrôle des Applications**.

La section **Contrôle des Applications** apparaît dans la fenêtre.

- Dans le groupe **Le mode des Applications sécurisées est désactivé**, utilisez le lien **Désactiver** dans la partie inférieure de la fenêtre.

Le mode des Applications sécurisées sera désactivé.

## PROTECTION DES DONNEES PERSONNELLES CONTRE LE VOL

Kaspersky Internet Security protège vos données personnelles suivantes contre le vol :

- mots de passe, noms d'utilisateur et autres données d'enregistrement ;
- numéros de compte et de cartes de crédit.

Kaspersky Internet Security reprend des modules et des outils qui permettent de protéger vos données personnelles contre le vol par des individus malintentionnés via des méthodes telles que le phishing et l'interception des données saisies au clavier.

L'Anti-Phishing, inclus dans l'Antivirus Internet, l'Antivirus Courrier et l'Antivirus IM ("Chat"), garantit la protection contre le phishing. Activez ces modules pour garantir la protection la plus efficace contre le phishing.

Pour la protection contre l'interception des données au clavier, le Clavier virtuel et la protection de saisie des données au clavier sont prévus.

Pour supprimer les informations sur les actions d'utilisateur sur l'ordinateur, l'Assistant d'élimination des traces d'activité est prévu.

Pour la protection des données lors de l'utilisation des services de la banque en ligne et lors des paiements dans les boutiques en ligne, les fonctions de la Protection bancaire sont prévues.

Pour la protection contre l'envoi des données personnelles via Internet, un des outils du Contrôle Parental (cf. section "Utilisation du Contrôle Parental" à la page [55](#)) est prévu.

**DANS CETTE SECTION**

Clavier virtuel ..... [47](#)

La protection de saisie des données au clavier..... [50](#)

Configuration de la Protection bancaire ..... [51](#)

Suppression des traces d'activité..... [52](#)

**CLAVIER VIRTUEL**

Au cours de l'utilisation d'Internet, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. Ceci se produit par exemple lors de l'ouverture d'une session sur un site Internet, lors de l'achat sur une boutique en ligne ou en cas d'utilisation d'une banque en ligne.

Le risque que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes existe.

Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

Le clavier virtuel protège contre l'interception des données personnelles uniquement avec les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Si vous utilisez un autre navigateur, le Clavier virtuel ne protège pas les données personnelles saisies contre l'interception.

Le clavier virtuel n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de la Boutique Windows, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé élargi** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur. Dans ce cas, il est conseillé d'appeler le clavier virtuel depuis l'interface Kaspersky Internet Security.

Le clavier virtuel ne peut protéger vos données si le site Internet nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

De nombreux logiciels espions peuvent réaliser des captures d'écran qui sont transmises automatiquement à l'individu malintentionné pour analyse et récupération des données personnelles de l'utilisateur. Le clavier virtuel protège les données personnelles saisies contre l'interception par capture d'écran.

Le clavier virtuel ne prévient pas la prise des images de l'écran à l'aide de la touche **Print Screen** et d'autres combinaisons des touches définies dans les paramètres du système d'exploitation, ainsi que la prise des images de l'écran à l'aide de la technologie DirectX®.

Le clavier virtuel possède les particularités suivantes :

- Il faut appuyer sur les touches du Clavier virtuel 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, si vous souhaitez utiliser une combinaison de touches (par exemple, **ALT+F4**), il faut d'abord appuyer sur la première touche (par exemple **ALT**), puis sur la deuxième (par exemple **F4**), puis à nouveau sur la première. La deuxième pression sur la première touche équivaut au relâchement des deux touches sur le clavier.
- La langue de saisie du Clavier virtuel est modifiée à l'aide de la même combinaison de touches que celle définie dans les paramètres du système d'exploitation pour le clavier normal. La deuxième touche doit être activée d'un clic droit de la souris (par exemple, si les paramètres du système d'exploitation indiquent que le changement de la langue du clavier s'opère à l'aide de la combinaison **LEFT ALT+SHIFT**, il faudra cliquer sur la touche **LEFT ALT** avec le bouton gauche de la souris, puis cliquer avec le bouton droit sur la touche **SHIFT**).

Pour protéger les données saisies à l'aide du Clavier virtuel, il faut redémarrer l'ordinateur après l'installation de Kaspersky Internet Security.

Les méthodes suivantes s'offrent à vous pour ouvrir le Clavier virtuel :

- via le menu contextuel de l'icône de l'application dans la zone de notification ;
- au départ de la fenêtre principale de l'application ;
- au départ du navigateur Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome ;
- à l'aide de l'icône d'accès rapide du Clavier virtuel dans le champ de saisie sur les sites Internet ;

L'affichage de l'icône d'accès rapide dans les champs de saisie sur les sites Internet peut être configuré.

Lors de l'utilisation du Clavier virtuel, Kaspersky Internet Security désactive la fonction d'autoremplissage pour les champs de saisie sur les sites Internet.

- à l'aide d'une combinaison de touches du clavier ;
- via le gadget Kaspersky Internet Security (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

► Pour ouvrir le Clavier virtuel depuis le menu contextuel de l'icône de l'application dans la zone de notification,

Sélectionnez l'option **Outils** → **Clavier virtuel** dans le menu contextuel de l'icône de l'application (cf. ill. ci-dessous).

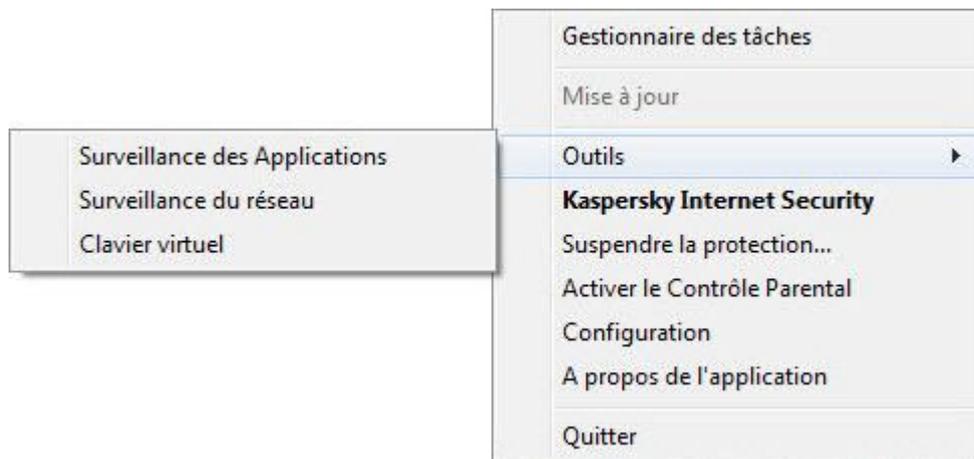


Illustration 6. Menu contextuel de Kaspersky Internet Security ;

► Pour ouvrir le Clavier virtuel depuis la fenêtre principale de l'application,

sélectionnez la section **Clavier virtuel** dans la partie inférieure de la fenêtre principale de l'application.

► Pour ouvrir le Clavier virtuel depuis la fenêtre du navigateur,

cliquez sur le bouton  **Clavier virtuel** dans la barre d'outils de Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome.

► Pour ouvrir le Clavier virtuel à l'aide du clavier,

appuyez sur la combinaison des touches **CTRL+ALT+SHIFT+P**.

- *Pour ouvrir le Clavier virtuel à l'aide du gadget,*

cliquez sur le bouton du gadget pour lequel cette action a été désignée.

- *Pour configurer l'affichage de l'icône d'accès rapide du Clavier virtuel dans les champs de saisie sur les sites Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre.
3. Dans la fenêtre ouverte **Configuration** dans la section **Avancé**, sélectionnez la sous-section **Saisie sécurisée de données**.

Les paramètres de la configuration de la saisie sécurisée des données s'affichent dans la fenêtre.

4. S'il faut, cochez la case **Ouvrir le Clavier virtuel via la combinaison de touches CTRL+ALT+SHIFT+P** dans le groupe **Clavier virtuel**.
5. Si vous voulez que l'icône d'appel du Clavier Virtuel s'affiche dans les champs de saisie, cochez la case **Afficher l'icône d'accès rapide dans les champs de saisie**.
6. Si vous voulez que l'icône d'appel du Clavier virtuel s'affiche uniquement lors de l'ouverture des sites Internet concrets, procédez comme suit :

- a. Dans le groupe **Clavier virtuel**, passez par le lien **Modifier les catégories**.

La fenêtre **Catégories pour le clavier virtuel** s'ouvre.

- b. Cochez les cases pour les catégories des sites Internet sur lesquels il faut afficher l'icône d'accès rapide dans les champs de saisie.

L'icône d'appel du Clavier virtuel sera affichée lors de l'ouverture du site Internet lié à une des catégories quelconques sélectionnées.

- c. Si vous voulez activer ou désactiver l'affichage de l'icône d'appel du Clavier virtuel sur le site Internet définie, procédez comme suit :

- a. Passez par le lien **Configuration des exclusions**.

La fenêtre **Exclusions pour la Clavier virtuel** s'ouvre.

- b. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.

La fenêtre d'ajout d'une exclusion pour le Clavier virtuel s'ouvre.

- c. Saisissez l'adresse du site Internet dans le champ **Adresse URL**.

- d. Si vous voulez que l'icône d'appel du Clavier virtuel s'affiche (ou ne s'affiche pas) uniquement sur la page Internet indiquée, dans le groupe **Zone d'application**, sélectionnez **Appliquer à la page indiquée**.

- e. Dans le groupe **Icône du Clavier virtuel**, indiquez si l'icône d'appel du Clavier virtuel doit s'afficher sur la page Internet indiquée.

- f. Cliquez sur le bouton **Ajouter**.

Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions pour la Clavier virtuel**. Lors de l'ouverture du site Internet, l'icône d'appel du Clavier virtuel sera affichée conformément aux paramètres configurés.

## PROTECTION DE SAISIE DES DONNEES DEPUIS LE CLAVIER

La protection de la saisie des données au clavier permet d'éviter l'interception des données saisies au clavier.

La protection de saisie des données au clavier fonctionne uniquement dans les navigateurs Microsoft Internet Explorer, Mozilla Firefox et Google Chrome. Lors de l'utilisation d'autres navigateurs Internet, les données, saisies au clavier, ne sont pas protégées contre l'interception.

La protection de saisie des données n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de la Boutique Windows, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé élargi** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur.

La protection de la saisie des données au clavier ne peut protéger vos données si le site Internet nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus malintentionnés.

Vous pouvez configurer la protection de la saisie des données au clavier sur des différents sites Internet. Dès que la protection de saisie des données au clavier est configurée, il ne faut pas exécuter les actions complémentaires lors de la saisie des données.

Pour protéger la saisie des données au clavier, il faut redémarrer l'ordinateur après l'installation de Kaspersky Internet Security.

► Pour configurer la protection de la saisie des données au clavier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre pour accéder à la section **Configuration**.
3. Dans la section **Avancé**, sélectionnez la sous-section **Saisie sécurisée des données**.  
Les paramètres de la saisie sécurisée des données s'affichent.
4. Dans le groupe **Clavier** situé dans la partie inférieure de la fenêtre, cochez la case **Protéger les données saisies au clavier**.
5. Définissez la zone de protection de la saisie des données à l'aide du clavier physique :
  - a. Ouvrez la fenêtre **Catégories pour la protection des données saisies au clavier** via le lien **Modifier les catégories** dans la partie inférieure de la fenêtre **Clavier physique**.
  - b. Cochez les cases pour les catégories des sites Internet sur lesquels il faut protéger les données saisies au clavier.
  - c. Si vous voulez activer la protection de la saisie des données au clavier sur le site Internet définie, procédez comme suit :
    - a. Ouvrez la fenêtre **Exclusions pour la protection des données saisies au clavier** via le lien **Configuration des exclusions**.
    - b. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Ajouter**.  
La fenêtre d'ajout d'une exclusion pour la protection des données saisies au clavier s'ouvre.
    - c. Dans la fenêtre qui s'ouvre, saisissez l'URL du site dans le champ **Adresse Internet**.
    - d. Sélectionnez une des options de protection des données saisies sur ce site Internet (**Appliquer à la page indiquée** ou **Appliquer à tout le site Internet**).

- e. Sélectionnez l'action de la protection de la saisie des données sur ce site (**Protéger** ou **Ne pas protéger**).
- f. Cliquez sur le bouton **Ajouter**.

Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions pour la protection des données saisies au clavier**. Quand vous ouvrirez ce site, la saisie des données sera protégée conformément aux paramètres définis.

## CONFIGURATION DE LA PROTECTION BANCAIRE

Pour protéger les données confidentielles que vous saisissez sur les sites Internet des banques et des systèmes de paiements (par exemple, les numéros des cartes bancaires, les mots de passe d'accès aux services des transactions bancaires en ligne), ainsi que pour prévenir le vol des moyens de paiements lors des paiements en lignes, Kaspersky Internet Security propose d'ouvrir ces sites Internet dans la navigation protégée.

Le lancement de la navigation sécurisée est impossible si la case **Activer l'autodéfense** est décochée dans la section **Paramètres avancés**, la sous-section **Autodéfense** de la fenêtre de configuration de l'application.

Vous pouvez configurer la Protection bancaire pour définir automatiquement les sites Internet des banques et des systèmes de paiements.

La Protection bancaire n'est pas disponible dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur. Vous pouvez lancer le mode du navigateur protégé depuis l'interface Kaspersky Internet Security.

Sous Microsoft Windows 8 x64, Kaspersky Internet Security ne protège pas la fenêtre de navigation sécurisée contre la prise de captures d'écran illicite.

➤ *Pour configurer la Protection bancaire, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Protection**.
4. Dans la partie droite de la section **Protection**, sélectionnez la sous-section **Protection bancaire**.  
La fenêtre affiche alors les paramètres du module Protection bancaire.
5. Activez le module Protection bancaire à l'aide du bouton dans la partie supérieure de la fenêtre.
6. Pour activer la notification sur les vulnérabilités détectées dans le système d'exploitation avant le lancement de la navigation protégée, cochez la case **Signaler les vulnérabilités dans le système d'exploitation**.

➤ *Pour configurer la Protection bancaire pour le site Internet défini, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Sélectionnez la section **Protection bancaire** dans la partie inférieure de la fenêtre principale.  
La section **Protection bancaire** apparaît.
3. Cliquez sur le bouton **Ajouter le site Internet d'une banque ou d'un système de paiement**.

Les champs de saisie des informations relatives au site apparaissent dans la partie droite de la fenêtre.

4. Dans le champ **Site Internet d'une banque ou d'un système de paiement**, saisissez l'adresse du site Internet à ouvrir dans le navigateur protégé.

Devant l'adresse du site Internet, le protocole <https://> doit être indiqué, utilisé par le navigateur protégé par défaut.

5. En cas de nécessité, saisissez le nom ou la description de ce site Internet dans le champ **Description**.
6. Sélectionnez le mode de lancement de la navigation protégée lors de l'ouverture de ce site Internet :
  - Si vous voulez que Kaspersky Internet Security propose d'ouvrir ce site Internet à chaque fois dans le navigateur protégé, sélectionnez l'option **Confirmer l'action**.
  - Si vous voulez que Kaspersky Internet Security ouvre automatiquement ce site Internet dans la navigation protégée, sélectionnez l'option **Lancer la navigation protégée automatiquement**.
  - Si vous voulez activer la Protection bancaire pour ce site Internet, sélectionnez l'option **Ne pas lancer la navigation sécurisée**.
7. Dans la partie droite de la fenêtre, cliquez sur le bouton **Ajouter**.

Le site Internet de la banque ou du système de paiement apparaît dans la liste dans la partie gauche de la fenêtre.

## SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système d'exploitation. Les informations suivantes sont conservées :

- données sur les termes de recherche et les sites Internet visités ;
- informations sur l'exécution d'applications et l'ouverture et l'enregistrement de fichiers ;
- entrées dans le journal système Microsoft Windows ;
- autres informations relatives aux actions de l'utilisateur.

Les informations relatives aux actions de l'utilisateur impliquant des données confidentielles sont potentiellement accessibles aux individus malintentionnés et aux tiers.

Kaspersky Internet Security propose un Assistant de suppression des traces d'activité de l'utilisateur dans le système.

► *Pour lancer l'Assistant de suppression des traces d'activité, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, sélectionnez la section **Outils**.
3. Dans le groupe **Suppression des traces d'activité** de la fenêtre qui s'ouvre, cliquez sur le bouton **Exécuter**.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Guide de démarrage de l'Assistant

Assurez-vous que l'option **Exécuter la recherche des traces d'activité de l'utilisateur** est sélectionnée, puis appuyez sur le bouton **Suivant** pour lancer l'Assistant.

## Etape 2. Recherche de traces d'activité

L'Assistant recherche les traces d'activité sur votre ordinateur. La recherche peut durer un certain temps. Une fois la recherche terminée, l'Assistant passe automatiquement à l'étape suivante.

## Etape 3. Sélection des actions pour la suppression des traces d'activité

A la fin de la recherche, l'Assistant signale les traces d'activité détectées et les moyens proposés pour s'en débarrasser (cf. ill. ci-après).

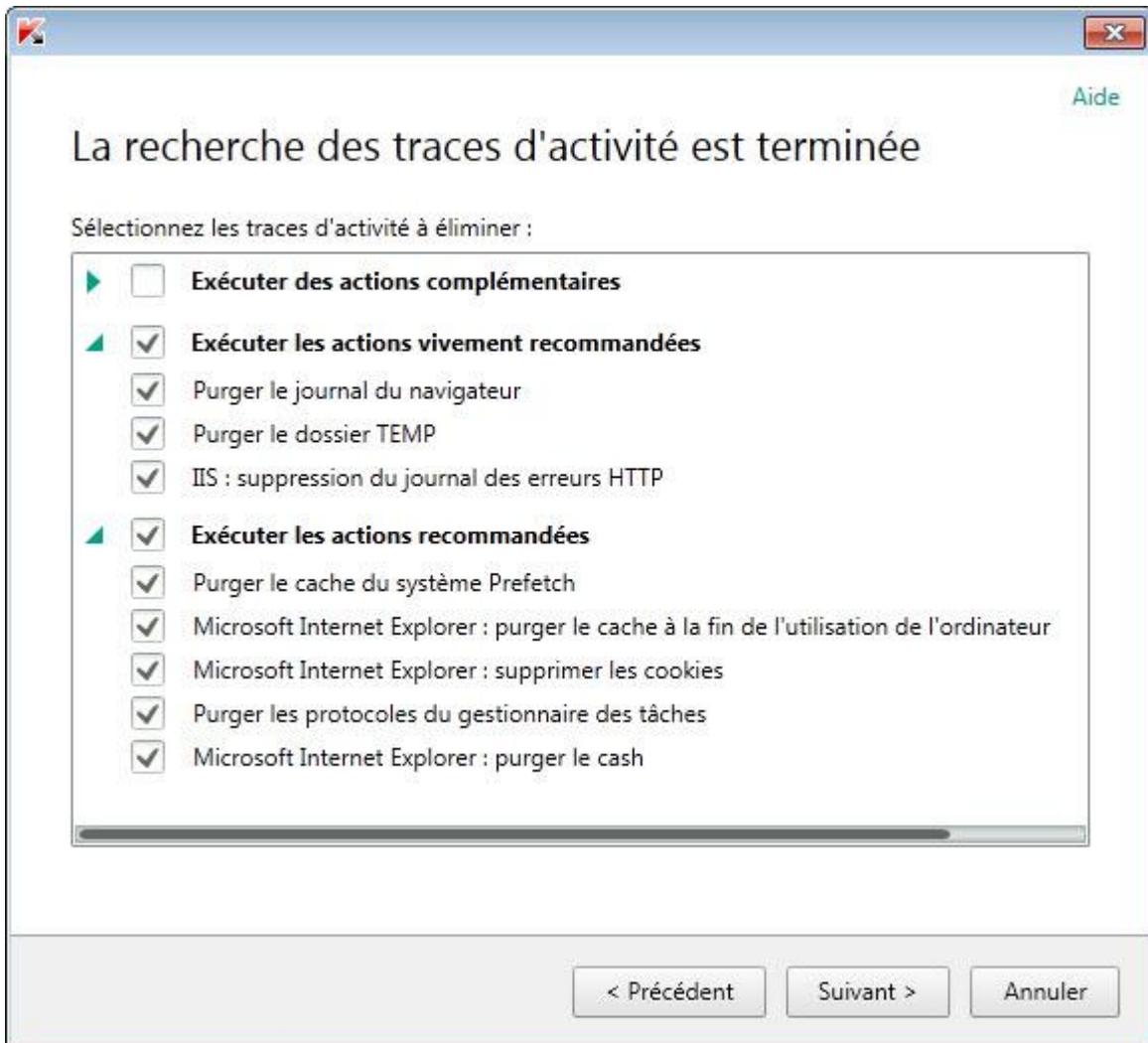


Illustration 7. Traces d'activité détectées et recommandations pour leur suppression

Pour voir les actions reprises dans le groupe, cliquez sur le signe ► situé à gauche du nom du groupe.

Pour que l'Assistant réalise une action, cochez la case à gauche du nom de l'action. Toutes les actions recommandées et vivement recommandées sont exécutées par défaut. Si vous ne souhaitez pas exécuter une action quelconque, désélectionnez la case en regard de celle-ci.

**Il est déconseillé de décocher les cases sélectionnées par défaut. Cela pourrait créer des menaces contre la sécurité de votre ordinateur.**

Une fois que vous aurez sélectionné les actions pour l'Assistant, cliquez sur **Suivant**.

## Etape 4. Suppression des traces d'activité

L'Assistant exécute les actions sélectionnées à l'étape précédente. La suppression des traces d'activité peut durer un certain temps. La suppression de certaines traces d'activité nécessitera peut-être le redémarrage de l'ordinateur. L'Assistant vous préviendra.

Une fois les traces d'activité supprimées, l'Assistant passe automatiquement à l'étape suivante.

## Etape 5. Fin de l'Assistant

Cliquez sur le bouton **Terminer** pour quitter l'Assistant.

# VERIFICATION DE LA SECURITE DU SITE INTERNET

Kaspersky Internet Security permet d'analyser la sécurité d'un site Internet avant de cliquer sur lien de ce site Internet. La vérification de la sécurité d'un site Internet est confiée à *URL Advisor*, *URL de confiance* et à *Filtrage de liens* repris dans l'Antivirus Internet.

Le module d'analyse des liens n'est pas accessible dans le navigateur Microsoft Internet Explorer 10 de la Boutique Windows, ainsi que dans le navigateur Microsoft Internet Explorer 10 si la case **Activer le mode protégé élargi** (Enhanced Protected Mode) est cochée dans les paramètres du navigateur.

Le module d'analyse des liens s'encastre dans les navigateurs Microsoft Internet Explorer, Google Chrome et Mozilla Firefox et analyse les liens sur la page Internet ouverte dans le navigateur. A côté de chaque lien, Kaspersky Internet Security affiche une des icônes suivantes :

-  – si la page Internet, qui s'ouvre à l'aide du lien, est saine selon les données de Kaspersky Lab ;
-  – s'il n'y a pas d'informations sur la sécurité de la page Internet, qui s'ouvre à l'aide du lien ;
-  – si la page Internet, qui s'ouvre à l'aide du lien, est dangereuse selon les données de Kaspersky Lab.

Lorsque vous placez le curseur de la souris sur l'icône, la fenêtre contextuelle avec la description plus détaillée du lien s'affiche.

Par défaut, Kaspersky Internet Security analyse les liens uniquement dans les résultats de recherche. Vous pouvez activer l'analyse des liens sur tout site Internet.

➤ *Pour configurer l'analyse des liens sur les sites Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Configuration**, situé dans la partie inférieure de la fenêtre principale, permet d'ouvrir la fenêtre **Configuration**.
3. Dans la section **Protection**, choisissez la sous-section **Antivirus Internet**.  
La fenêtre reprend les paramètres de l'Antivirus Internet.
4. Le lien **Paramètres avancés** de la partie inférieure de la fenêtre ouvre la fenêtre des paramètres avancés de l'Antivirus Internet.
5. Dans le groupe **URL Advisor**, cochez la case **Analyser les liens**.
6. Pour que l'Antivirus Internet analyse le contenu de tous les sites Internet, choisissez l'option **Sur tous les sites Internet sauf les sites indiqués**.

Le cas échéant, désignez les pages Internet auxquelles vous faites confiance à l'aide du lien **Configurer les exclusions**. L'Antivirus Internet ne va pas analyser le contenu des pages Internet indiquées, ainsi que les connexions cryptées avec les sites Internet indiqués.

7. Pour que l'Antivirus Internet analyse le contenu unique de certaines pages Internet, procédez comme suit :
  - a. Choisissez l'option **Uniquement sur les sites Internet indiqués**.
  - b. Utilisez le lien **Configurer les sites Internet vérifiés**.
  - c. Dans la fenêtre **Configurer les sites Internet vérifiés** qui s'ouvre, cliquez sur **Ajouter**.
  - d. Dans la fenêtre **Ajouter l'URL** qui s'ouvre, saisissez l'adresse de la page Internet dont le contenu ne devra pas être analysé.
  - e. Sélectionnez l'état d'analyse de la page Internet (*Actif* : l'Antivirus Internet analysera le contenu de la page Internet).
  - f. Cliquez sur le bouton **Ajouter**.

La page indiquée apparaît dans la liste de la fenêtre **URL analysées**. L'Antivirus Internet analysera les liens sur cette page.

8. Si vous souhaitez configurer les paramètres complémentaires d'analyse des liens, dans la fenêtre **Paramètres complémentaires de l'Antivirus Internet** du groupe **URL Advisor**, utilisez le lien **Configurer le module d'analyse des liens**.

La fenêtre **Configurer le module d'analyse des liens** s'ouvre.

9. Pour que l'Antivirus Internet vous alerte sur la sécurité des liens dans toutes les pages Internet, cochez la case **Tout lien** dans le groupe **Liens à analyser**.
10. Pour que l'Antivirus Internet affiche les informations relatives à l'appartenance d'un lien à une catégorie de contenu définie (par exemple, *langage vulgaire*), procédez comme suit :
  - a. Cochez la case **Afficher les informations sur les catégories de contenu des sites Internet**.
  - b. Cochez les cases en regard des catégories de contenu dont les informations devront apparaître dans les commentaires.

L'Antivirus Internet analyse les liens sur les pages indiquées et affichera les informations relatives aux catégories conformément aux paramètres configurés.

## UTILISATION DU CONTROLE PARENTAL

Le *Contrôle Parental* permet de contrôler les actions de différents utilisateurs sur l'ordinateur et sur le réseau. A l'aide du Contrôle Parental vous pouvez limiter l'accès aux ressources Internet et aux applications et consulter des rapports sur les actions des utilisateurs.

De nos jours, de plus en plus d'enfants et d'adolescents utilisent un ordinateur et Internet. Lors de l'utilisation de l'ordinateur et d'Internet, les enfants se mettent face à toute une série des menaces :

- la perte de temps et/ou de l'argent lors des connexions aux messageries instantanées, des ressources de jeu, des boutiques en ligne, des ventes aux enchères ;
- l'accès à des sites Internet réservés aux adultes (contenu pornographique, extrémiste, contenu extrême faisant l'apologie des armes, de la drogue, de la violence, etc.) ;
- le téléchargement de fichiers infectés par des programmes malveillants ;
- le dommage corporel dû au séjour de longue durée devant l'ordinateur ;
- les contacts avec des inconnus qui, en se faisant passer pour des amis, peuvent obtenir des informations personnelles de l'enfant (nom véridique, adresse, heure à laquelle il n'y a personne à la maison).

Le Contrôle Parental permet de diminuer les risques liés à l'utilisation de l'ordinateur et d'Internet. Pour ce faire, les fonctions suivantes du module sont utilisées :

- restriction de l'utilisation de l'ordinateur et d'Internet dans le temps ;
- composition de listes d'applications et de jeux dont l'exécution est autorisée ou interdite et restriction temporaire sur l'exécution d'applications autorisées ;
- composition de listes de sites dont la visite est autorisée ou interdite et sélection de catégories de contenu ne pouvant être consulté ;
- activation du mode de recherche sécurisée à l'aide des moteurs de recherche (dans ce cas, les liens de sites au contenu douteux n'apparaissent pas dans les résultats de la recherche) ;
- restriction du téléchargement de fichiers depuis Internet ;
- composition de listes de contacts avec lesquels les communications sont autorisées ou interdites dans les clients de messagerie instantanée ou dans les réseaux sociaux ;
- consultation du texte de la correspondance dans les clients de messageries instantanées et dans les réseaux sociaux ;
- interdiction du transfert de certaines données personnelles ;
- recherche de mots clés définis dans les communications.

Vous pouvez configurer les fonctions du Contrôle Parental séparément pour chaque compte utilisateur sur l'ordinateur. Vous pouvez également consulter les rapport du Contrôle Parental sur les actions des utilisateurs contrôlés.

## DANS CETTE SECTION

Contrôle de l'utilisation de l'ordinateur.....	<a href="#">56</a>
Contrôle de l'utilisation d'Internet .....	<a href="#">57</a>
Contrôle du lancement des jeux et des applications .....	<a href="#">59</a>
Contrôle des communications via les réseaux sociaux .....	<a href="#">60</a>
Contrôle du contenu de la correspondance.....	<a href="#">61</a>
Consultation du rapport sur les actions de l'utilisateur .....	<a href="#">62</a>

## CONTROLE D'UTILISATION DE L'ORDINATEUR

Le Contrôle Parental permet de définir une limite d'utilisation de l'ordinateur. Vous pouvez indiquer une plage de temps pendant laquelle le Contrôle Parental doit bloquer l'accès à l'ordinateur (pendant la nuit par exemple) ou définir une durée d'utilisation maximum par journée. Ces restrictions peuvent varier pour les jours ouvrables et les jours de repos.

➔ *Pour configurer les durées d'utilisation autorisées de l'ordinateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Ordinateur** ouvre la fenêtre de configuration du contrôle de l'utilisation de l'ordinateur.
5. Pour définir l'intervalle pendant lequel le Contrôle Parental va bloquer l'accès à l'ordinateur, cochez les cases **Bloquer l'accès pendant le temps de sommeil** dans les groupes **Jours ouvrables** et **Jours de repos**, puis définissez le début et la fin de l'intervalle à l'aide des listes déroulantes en regard des cases.

La programmation de la durée d'utilisation de l'ordinateur peut également être effectuée à l'aide d'une matrice.

La matrice s'affiche lorsque vous cliquez sur le bouton .

Le Contrôle Parental empêchera l'utilisateur d'accéder à l'utilisateur pendant la période indiquée.

6. Pour limiter la durée globale d'utilisation de l'ordinateur, cochez les cases **Limiter l'accès pendant la journée** dans les groupes **Jours ouvrables** et **Jours de repos**, puis définissez l'intervalle à l'aide des listes déroulantes en regard des cases.

Le Contrôle Parental empêchera l'utilisateur d'accéder à l'ordinateur une fois que la durée globale d'utilisation pour la journée dépassera l'intervalle défini.

7. Pour définir des pauses dans l'utilisation de l'ordinateur, cochez la case **Temps de repos** dans le groupe **Bloquer l'accès tous les**, puis définissez la fréquence (par exemple, toutes les heures) et la durée (par exemple, 10 minutes) des pauses à l'aide des listes déroulantes en regard de la case.

Le Contrôle Parental empêchera l'utilisateur d'accéder à l'ordinateur conformément aux paramètres.

## CONTROLE D'UTILISATION D'INTERNET

Le Contrôle Parental permet de limiter la durée d'utilisation d'Internet et de bloquer l'accès à des catégories sélectionnées de sites, voire à des sites en particulier. De plus, vous pouvez interdire le téléchargement de fichiers d'un certain type depuis Internet (par exemple, des archives, des vidéos, etc.).

➡ *Pour configurer les durées d'utilisation autorisées d'Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Internet** ouvre la fenêtre de configuration du contrôle de l'utilisation d'Internet.
5. Si vous souhaitez limiter la durée totale d'utilisation d'Internet pendant les jours ouvrables, cochez la case **Limiter l'accès les jours ouvrables** dans le groupe **Restriction d'accès dans Internet** et définissez la période à l'aide de la liste déroulante en regard de la case.
6. Si vous souhaitez limiter la durée total d'utilisation d'Internet les jours de repos, cochez la case **Limiter l'accès les jours de repos** et définissez la période à l'aide de la liste déroulante en regard de la case.

Le Contrôle Parental limitera la durée totale que l'utilisateur peut passer sur Internet conformément aux valeurs définies.

➤ *Pour limiter l'accès à certains sites Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.
- La section **Contrôle Parental** s'affiche dans la fenêtre.
3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
  4. Le lien **Configuration** du groupe **Internet** ouvre la fenêtre de configuration du contrôle de l'utilisation d'Internet.
  5. Pour que le contenu pour adulte n'apparaisse pas dans les résultats de la recherche, cochez la case **Activer la recherche sécurisée** dans le groupe **Consultation de sites**.

Le contenu "pour adultes" n'apparaîtra pas dans les résultats de recherche des moteurs (par exemple, Google, Bing®, Yahoo!™).

6. Pour interdire l'accès à certaines catégories de sites Internet, procédez comme suit :
  - a. Dans le groupe **Consultation de sites**, cochez la case **Bloquer l'accès aux sites Internet suivants**.
  - b. Choisissez l'option **Sites Internet pour les majeurs**, puis cliquez sur le lien **Sélectionner les catégories des sites Internet** pour ouvrir la fenêtre **Interdire l'accès aux catégories suivantes des sites Internet**.
  - c. Cochez les cases en regard des catégories de site dont l'ouverture sera interdite.

Le Contrôle Parental bloquera l'ouverture du site si son contenu appartient à une des catégories sélectionnées.

7. Pour bloquer l'accès à des sites Internet en particulier, procédez comme suit :
  - a. Dans le groupe **Consultation de sites**, cochez la case **Bloquer l'accès aux sites Internet suivants**.
  - b. Choisissez l'option **Tous les sites Internet sauf les sites autorisés dans la liste des exclusions**, puis cliquez sur le lien **Ajouter les exclusions** pour ouvrir la fenêtre **Exclusion des sites Internet**.
  - c. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.
 

La fenêtre **Ajouter un nouveau site Internet** s'ouvrira.
  - d. Saisissez l'adresse du site auquel vous souhaitez interdire l'accès dans le champ **Adresse Internet**.
  - e. Définissez la portée de l'interdiction dans le groupe **Zone d'action** : ensemble du site ou uniquement la page renseignée.
  - f. Si vous souhaitez interdire l'accès au site indiqué, choisissez l'option **Interdire** dans le groupe **Action**.
  - g. Cliquez sur le bouton **Ajouter**.

Le site Internet renseigné apparaît dans la liste de la fenêtre **Exclusions de sites Internet**. Le Contrôle Parental va interdire l'accès aux sites repris dans la liste conformément aux paramètres définis.

➤ *Pour interdire le téléchargement de certains fichiers depuis Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Internet** ouvre la fenêtre de configuration du contrôle de l'utilisation d'Internet.
5. Dans le groupe **Restriction de téléchargement des fichiers**, cochez les cases en regard des types de fichiers dont le téléchargement sera interdit.

Le Contrôle Parental interdira le téléchargement des fichiers du type indiqué.

## CONTROLE DU LANCEMENT DES JEUX ET DES APPLICATIONS

Le Contrôle Parental permet d'autoriser ou d'interdire le lancement de jeux en fonction de l'âge de l'utilisateur. Vous pouvez également interdire l'exécution de certaines applications (par exemple, des jeux, des clients de messagerie instantanée) ou limiter la durée d'utilisation de celles-ci.

➤ *Pour interdire le lancement de jeux dont le contenu n'est pas adapté à l'âge de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Applications** ouvre la fenêtre de configuration du contrôle du lancement des applications.
5. Le groupe **Bloquer les jeux selon le contenu** permet d'interdire le lancement de jeux qui en conviennent pas à l'utilisateur en fonction de leur contenu et/ou de l'âge de l'utilisateur :
  - a. Si vous souhaitez interdire le lancement de tous les jeux dont le contenu n'est pas adapté à l'âge de l'utilisateur, cochez la case **Bloquer les jeux selon l'âge** et définissez l'âge dans la liste déroulante à côté de la case.
  - b. Si vous souhaitez interdire le lancement des jeux dont le contenu appartient à une catégorie en particulier, procédez comme suit :
    - a. Cochez la case **Bloquer les jeux depuis les catégories pour les adultes**.
    - b. A l'aide du lien **Sélectionner les catégories des jeux**, ouvrez la fenêtre **Restrictions de lancement des jeux selon le contenu**.
    - c. Cochez les cases en regard des catégorie de contenu des jeux à interdire.

➤ *Pour restreindre le lancement d'une application en particulier, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.

4. Le lien **Configuration** du groupe **Applications** ouvre la fenêtre de configuration du contrôle du lancement des applications.
5. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter l'application** et sélectionnez le fichier exécutable de l'application dans la fenêtre qui s'ouvre.

L'application sélectionnée apparaît dans la liste dans le groupe **Bloquer les applications indiquées**. Kaspersky Internet Security l'ajoute automatiquement à la catégorie définie, par exemple *Jeux*.

6. Si vous souhaitez interdire le lancement d'une application, cochez la case en regard de son nom dans la liste. Vous pouvez également interdire le lancement de toutes les applications d'une catégorie définie en cochant la case en regard du nom de la catégorie dans la liste (par exemple, vous pouvez appliquer l'interdiction aux applications de la catégorie *Jeux*).
7. Si vous souhaitez introduire une limite sur la durée d'utilisation de l'application, sélectionnez l'application ou une catégorie d'applications dans la liste, puis cliquez sur le bouton **Configurer les règles**.

La fenêtre **Limites d'utilisation de l'application** s'ouvre.

8. Si vous souhaitez limiter la durée d'utilisation de l'application pendant les jours ouvrables et les jours de repos, cochez les cases dans les groupes **Jours ouvrables** et **Jours de repos** et établissez les limites d'utilisation à l'aide des listes déroulantes. Vous pouvez également définir les périodes exactes pendant lesquelles l'utilisateur peut ou ne peut pas utiliser l'application à l'aide de la matrice. La matrice s'affiche lorsque vous cliquez sur le bouton .
9. Si vous souhaitez définir des interruptions dans l'utilisation d'une application, cochez la case **Bloquer l'accès tous les** dans le groupe **Temps de repos** et définissez la longueur de la pause à l'aide de la liste déroulante.
10. Cliquez sur le bouton **Enregistrer**.

Le Contrôle Parental appliquera les restrictions définies lorsque l'utilisateur utilisera l'application.

## CONTROLE DES COMMUNICATIONS VIA LES RESEAUX SOCIAUX

Le Contrôle Parental permet de consulter les communications des utilisateurs des réseaux sociaux et de clients de messagerie instantanée et de bloquer les échanges avec certains contacts.

➤ *Pour configurer le contrôle des communications de l'utilisateur, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Messageries** ouvre la fenêtre de configuration du contrôle des communications de l'utilisateur.
5. Pour consulter les communications et, le cas échéant, bloquer certains contacts, procédez comme suit :
  - a. Dans le groupe **Contrôle de la correspondance**, choisissez l'option **Interdire la correspondance avec les contacts indiqués**.
  - b. Le lien **Contacts** ouvre la fenêtre **Contact**.

- c. Consultez la liste des contacts avec lesquels l'utilisateur a communiqué. Vous pouvez afficher des contacts en particulier dans la fenêtre à l'aide d'une des méthodes suivantes :
- Pour consulter les communications de l'utilisateur dans un réseau social en particulier ou dans un client de messagerie instantanée, sélectionnez l'élément requis dans la liste déroulante dans la partie supérieure de la fenêtre.
  - Pour afficher les contacts avec lesquels l'utilisateur communique le plus, sélectionnez l'option **Par nombre de messages** dans la liste déroulante **Tri**.
  - Pour afficher les contacts avec lesquels l'utilisateur a communiqué récemment, sélectionnez l'option **A partir des messages les plus récents** dans la liste déroulante **Tri**.
- d. Pour consulter les communications de l'utilisateur avec un contact en particulier, cliquez sur le contact dans la liste.
- La fenêtre **Historique de la correspondance** s'ouvre.
- e. Si vous souhaitez interdire les communications de l'utilisateur avec le contact sélectionné, cliquez sur le bouton **Bloquer**.

Le Contrôle Parental bloquera les communications entre l'utilisateur et le contact sélectionné.

## CONTROLE DU CONTENU DE LA CORRESPONDANCE

Le Contrôle Parental permet de voir si l'utilisateur partage des données personnelles (nom de famille, numéro de téléphone, numéro de carte de crédit) ou utilise des expressions clés (par exemple, du langage vulgaire) dans sa correspondance et de bloquer de tels messages.

➡ Pour configurer le contrôle du transfert de données personnelles, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.  
La section **Contrôle Parental** s'affiche dans la fenêtre.
3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.
4. Le lien **Configuration** du groupe **Contrôle du contenu** ouvre la fenêtre de configuration du contrôle des informations transmises.
5. Dans le groupe **Contrôle de transfert des données personnelles**, cochez la case **Interdire le transfert des données personnelles aux tierces personnes**.
6. Le lien **Modifier la liste des données personnelles** ouvre la fenêtre **Liste des données personnelles**.
7. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.  
La fenêtre d'ajout des données personnelles s'ouvre.
8. Saisissez les données personnelles (par exemple, un numéro de téléphone), dans le champ **Valeur**.
9. Pour ajouter une description des données personnelles (par exemple, "numéro de téléphone"), cliquez sur le lien requis dans le groupe **Types de données personnelles** ou saisissez la description dans le champ **Nom du champ**.
10. Cliquez sur le bouton **Ajouter**.

Les données personnelles apparaissent dans la liste de la fenêtre **Liste des données personnelles**. Le Contrôle Parental surveillera la mention des données personnelles indiquées dans les messages instantanés ou sur des sites Internet et les bloquera.

➤ *Pour configurer le contrôle de l'utilisation d'expressions clés dans la correspondance, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.

4. Le lien **Configuration** du groupe **Contrôle du contenu** ouvre la fenêtre de configuration du contrôle des informations transmises.

5. Dans le groupe **Contrôle de l'utilisation des mots clés**, cochez la case **Activer le contrôle de l'utilisation des mots clés**.

6. A l'aide du lien **Modifier la liste des mots clés**, ouvrez la fenêtre **Contrôle de l'utilisation des mots clés**.

7. Dans la partie inférieure de la fenêtre, cliquez sur le bouton **Ajouter**.

La fenêtre d'ajout du mot clé s'ouvre.

8. Saisissez l'expression clé dans le champ **Valeur**, puis cliquez sur le bouton **Ajouter**.

L'expression clé indiquée apparaît dans la liste des mots clés de la fenêtre **Contrôle de l'utilisation des mots clés**. Le Contrôle Parental interdira la diffusion des messages contenant l'expression clé indiquée via Internet ou les clients de messagerie instantanée.

## CONSULTATION DU RAPPORT SUR LES ACTIONS DE L'UTILISATEUR

Vous pouvez consulter les rapports sur les actions de chaque utilisateur pour lequel le Contrôle Parental a été configuré ainsi que pour chaque catégorie d'événement contrôlé.

➤ *Pour consulter les rapports sur les actions de l'utilisateur contrôlé, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre, puis sélectionnez la section **Contrôle Parental**.

La section **Contrôle Parental** s'affiche dans la fenêtre.

3. Cliquez sur le lien désignant un compte utilisateur afin de consulter les statistiques d'activité de l'utilisateur sélectionné.

4. Dans le groupe reprenant le type de restrictions souhaitées (par exemple, **Internet** ou **Général**), ouvrez le rapport relatif aux actions contrôlées via le lien **Détails**.

Le rapport relatif aux actions contrôlées s'affiche.

## UTILISATION DU MODE JEUX POUR TRAVAILLER EN MODE PLEIN ECRAN

Lors du fonctionnement simultané de Kaspersky Internet Security avec certaines applications (surtout des jeux d'ordinateur) en mode plein écran, des inconvénients suivants peuvent survenir :

- le fonctionnement de l'application ou du jeu se ralentit à cause d'un manque des ressources de système ;
- les fenêtres des notifications de Kaspersky Internet Security distraient du jeu.

Pour ne pas modifier manuellement les paramètres de Kaspersky Internet Security avant chaque permutation en mode plein écran, vous pouvez utiliser le Mode Jeux. Quand le Mode Jeux est activé, les paramètres de tous les modules de Kaspersky Internet Security sont automatiquement modifiés quand l'utilisateur passe en mode plein écran afin de garantir le fonctionnement optimal dans ce mode. Au moment de quitter le mode plein écran, les paramètres de l'application reprennent les valeurs en vigueur au moment de passer en mode plein écran.

► Pour activer le Mode Jeu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre sélectionnez la section **Performance**.  
  
Les paramètres de performance de Kaspersky Internet Security apparaissent dans la fenêtre.
4. Dans le groupe **Mode Jeux**, cochez la case **Utiliser le Mode Jeux**.

## CREATION ET UTILISATION DU DISQUE DE DEPANNAGE

Le disque de dépannage représente l'application Kaspersky Rescue Disk enregistrée sur le support amovible (CD ou périphérique USB).

Vous pouvez utiliser Kaspersky Rescue Disk pour analyser et réparer l'ordinateur infecté dont la réparation par n'importe quel autre moyen est impossible (par exemple, à l'aide d'un logiciel antivirus).

### DANS CETTE SECTION

Création d'un disque de dépannage.....	<a href="#">63</a>
Démarrage de l'ordinateur à l'aide du disque de dépannage .....	<a href="#">65</a>

## CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier au format ISO) avec la version actuelle de l'application Kaspersky Rescue Disk et son enregistrement sur le support amovible.

L'image du disque de départ peut être téléchargée du serveur de Kaspersky Lab ou copiée depuis une source locale.

- Le disque de dépannage est créé à l'aide de l'*Assistant de création et d'enregistrement de Kaspersky Rescue Disk*. Le fichier de l'image rescuedisk.iso créé par l'Assistant est enregistré sur le disque dur de l'ordinateur.

➤ Pour lancer l'Assistant de création et d'enregistrement Kaspersky Rescue Disk, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Cliquez sur le bouton  dans la partie inférieure de la fenêtre principale, puis sélectionnez la section **Outils**.
3. Dans la fenêtre ouverte dans le groupe **Kaspersky Rescue Disk**, cliquez sur le bouton **Créer**.

L'Assistant se compose d'une série de fenêtres (étapes) entre lesquelles vous pouvez naviguer grâce aux boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le bouton **Terminer**. Pour interrompre l'Assistant à n'importe quelle étape, cliquez sur le bouton **Annuler**.

Examinons en détails les étapes de l'Assistant.

### Etape 1. Guide de démarrage de l'Assistant. Recherche d'une image de disque existante

La première fenêtre de l'Assistant reprend les informations sur l'application Kaspersky Rescue Disk. Pour continuer l'Assistant, cliquez sur **Suivant**. L'Assistant passera à la fenêtre **Sélection de la source de l'image du disque**.

### Etape 2. Sélection de la source de l'image du disque

Cette étape vous oblige à sélectionner une source de l'image du disque parmi les options proposées :

- Sélectionnez l'option **Télécharger l'image depuis les serveurs de Kaspersky Lab** si vous n'avez pas de fichier de l'image du disque de dépannage afin de le télécharger depuis le serveur de Kaspersky Lab (le fichier pèse environ 175 Mo).
- Si vous possédez déjà une image de disque de dépannage, sélectionnez l'option **Utiliser l'image de disque existante**.
- Sélectionnez l'option **Copier l'image sur le disque local ou réseau** si vous possédez déjà une image du disque de dépannage ou son image (fichier au format ISO) et qu'elle se trouve sur l'ordinateur ou sur une ressource du réseau local.

Cliquez sur le bouton **Parcourir**. Après avoir indiqué le chemin d'accès au fichier, cliquez sur **Suivant**.

### Etape 3. Copie (téléchargement) de l'image du disque

Si dans la fenêtre précédente de l'Assistant vous aviez choisi l'option **Utiliser l'image de disque existante**, alors cette étape est ignorée.

Une fois que la copie ou le téléchargement de l'image de disque sera terminé, l'Assistant passera automatiquement à l'étape suivante.

### Etape 4. Mise à jour du fichier de l'image du disque

La procédure de mise à jour du fichier de l'image du disque reprend les actions suivantes :

- la mise à jour des bases de l'application ;
- la mise à jour des fichiers de configuration.

Les fichiers de configuration déterminent la possibilité de charger l'ordinateur depuis le support amovible (par exemple, CD/DVD ou périphérique USB avec Kaspersky Rescue Disk) créé à l'aide de l'Assistant.

Lors de la mise à jour des bases de l'application, les bases obtenues suite à la mise à jour la plus récente de Kaspersky Internet Security sont utilisées. Si les bases sont dépassées, il est conseillé de réaliser une mise à jour, de relancer l'Assistant de création et d'enregistrement de Kaspersky Rescue Disk.

Pour lancer la mise à jour du fichier, cliquez sur **Suivant**. La fenêtre de l'Assistant illustrera la progression de la mise à jour.

## Etape 5. Enregistrement de l'image du disque sur un support

Cette étape de l'Assistant vous informera que la création de l'image du disque a réussi et proposera d'enregistrer l'image du disque sur le support.

Désignez le support pour l'enregistrement de Kaspersky Rescue Disk :

- Pour l'enregistrement sur un CD/DVD, choisissez l'option **Graver sur un CD/DVD**.
- Pour l'enregistrement sur un périphérique USB, choisissez l'option **Enregistrer sur un périphérique USB**.

Kaspersky Lab déconseille d'enregistrer l'image de disque sur un périphérique qui n'est pas prévu exclusivement pour le stockage de données, comme un smartphone, un téléphone mobile, un ordinateur de poche ou un lecteur MP3. L'enregistrement de l'image de disque sur de tels périphériques pourrait nuire au fonctionnement ultérieur de ceux-ci.

- Pour enregistrer sur un disque dur de votre ordinateur ou d'un autre ordinateur accessible via le réseau, choisissez l'option **Enregistrer l'image dans le fichier sur le disque local ou réseau**.

## Etape 6. Sélection du périphérique/du fichier pour l'enregistrement de l'image de disque

Cette étape de l'Assistant propose d'indiquer le chemin d'accès au périphérique/au fichier dans lequel l'image du disque va être enregistrée.

- Si vous aviez choisi l'option **Graver sur un CD/DVD** à l'étape précédente, sélectionnez le disque sur lequel vous souhaitez enregistrer l'image dans la liste déroulante.
- Si vous aviez choisi l'option **Enregistrer sur un périphérique USB** à l'étape précédente, sélectionnez le périphérique sur lequel vous souhaitez enregistrer l'image dans la liste déroulante.
- Si vous aviez choisi l'option **Enregistrer l'image dans le fichier sur le disque local ou réseau** à l'étape précédente, désignez le dossier dans lequel vous souhaitez enregistrer l'image ou le nom du fichier au format ISO.

## Etape 7. Enregistrement de l'image du disque sur un périphérique ou dans un fichier

Cette étape affiche la progression de l'enregistrement de l'image du disque sur le CD/DVD, sur un périphérique USB ou dans un fichier.

## Etape 8. Fin de l'Assistant

Pour quitter l'Assistant, cliquez sur **Terminer**. Vous pouvez utiliser le disque de dépannage créé pour démarrer l'ordinateur, si, suite à des actions des virus et des programmes malveillants, il n'est pas possible de démarrer l'ordinateur et de lancer Kaspersky Internet Security en mode normal.

## DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Le chargement du système d'exploitation requiert le CD-/DVD- ou le périphérique USB contenant le programme Kaspersky Rescue Disk (cf. section "Création d'un disque de dépannage" à la page [63](#)).

Le lancement de l'ordinateur depuis un support amovible n'est pas toujours possible. C'est le cas par exemple si l'ordinateur appartient à des anciennes générations. Avant d'éteindre l'ordinateur en vue de le redémarrer depuis un support amovible, vérifiez si cette option est prise en charge par l'ordinateur.

➔ Pour démarrer l'ordinateur à l'aide du disque de dépannage, procédez comme suit :

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD ou depuis un périphérique USB (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).
2. Introduisez le CD/DVD dans le lecteur de l'ordinateur infecté ou connectez le périphérique USB contenant l'application Kaspersky Rescue Disk.
3. Redémarrez l'ordinateur.

Pour en savoir plus sur l'utilisation du disque de dépannage, consultez le guide de l'utilisateur de Kaspersky Rescue Disk.

## PROTECTION DE L'ACCES AUX PARAMETRES DE KASPERSKY INTERNET SECURITY A L'AIDE DU MOT DE PASSE

Il peut arriver que plusieurs personnes aux connaissances de l'outil informatique variées utilisent le même ordinateur. L'accès sans restriction de différents utilisateurs à l'administration de Kaspersky Internet Security et à ses paramètres peut déboucher sur une réduction du niveau de protection de l'ordinateur.

Pour limiter l'accès à l'application, vous pouvez définir un mot de passe d'administrateur et identifier les actions dont l'exécution ne pourra avoir lieu qu'après la saisie de ce mot de passe :

- configuration des paramètres de l'application ;
- arrêt de l'application ;
- suppression de l'application.

➔ Pour protéger l'accès à Kaspersky Internet Security à l'aide d'un mot de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour accéder à la section **Configuration**.
3. Dans la partie gauche de la fenêtre, sélectionnez la section **Général**, puis cliquez sur le lien **Installer la protection par mot de passe** afin d'ouvrir la fenêtre **Protection par mot de passe**.
4. Dans la fenêtre ouverte, remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.
5. Si vous souhaitez modifier un mot de passe existant, saisissez-le dans le champ **Ancien mot de passe**.
6. Indiquez dans le groupe de paramètres **Zone d'action du mot de passe** les actions dont l'exécution ne pourra avoir lieu qu'après la saisie du mot de passe.

Il est impossible de récupérer un mot de passe oublié. Si vous oubliez le mot de passe, il faudra contacter le Support Technique pour pouvoir accéder aux paramètres de Kaspersky Internet Security.

## SUSPENSION ET RESTAURATION DE LA PROTECTION DE L'ORDINATEUR

La suspension de la protection signifie la désactivation de tous ses modules pour un certain temps.

► Pour suspendre la protection de l'ordinateur, procédez comme suit :

1. Choisissez l'option **Suspendre la protection** dans le menu contextuel de l'icône de l'application dans la zone de notification.

La fenêtre **Suspension de la protection** s'ouvre (cf. ill. ci-dessous).



Illustration 8. Fenêtre **Suspension de la protection**

2. Dans la fenêtre **Suspension de la protection** sélectionnez la durée à l'issue de laquelle la protection sera à nouveau activée :
  - **Suspendre pendant la période indiquée** : la protection sera activée à l'issue de l'intervalle défini dans la liste déroulante ci-dessous.
  - **Suspendre jusqu'au redémarrage** : la protection sera activée après le redémarrage de l'application ou du système d'exploitation (si le lancement automatique de l'application est activé).
  - **Suspendre** : la protection sera activée lorsque vous déciderez de la rétablir.

► Pour reprendre la protection de l'ordinateur,

sélectionnez l'option **Reprendre la protection** dans le menu contextuel de l'icône de l'application dans la zone de notifications.

## RESTAURATION DES PARAMETRES STANDARDS DU FONCTIONNEMENT DE L'APPLICATION

A tout moment, vous pouvez restaurer les paramètres de Kaspersky Internet Security recommandés par Kaspersky Lab. La restauration des paramètres s'opère à l'aide de l'*Assistant de configuration de l'application*.

A l'issue de l'utilisation de l'Assistant, le niveau de protection *Recommandé* sera sélectionné pour tous les modules de la protection. Lors de la restauration du niveau de protection recommandé, vous pouvez enregistrer sélectivement les valeurs des paramètres configurés auparavant pour les modules de l'application.

► Pour lancer l'Assistant de configuration de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre.

La section **Configuration** apparaît dans la fenêtre.

3. Sélectionnez la section **Général**.

Les paramètres de configuration de Kaspersky Internet Security apparaissent dans la fenêtre.

4. La partie inférieure de la fenêtre permet de cliquer sur le lien **Restaurer les paramètres** (cf. ill. ci-après).

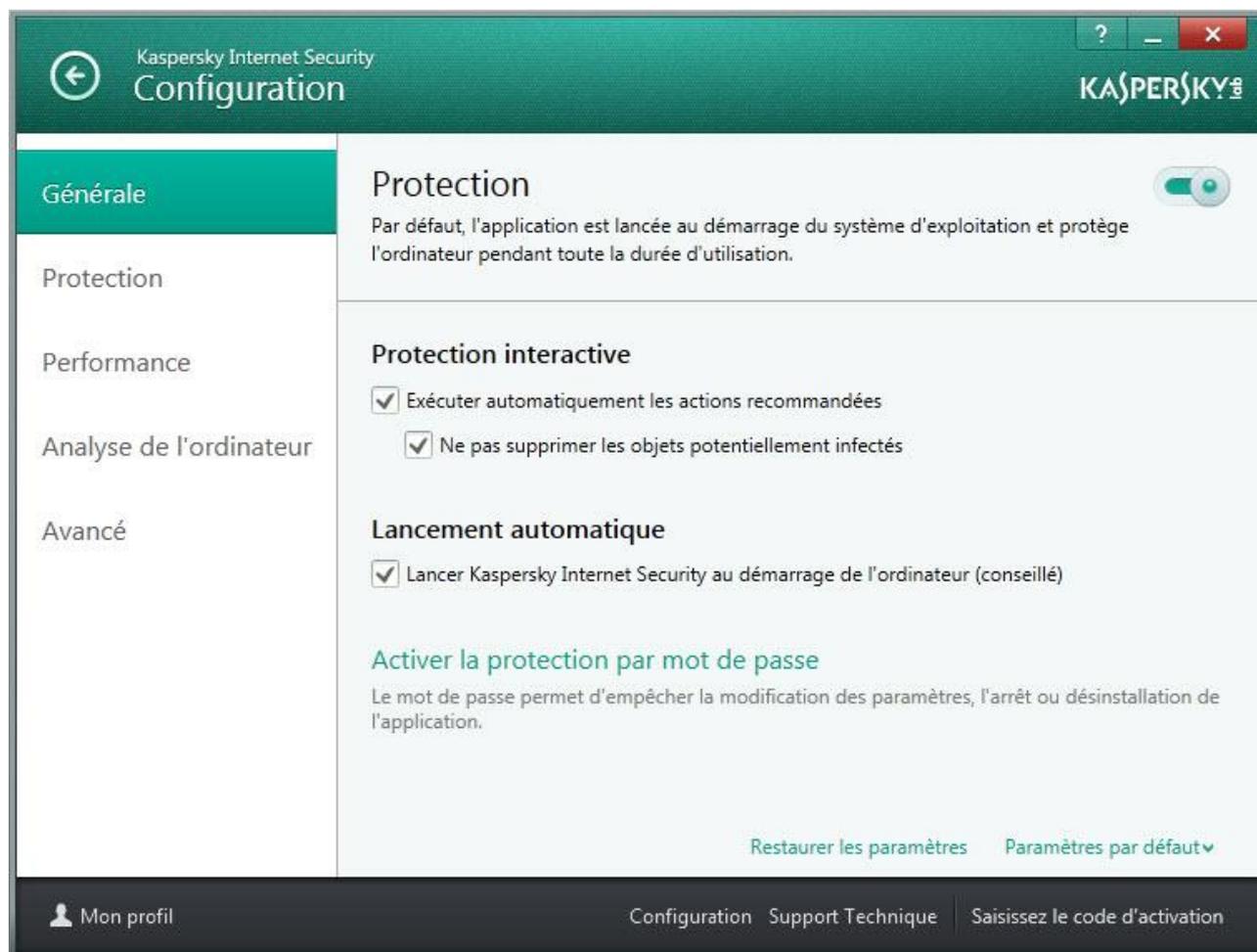


Illustration 9. Fenêtre **Configuration**, sous-section **Général**

Examinons en détails les étapes de l'Assistant.

## Etape 1. Guide de démarrage de l'Assistant

Cliquez sur le bouton **Suivant** afin de poursuivre l'Assistant.

## Etape 2. Restauration des paramètres

Cette fenêtre de l'Assistant reprend les modules de la protection de Kaspersky Internet Security dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky Internet Security durant l'entraînement des modules de la protection Pare-feu et Anti-Spam. Si des paramètres uniques ont été définis pour un module quelconque, ils figureront également dans la fenêtre (cf. ill. ci-après).

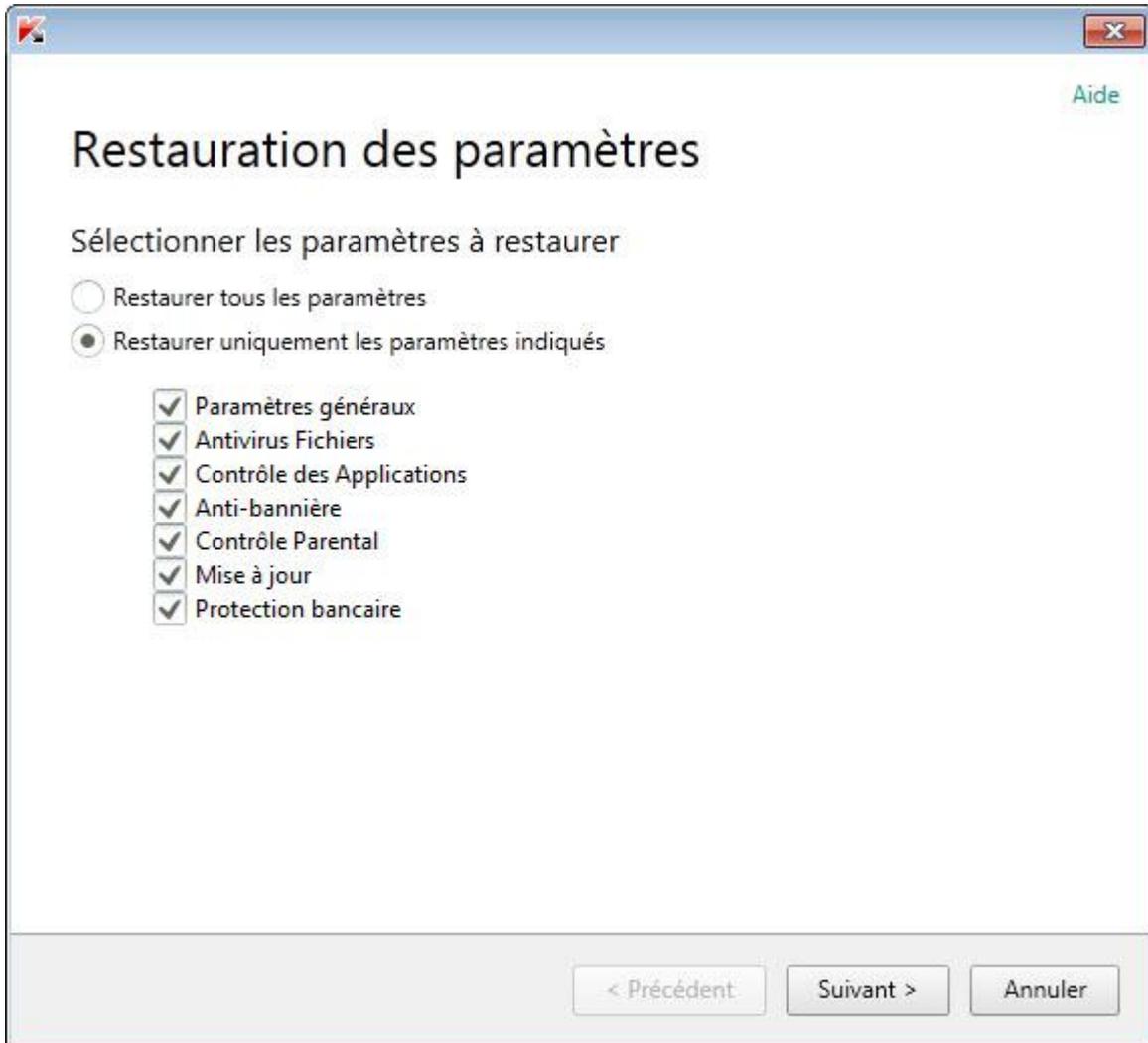


Illustration 10. Fenêtre **Restauration des paramètres**

Parmi les paramètres uniques, il y a les listes blanche et noire des expressions et des adresses utilisées par Anti-Spam, la liste des adresses Internet et des numéros d'accès de confiance, les règles d'exclusion pour les modules de l'application, les règles de filtrage des paquets et les règles des applications du Pare-feu.

Les paramètres uniques sont composés pendant l'utilisation de Kaspersky Internet Security et tiennent compte des tâches individuelles et des exigences de sécurité. Kaspersky Lab recommande d'enregistrer les paramètres uniques lors de la restauration des paramètres initiaux de l'application.

Cochez la case en regard des paramètres à enregistrer, puis cliquez sur le bouton **Suivant**.

## Etape 3. Analyse du système

Cette étape correspond à la collecte d'informations sur les applications reprises dans Microsoft Windows. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système.

Une fois l'analyse terminée, l'Assistant passe automatiquement à l'étape suivante.

## Etape 4. Fin de la restauration

Pour quitter l'Assistant, cliquez sur **Terminer**.

# CONSULTATION DU RAPPORT SUR L'UTILISATION DE L'APPLICATION

Kaspersky Internet Security génère des rapports sur le fonctionnement de chaque module de la protection. Ce rapport donne des données statistiques sur le fonctionnement de l'application (par exemple, nombre d'objets malveillants détectés et neutralisés pendant la période indiquée, nombre de fois que l'application a été actualisée, nombre de messages non sollicités détectés, etc.).

Si vous travaillez sur un ordinateur fonctionnant sous Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez consulter les rapports à l'aide du Kaspersky Gadget. Pour ce faire, il faut attribuer la fonction d'ouverture des rapports à un des boutons de Kaspersky Gadget.

➔ Pour consulter le rapport sur le fonctionnement du module, procédez comme suit :

- Ouvrez la fenêtre **Rapports** d'une des méthodes suivantes :
  - Sélectionnez la section **Rapports** dans la partie inférieure de la fenêtre principale de l'application.
  - Cliquez sur le bouton avec l'icône  **Rapports** dans l'interface de Kaspersky Gadget (uniquement pour les systèmes d'exploitation Microsoft Windows Vista et Microsoft Windows 7).

La fenêtre **Rapports** reprend les rapports sur le fonctionnement de l'application pour la journée en cours (partie gauche de la fenêtre) et pour la période définie (partie droite de la fenêtre).

- Si vous souhaitez consulter un rapport détaillé sur le fonctionnement de l'application, ouvrez la fenêtre **Rapport détaillé** via le lien **Tous les événements** situé dans la partie supérieure de la fenêtre **Rapports**.

La fenêtre **Rapport détaillé** présente les données sous forme d'un tableau. Pour faciliter la lecture du tableau, il est possible de regrouper les entrées du tableau selon différents critères.

## UTILISATION DE KASPERSKY GADGET

Si vous utilisez Kaspersky Internet Security sur un ordinateur tournant sous le système d'exploitation Microsoft Windows Vista ou Microsoft Windows 7, vous pouvez utiliser Kaspersky Gadget (ci-après *gadget*). Le gadget apparaît automatiquement sur le Bureau après l'installation de Kaspersky Internet Security sur un ordinateur fonctionnant sous Microsoft Windows 7. Après l'installation de l'application sur un ordinateur fonctionnant sous Microsoft Windows Vista, le gadget devra être ajouté manuellement au Volet Windows de Microsoft Windows (cf. la documentation du système d'exploitation).

L'indicateur de couleur du gadget signale l'état de la protection de votre ordinateur de la même manière que l'indicateur situé dans la fenêtre principale de l'application (cf. section "Analyse de l'état de protection de l'ordinateur et suppression des problèmes de sécurité" à la page [32](#)). La couleur verte indique que l'ordinateur est protégé, la couleur jaune signale un problème dans la protection, la couleur rouge indique une menace sérieuse pour la sécurité de l'ordinateur. La couleur grise de l'indicateur indique que le fonctionnement de l'application a été arrêté.

A l'aide du gadget, vous pouvez exécuter les actions suivantes :

- Restaurer le fonctionnement de l'application s'il a été suspendu.
- Ouvrir le menu principal de l'application.
- Rechercher la présence éventuelle de virus dans des objets en particuliers.
- Ouvrir la fenêtre de consultation des nouvelles.

Vous pouvez aussi configurer les boutons du gadget pour exécuter les actions complémentaires :

- lancer la mise à jour ;
- modifier les paramètres de fonctionnement de l'application ;
- consulter les rapports de l'application ;
- consulter les rapports du Contrôle Parental ;
- consulter les informations sur l'activité réseau (surveillance du réseau) et sur l'activité des applications ;
- suspendre la protection ;
- ouvrir le clavier virtuel ;
- ouvrir la fenêtre Gestionnaire des tâches.

➤ *Pour lancer l'application à l'aide du gadget,*

cliquez sur l'icône  **Activer** située au milieu du gadget.

➤ *Pour ouvrir la fenêtre principale de l'application à l'aide du gadget,*

cliquez sur l'image du moniteur au milieu du gadget.

➤ *Pour rechercher la présence éventuelle de virus à l'aide du gadget,*

faites glisser l'objet sur le gadget.

Le processus d'exécution de la tâche apparaîtra dans la fenêtre **Gestionnaire des tâches**.

➤ *Pour ouvrir la fenêtre de consultation des nouvelles à l'aide du gadget,*

cliquez sur l'icône  affichée au milieu du gadget quand une nouvelle est disponible.

➤ *Pour configurer le gadget, procédez comme suit :*

1. Ouvrez la fenêtre de configuration du gadget en cliquant sur l'icône  qui apparaît dans le coin supérieur droit du gadget lorsque le curseur est placé sur celui-ci.
2. Dans les listes déroulantes qui correspondent aux boutons du gadget, sélectionnez les actions à exécuter lorsque vous cliquez sur les boutons du gadget.
3. Cliquez sur le bouton **OK**.

## PARTICIPATION AU KASPERSKY SECURITY NETWORK (KSN)

Afin d'améliorer l'efficacité de la protection de votre ordinateur, Kaspersky Internet Security utilise les données obtenues auprès d'utilisateurs issus du monde entier. Le réseau Kaspersky Security Network permet de récolter ces données.

Kaspersky Security Network (KSN) est un ensemble de services en ligne qui permet d'accéder à la Base des connaissances de Kaspersky Lab sur la réputation des fichiers, des sites et des applications. Grâce aux données de Kaspersky Security Network, Kaspersky Internet Security peut réagir plus rapidement aux menaces inconnues. L'efficacité de certains modules est améliorée et la probabilité de faux positifs est réduite.

L'implication des utilisateurs dans le Kaspersky Security Network permet à Kaspersky Lab de recueillir efficacement des informations sur les nouvelles menaces et leurs sources, de développer des moyens de neutralisation et de réduire le nombre de faux positifs. La participation au Kaspersky Security Network vous donne accès aux données sur la réputation des applications et des sites Internet.

Lors du lancement de Kaspersky Internet Security après le redémarrage du système d'exploitation, l'application envoie à Kaspersky Security Network les informations sur la configuration de votre système et sur l'heure de lancement et de fin des processus de Kaspersky Internet Security.

## DANS CETTE SECTION

Activation et désactivation de la participation à Kaspersky Security Network .....	<a href="#">72</a>
Vérification de la connexion à Kaspersky Security Network.....	<a href="#">72</a>

## ACTIVATION ET DESACTIVATION DE LA PARTICIPATION A KASPERSKY SECURITY NETWORK

La participation au Kaspersky Security Network est volontaire. Vous pouvez activer ou désactiver l'utilisation de Kaspersky Security Network pendant l'installation de Kaspersky Internet Security et/ou à tout moment après l'installation de l'application.

➔ Pour activer ou désactiver la participation au Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Avancé**, choisissez le groupe **Kaspersky Security Network**.

Cette fenêtre affiche les informations relatives au Kaspersky Security Network (KSN) ainsi que les paramètres de participation au KSN.

4. Les boutons **Activer** / **Désactiver** permet d'activer ou de désactiver la participation au Kaspersky Security Network :
  - si vous voulez participer au Kaspersky Security Network, cliquez sur **Activer** ;
  - si vous ne voulez pas participer au Kaspersky Security Network, cliquez sur **Désactiver**.

## VERIFICATION DE LA CONNEXION A KASPERSKY SECURITY NETWORK

La connexion à Kaspersky Security Network peut être absente pour une des raisons suivantes :

- Vous ne participez pas au Kaspersky Security Network.
- Votre ordinateur n'est pas connecté à Internet.
- L'état actuel de la clé ne permet pas d'effectuer la connexion à Kaspersky Security Network.

L'état actuel de la clé s'affiche dans la fenêtre **Licence**.

➤ Pour vérifier la connexion à Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Configuration** dans la partie inférieure de la fenêtre principale de l'application pour ouvrir la fenêtre **Configuration**.
3. Dans la section **Avancé**, choisissez la sous-section **Kaspersky Security Network**.

La fenêtre indique l'état de la participation au Kaspersky Security Network.

## PARTICIPATION AU PROGRAMME "PROTEGE TON AMI"

Le programme "Protège ton ami" permet de publier dans Twitter et sur les pages dans les réseaux sociaux Facebook et Vkontakte le lien sur le téléchargement du distributif de Kaspersky Internet Security avec une période agrandie de présentation. Si votre ami dans Twitter, Facebook ou Vkontakte téléchargera le distributif de Kaspersky Internet Security à l'aide du lien que vous avez publié et s'il active l'application, vous recevrez les points. Les points accumulés peuvent être échangés sur le code d'activation offert de Kaspersky Internet Security.

La possibilité de participation au programme "Protège ton ami" peut être disponible non pas pour tous les utilisateurs.

En participant au programme "Protège ton ami", la popularité vous sera attribuée. La popularité dépend de la version de l'application et des fonctions et des modules de l'application que vous utilisez le plus souvent (par exemple, l'analyse, le Contrôle Parental, la Protection bancaire).

Pour participer au programme "Protège ton ami", il faut ouvrir la page Internet de votre profil dans le programme "Protège ton ami". La page Internet de votre profil est disponible à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre principale de Kaspersky Internet Security. Votre profil est créé automatiquement à la première entrée.

Pour entrer dans votre profil dans le programme "Protège ton ami", il faut s'autoriser à l'aide du compte Kaspersky Account. Si vous n'avez pas encore de compte Kaspersky Account, vous pouvez le créer à la première ouverture du profil dans le programme "Protège ton ami".

Sur la page Internet de votre profil dans le programme "Protège ton ami", vous pouvez exécuter les actions suivantes :

- consulter votre popularité dans le programme "Protège ton ami" et le nombre de points accumulés ;
- publier les liens sur le téléchargement du distributif de Kaspersky Internet Security ;
- modifier les propriétés de votre profil (l'image et le nom qui seront publiés dans Twitter, dans les réseaux sociaux et dans le blog avec le lien sur le téléchargement du distributif de Kaspersky Internet Security).

### DANS CETTE SECTION

Entrée dans votre profil dans le programme "Protège ton ami".....	<a href="#">74</a>
Comment partager le lien sur Kaspersky Internet Security avec les amis.....	<a href="#">75</a>
Echange des points sur le code d'activation offert .....	<a href="#">76</a>

## ENTREE DANS VOTRE PROFIL DANS LE PROGRAMME "PROTEGE TON AMI"

Pour entrer dans votre profil dans le programme "Protège ton ami", il faut s'autoriser à l'aide du compte Kaspersky Account. Si vous n'avez pas encore du compte Kaspersky Account, à la première entrée sur la page Internet du programme "Protège ton ami", vous devez créer Kaspersky Account.

Le compte Kaspersky Account représente l'adresse de votre courrier électronique et le mot de passe (au moins huit symboles) que vous avez indiqué lors de l'enregistrement.

Après la création du compte, vous recevrez à l'adresse indiquée du courrier électronique un message, contenant le lien pour activer votre compte Kaspersky Account.

Après l'activation, vous pouvez utiliser votre compte Kaspersky Account pour entrer sur la page de votre profil dans le programme "Protège ton ami".

➤ *Pour créer un compte Kaspersky Account, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application, puis passez dans la partie inférieure de la fenêtre à l'aide du lien **Mon profil**.

La page Internet du programme "Protège ton ami" s'ouvre. Cette page contient les champs pour l'enregistrement ou l'autorisation à l'aide de Kaspersky Account.

2. Créez et activez le compte Kaspersky Account :

- a. Dans la partie gauche de la page Internet, saisissez l'adresse du courrier électronique dans le champ **E-mail**.
- b. Saisissez le mot de passe et la confirmation du mot de passe dans les champs **Mot de passe** et **Confirmation du mot de passe**. Le mot de passe doit contenir au moins huit symboles.
- c. Cliquez sur le bouton **S'enregistrer**.

La page Internet affichera le message sur l'enregistrement réussi de Kaspersky Account. A l'adresse indiquée du courrier électronique, vous recevrez un message avec le lien à l'aide duquel il faut passer pour activer Kaspersky Account.

- d. Passez à l'aide du lien pour activer Kaspersky Account dans le message reçu.

La page Internet affichera le message sur l'activation réussie du compte Kaspersky Account. Vous pouvez utiliser le compte créé Kaspersky Account pour entrer dans votre profil du programme "Protège ton ami".

Si vous avez déjà un compte Kaspersky Account, vous pouvez l'utiliser pour entrer sur la page de votre profil.

➤ *Pour entrer sur la page du profil du programme "Protège ton ami", procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application, puis passez dans la partie inférieure de la fenêtre à l'aide du lien **Mon profil**.

La page Internet du programme "Protège ton ami" s'ouvre. Cette page contient les champs pour l'enregistrement ou l'autorisation à l'aide de Kaspersky Account.

2. La partie droite de la page Internet permet de saisir dans les champs l'adresse du courrier électronique et le mot de passe indiqués à l'enregistrement de Kaspersky Account.
3. Cliquez sur le bouton **Entrer**.

La page Internet affichera votre profil dans le programme "Protège ton ami".

## COMMENT PARTAGER LE LIEN SUR KASPERSKY INTERNET SECURITY AVEC LES AMIS

De la page Internet de votre profil dans le programme "Protège ton ami", vous pouvez publier le lien sur le téléchargement du distributif de Kaspersky Internet Security dans Twitter, ainsi que dans les réseaux sociaux Facebook et Vkontakte. Outre cela, vous pouvez insérer sur la page de votre site Internet ou du blog les informations sur votre profil dans le programme "Protège ton ami" avec le lien sur le distributif. Vous pouvez aussi envoyer le lien sur le téléchargement du distributif de Kaspersky Internet Security par courrier électronique ou à l'aide des clients de messagerie instantanée (par exemple, ICQ).

► *Pour publier le lien sur le téléchargement du distributif de Kaspersky Internet Security dans Twitter ou dans les réseaux sociaux, procédez comme suit :*

1. Ouvrez la fenêtre principale de Kaspersky Internet Security et passez à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre.

La page Internet d'autorisation dans le programme "Protège ton ami" s'ouvre.

2. Exécutez l'autorisation sur la page Internet à l'aide de votre compte Kaspersky Account.

La page Internet affichera les informations de votre profil dans le programme "Protège ton ami".

3. Dans la partie gauche de la page Internet, cliquez sur le bouton avec le logo du réseau social nécessaire (Facebook ou Vkontakte) ou Twitter.

La site Internet du réseau social sélectionné ou Twitter s'ouvre. Dans la file d'actualité de vos amis, le lien sur le téléchargement du distributif de Kaspersky Internet Security avec la période prolongée de l'utilisation gratuite sera publié. En cas de nécessité, vous pouvez saisir le texte complémentaire sous forme de publication.

Si l'entrée sur votre page dans le réseau social ou dans Twitter n'est pas exécutée, la page Internet d'autorisation s'ouvre.

► *Pour placer sur votre site Internet le widget Internet avec le lien sur le téléchargement du distributif de Kaspersky Internet Security, procédez comme suit :*

1. Ouvrez la fenêtre principale de Kaspersky Internet Security et passez à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre.

La page Internet d'autorisation dans le programme "Protège ton ami" s'ouvre.

2. Exécutez l'autorisation sur la page Internet à l'aide de votre compte Kaspersky Account.

La page Internet affichera les informations de votre profil dans le programme "Protège ton ami".

3. Dans la partie supérieure de la page Internet dans la liste déroulante **Partager**, sélectionnez l'élément **Recevoir le code du widget Internet**.

La fenêtre **Code du widget Internet**, contenant le code du widget Internet pour insérer sur la page de votre site Internet, s'ouvre.

Vous pouvez copier le code du widget Internet dans le presse-papiers et l'insérer dans le code html de la page de votre site Internet ou du blog.

► *Pour recevoir le lien pour télécharger le distributif de Kaspersky Internet Security pour transmettre par courrier électronique ou à l'aide du client de messagerie instantanée, procédez comme suit :*

1. Ouvrez la fenêtre principale de Kaspersky Internet Security et passez à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre.

La page Internet d'autorisation dans le programme "Protège ton ami" s'ouvre.

2. Exécutez l'autorisation sur la page Internet à l'aide de votre compte Kaspersky Account.

La page Internet affichera les informations de votre profil dans le programme "Protège ton ami".

3. Dans la partie gauche de la page Internet, passez à l'aide du lien **Recevoir le lien**.

La fenêtre **Lien sur le distributeur**, contenant le lien pour télécharger le distributeur de Kaspersky Internet Security, s'ouvre.

Vous pouvez copier le lien dans le presse-papiers et l'envoyer par courrier électronique ou à l'aide des clients de messagerie instantanée.

## ECHANGE DES POINTS SUR LE CODE D'ACTIVATION OFFERT

En participant au programme "Protège ton ami", vous pouvez recevoir le code d'activation offert de Kaspersky Internet Security, en accumulant un nombre concret des points. Les points sont calculés quand les utilisateurs activent Kaspersky Internet Security télécharger à l'aide du lien que vous avez partagé depuis votre profil.

Les codes d'activation offerts sont offerts dans les cas suivants :

- lors de l'activation simple de la version d'évaluation de Kaspersky Internet Security par l'utilisateur avec lequel vous avez partagé le lien ;
- lors de l'activation de la licence pour Kaspersky Internet Security version 2013 et suivante par l'utilisateur avec lequel vous avez partagé le lien.

La page Internet de votre profil permet de consulter l'historique d'accumulation des points et les informations sur les codes d'activation offerts à vous. Le code d'activation offert sera aussi envoyé à votre courrier électronique.

Le code d'activation offert peut être indiqué dans l'application en tant que code d'activation de réserve.

Le code d'activation offert peut être appliqué pour activer l'application sur un autre ordinateur (par exemple, vous pouvez l'offrir à un autre utilisateur).

L'application du code d'activation offert est impossible dans les cas suivants :

- L'application est utilisée par abonnement. Dans ce cas, vous pouvez appliquer le code d'activation offert après la fin de l'abonnement. Vous pouvez aussi appliquer le code d'activation offert sur un autre ordinateur.
- Le code d'activation de réserve est déjà indiqué dans l'application. Dans ce cas, vous pouvez appliquer le code d'activation offert à l'expiration de la durée de validité de la licence.

➡ *Pour recevoir le code d'activation offert et pour activer l'application avec son aide, procédez comme suit :*

1. Ouvrez la fenêtre principale de Kaspersky Internet Security et passez à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre.

La page Internet de votre profil dans le programme "Protège ton ami" s'ouvre.

2. Exécutez l'autorisation sur la page Internet à l'aide de votre compte Kaspersky Account.

La page Internet affichera les informations de votre profil dans le programme "Protège ton ami".

Vous pouvez consulter les informations sur les points accumulés dans le groupe **Mes points**. Si le nombre de points accumulés suffit pour recevoir un code d'activation offert, à côté du bouton **Obtenir un code d'activation offert**, une notification  s'affiche dans la partie droite de la page Internet .

3. Pour recevoir le code d'activation offert et pour activer l'application avec son aide, procédez comme suit :
  - a. Cliquez sur le bouton **Obtenir un code d'activation offert**.

Attendez l'obtention du code d'activation. Le code d'activation offert obtenu s'affiche dans la fenêtre ouverte.

- b. Cliquez sur le bouton **Activer**.

La fenêtre **Activation** s'ouvre avec le message sur la vérification du code d'activation. Après la vérification du code d'activation, la fenêtre avec le message sur l'activation réussie de Kaspersky Internet Security s'ouvre.

► *Pour consulter l'historique d'octroi des codes d'activation offerts et pour activer l'application avec le code d'activation offert, procédez comme suit :*

1. Ouvrez la fenêtre principale de Kaspersky Internet Security et passez à l'aide du lien **Mon profil** dans la partie inférieure de la fenêtre.

La page Internet de votre profil dans le programme "Protège ton ami" s'ouvre.

2. Exécutez l'autorisation sur la page Internet à l'aide de votre compte Kaspersky Account.

La page Internet affichera les informations de votre profil dans le programme "Protège ton ami".

3. Dans la partie inférieure de la page Internet, passez à l'aide du lien **Codes d'activation offerts**.

La fenêtre **Points** s'ouvre sous l'onglet **Codes d'activation offerts**.

4. Dans la liste des codes d'activation offerts reçus, cliquez sur le code d'activation à l'aide duquel vous voulez activer l'application.

La fenêtre, contenant le code d'activation offert, s'ouvre.

5. Cliquez sur le bouton **Activer**.

La fenêtre **Activation** s'ouvre avec le message sur la vérification du code d'activation. Après la vérification du code d'activation, la fenêtre avec le message sur l'activation réussie de Kaspersky Internet Security s'ouvre.

# CONTACTER LE SUPPORT TECHNIQUE

Cette section reprend les informations sur les différentes méthodes d'obtention du Support Technique et les conditions à remplir pour pouvoir bénéficier de l'aide du Support Technique.

## DANS CETTE SECTION

---

Modes d'obtention du Support Technique.....	78
Support Technique par téléphone.....	78
Obtention du Support Technique via Mon Espace Personnel.....	78
Utilisation du fichier de traçage et du script AVZ.....	79

## MODES D'OBTENTION DU SUPPORT TECHNIQUE

Si vous n'avez pas trouvé comment résoudre votre problème dans la documentation de l'application ou dans une des sources d'informations sur l'application (cf. section "Sources d'informations sur l'application" à la page 9), veuillez contacter le Support technique de Kaspersky Lab. Les experts du Support Technique répondront à vos questions sur l'installation et l'utilisation de l'application.

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

Vous pouvez contacter les experts du Support Technique d'une des manières suivantes :

- Via téléphone. Vous pouvez contacter les experts du Support Technique en France.
- Via une demande depuis Mon Espace Personnel sur le site Internet du Support Technique. Cette méthode permet de contacter les experts du Support Technique via un formulaire.

Le Support technique est uniquement accessible aux utilisateurs qui ont acheté une licence pour l'application. Les utilisateurs des versions d'évaluation n'ont pas droit au Support technique.

## SUPPORT TECHNIQUE PAR TELEPHONE

Si vous êtes confronté à un problème que vous ne parvenez pas à résoudre, vous pouvez contacter les experts du Support Technique francophones (<http://support2.kaspersky.com/us/support/contacts>).

Avant de contacter le service du Support Technique, veuillez prendre connaissances des Règles d'octroi du Support Technique (<http://support.kaspersky.com/fr/support/rules>). Ceci permettra nos experts à vous venir en aide le plus vite possible.

## OBTENTION DU SUPPORT TECHNIQUE VIA MON ESPACE PERSONNEL

*Mon Espace Personnel* est un espace qui vous est réservé (<https://my.kaspersky.com/fr>) sur le site du Support technique.

Pour pouvoir accéder à Mon Espace Personnel, vous devez vous inscrire sur la page d'enregistrement (<https://my.kaspersky.com/?logonSessionData=MyAccount&returnUrl=fr%2Findex.html>). Vous devrez saisir votre adresse de messagerie et un mot de passe d'accès à Mon Espace Personnel.

Mon Espace Personnel permet de réaliser les opérations suivantes :

- Envoyer des demandes au Support Technique et au laboratoire d'étude des virus.
- Communiquer avec le Support Technique sans devoir envoyer des messages électroniques.
- Suivre le statut de vos demandes en temps réel.
- Consulter l'historique complet de votre interaction avec le Support Technique.
- Obtenir une copie du fichier clé en cas de perte ou de suppression de celui-ci.

### **Demande adressée par email au Support Technique**

Vous pouvez envoyer une demande par email au Support Technique en anglais et en français.

Vous devez fournir les informations suivantes dans les champs du formulaire :

- type de demande ;
- nom et numéro de version de l'application ;
- texte de la demande ;
- numéro de client et mot de passe ;
- adresse de messagerie.

L'expert du Support Technique répond via Mon Espace Personnel et en envoyant un message électronique à l'adresse indiquée dans la demande.

### **Demande électronique adressée au laboratoire d'étude des virus**

Certaines demandes ne sont pas envoyées au Support Technique mais au laboratoire d'étude des virus.

Vous pouvez envoyer au Laboratoire d'étude des virus les demandes sur la recherche des fichiers suspects ou des ressources Internet. Vous pouvez aussi s'y adresser dans les cas des faux positifs de Kaspersky Internet Security sur les fichiers que vous considérez comme dangereux.

Vous pouvez également envoyer une demande au laboratoire d'étude des virus depuis le formulaire de demande (<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>), sans vous enregistrer dans Mon Espace Personnel. Dans ce cas, vous ne devez pas indiquer le code d'activation de l'application.

## **UTILISATION DU FICHIER DE TRAÇAGE ET DU SCRIPT AVZ**

Après avoir signalé le problème aux experts du Support Technique, ceux-ci peuvent vous demander de composer un rapport reprenant les informations relatives au système d'exploitation et de l'envoyer au Support Technique. Les experts du Support Technique peuvent vous demander également de créer un *fichier de traçage*. Le fichier de traçage permet de suivre le processus d'exécution des instructions de l'application pas à pas et de découvrir à quel moment l'erreur survient.

L'analyse des données que vous envoyez permet aux experts du Support Technique de créer et de vous envoyer un script AVZ. L'exécution de scripts AVZ permet d'analyser les processus exécutés à la recherche de code malveillant, de rechercher la présence de code malveillant dans le système, de réparer ou de supprimer les fichiers infectés ou de composer des rapports sur les résultats de l'analyse du système.

**DANS CETTE SECTION**

Création d'un rapport sur l'état du système .....	<a href="#">80</a>
Envoi des fichiers de données .....	<a href="#">80</a>
Exécution du script AVZ.....	<a href="#">81</a>

**CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME**

➤ *Pour créer un rapport sur l'état du système, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre ouverte, cliquez sur le lien **Surveillance des problèmes**.  
La fenêtre **Surveillance des problèmes** s'ouvre.
4. Dans la fenêtre ouverte, cliquez sur le lien **Créer un rapport sur le système**.

Le rapport sur l'état du système est généré au format HTML et XML et il est enregistré dans l'archive sysinfo.zip. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

➤ *Pour consulter le rapport, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre ouverte, cliquez sur le lien **Surveillance des problèmes**.  
La fenêtre **Surveillance des problèmes** s'ouvre.
4. Dans la fenêtre ouverte, cliquez sur le lien **Consulter le rapport**.  
La fenêtre de l'Assistant de Microsoft Windows s'ouvre.
5. Dans la fenêtre ouverte, ouvrez l'archive sysinfo.zip qui contient les fichiers du rapport.

**ENVOI DES FICHIERS DE DONNEES**

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du Support Technique de Kaspersky Lab.

Pour charger les fichiers sur le serveur du Support Technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans Mon Espace Personnel sur le site Internet du Support Technique lorsque des requêtes actives sont présentes.

► Pour télécharger les fichiers de données sur le serveur du Support Technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre ouverte, cliquez sur le lien **Surveillance des problèmes**.  
La fenêtre **Surveillance des problèmes** s'ouvre.
4. Dans la fenêtre ouverte, cliquez sur le lien **Envoyer les informations de service au Service du Support technique**.  
La fenêtre **Envoi du rapport** s'ouvre.
5. Cochez les cases en regard des données que vous souhaitez envoyer au Support Technique.
6. Cliquez sur le bouton **Envoyer le rapport**.

Les fichiers de données sélectionnés seront compressés et envoyés sur le serveur du Support Technique.

S'il n'est pas possible pour une raison quelconque de contacter le Support Technique, vous pouvez enregistrer les fichiers de données sur votre ordinateur et les envoyer plus tard depuis Mon Espace Personnel.

► Pour enregistrer les fichiers de données sur le disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre ouverte, cliquez sur le lien **Surveillance des problèmes**.
4. La fenêtre **Surveillance des problèmes** s'ouvre.
5. Dans la fenêtre ouverte, cliquez sur le lien **Envoyer les informations de service au Service du Support technique**.  
La fenêtre **Envoi du rapport** s'ouvre.
6. Cochez les cases en regard des données que vous souhaitez envoyer au Support Technique.
7. Passez à l'aide du lien **Enregistrer le rapport**.  
La fenêtre d'enregistrement des archives s'ouvre.
8. Saisissez le nom de l'archive et confirmez l'enregistrement.

Vous pouvez envoyer l'archive créée au Support Technique via Mon Espace Personnel.

## EXECUTION DU SCRIPT AVZ

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le Support technique (cf. section "Modes d'obtention du Support Technique" à la page 78).

➡ *Pour exécuter le script AVZ, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.
2. Cliquez sur le lien **Support Technique** situé dans la partie inférieure de la fenêtre afin d'ouvrir la fenêtre **Support Technique**.
3. Dans la fenêtre ouverte, cliquez sur le lien **Surveillance des problèmes**.

La fenêtre **Surveillance des problèmes** s'ouvre.

4. Dans la fenêtre ouverte, cliquez sur le lien **Exécuter le script**.

La fenêtre **Exécution du script** s'ouvrira.

5. Copiez le texte du script, reçu en provenance des experts du Support Technique, insérez-le dans le champ de saisie dans la fenêtre ouverte et cliquez sur le bouton **Suivant**.

L'exécution du script sera lancée.

Si l'exécution du script réussit, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

# GLOSSAIRE

## A

### **ACTIVATION DE L'APPLICATION**

L'application devient entièrement fonctionnelle. L'utilisateur réalise l'activation pendant ou après l'installation de l'application. Pour pouvoir activer l'application, l'utilisateur doit disposer d'un code d'activation.

### **ANALYSE DU TRAFIC**

Analyse en temps réel des objets transitant par tous les protocoles (exemple : HTTP, FTP et autres), à l'aide de la dernière version des bases.

### **ANALYSEUR HEURISTIQUE**

Technologie de détection des menaces dont les définitions ne figurent pas encore dans les bases de Kaspersky Lab. L'analyseur heuristique permet de détecter les objets dont le comportement dans le système peut présenter une menace de la sécurité. Les objets identifiés à l'aide de l'analyseur heuristique sont considérés comme potentiellement infectés. Par exemple, un objet contenant une succession d'instructions propres aux objets malveillants (ouverture d'un fichier, écriture dans le fichier) peut être considéré comme étant potentiellement infecté.

### **APPLICATION INCOMPATIBLE**

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Internet Security.

## B

### **BASE DES URL DE PHISHING**

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

### **BASE DES URL MALVEILLANTES**

Liste des d'adresses des sites Internet dont le contenu pourrait constituer une menace. La liste est composée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

### **BASES**

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 permettent de détecter le code malveillant dans les objets analysés. Ces bases sont créées par les experts de Kaspersky Lab et mises à jour toutes les heures.

### **BLOPAGE D'UN OBJET**

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

## C

### **CLASSEMENT DE L'UTILISATEUR**

Le niveau d'activité de l'utilisateur lors de l'utilisation de Kaspersky Internet Security. Le classement de l'utilisateur s'affiche dans le profil de l'utilisateur et dépend des paramètres et de la version utilisée de l'application.

### **CODE D'ACTIVATION**

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

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

## **CODE D'ACTIVATION OFFERT**

Le code d'activation de Kaspersky Internet Security offert à l'utilisateur en échange des points.

## **COURRIER INDESIRABLE**

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

## **COURRIER INDESIRABLE POTENTIEL**

Message qui ne peut être considéré comme courrier indésirable de manière certaine mais qui possède certaines caractéristiques du courrier indésirable (par exemple, certains types d'envois et de messages publicitaires).

## **D**

### **DEGRE DE MENACE**

L'indice de probabilité avec laquelle le programme d'ordinateur peut présenter une menace pour le système d'exploitation. Le degré de menace est calculé à l'aide de l'analyse heuristique sur la base des critères de deux types :

- statiques (par exemple, les informations sur le fichier exécutable de l'application : la taille du fichier, la date de création, etc.) ;
- dynamiques qui sont appliqués pendant la simulation du fonctionnement de l'application dans l'environnement virtuel (l'analyse des fonctions de système appelées par l'application).

Le degré de menace permet d'identifier le comportement typique aux applications malveillantes. Plus le degré de menace est bas, plus le nombre d'actions autorisées pour l'application est élevé.

### **DUREE DE VALIDITE DE LA LICENCE**

Période au cours de laquelle vous pouvez utiliser les fonctions de l'application et les services complémentaires.

## **E**

### **ENREGISTREUR DE FRAPPES**

L'application conçue pour l'enregistrement masqué des informations sur les touches que l'utilisateur appuie pendant son travail sur l'ordinateur. Les enregistreurs de frappes sont aussi appelés les claviers-espions ou keyloggers.

## **F**

### **FAUX POSITIF**

Situation où un objet sain est considéré comme infecté par l'application de Kaspersky Lab car son code évoque celui d'un virus.

### **FICHIER COMPRESSE**

Fichier d'archivage contenant un programme de décompression ainsi que des instructions du système d'exploitation nécessaires à son exécution.

## **G**

### **GROUPE DE CONFIANCE**

Groupe dans lequel Kaspersky Internet Security place une application ou un processus en fonction de l'existence d'une signature numérique pour l'application, de la réputation de l'application dans KSN, de la fiabilité de la source de l'application et du danger potentiel des actions exécutées par l'application ou le processus. Sur la base de l'appartenance de l'application au groupe de confiance, Kaspersky Internet Security peut imposer des restrictions sur les actions de l'application en question dans le système.

Kaspersky Internet Security prévoit les groupes de confiance suivants : De confiance, Restrictions faibles, Restrictions élevées et Douteuses.

## K

### **KASPERSKY SECURITY NETWORK (KSN)**

L'infrastructure des services en ligne et des services offrant l'accès à la base opérationnelle de connaissance de Kaspersky Lab sur la réputation des fichiers, des ressources Internet et du logiciel. L'utilisation des données de Kaspersky Security Network assure une vitesse de réaction plus élevée des applications de Kaspersky Lab face aux menaces inconnues, augmente l'efficacité de fonctionnement de certains modules de la protection et réduit la possibilité de faux positifs.

## M

### **MASQUE DE FICHIER**

Représentation du nom d'un fichier par des caractères génériques. Les deux caractères principaux utilisés dans les masques de fichiers sont \* et ? (où \* représente n'importe quel nombre de n'importe quel caractère et ? représente un caractère unique).

### **MISE A JOUR**

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules de l'application), récupérés sur les serveurs de mises à jour de Kaspersky Lab.

### **MODULES DE L'APPLICATION**

Fichiers qui font partie de la distribution d'une application de Kaspersky Lab et qui sont responsables de la réalisation des tâches principales. Chaque type de tâche exécutée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) a son propre module exécutable. En lançant l'analyse complète de votre ordinateur depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

### **MODULES DE LA PROTECTION**

Les parties de Kaspersky Internet Security, conçues pour protéger l'ordinateur contre des différents types de menaces (par exemple, Anti-Spam, Anti-Phishing). Chaque module de la protection est relativement indépendant des autres modules et peut être désactivé ou configuré séparément.

## N

### **NIVEAU DE PROTECTION**

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du module de l'application.

## O

### **OBJET INFECTE**

Objet dont une partie du code correspond parfaitement à une partie du code d'un programme connu présentant une menace. Les experts de Kaspersky Lab déconseillent de manipuler de tels objets.

### **OBJET POTENTIELLEMENT INFECTE**

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

### **OBJETS DE DEMARRAGE**

Ensemble d'applications indispensables au lancement et au fonctionnement correct du système d'exploitation et du logiciel de votre ordinateur. Le système d'exploitation lance ces objets à chaque démarrage. Il existe des virus capables d'infecter les objets de démarrage, ce qui peut entraîner, par exemple, le blocage du lancement du système d'exploitation.

## OUTIL DE DISSIMULATION D'ACTIVITE

Programme ou ensemble de programmes qui permet de dissimuler la présence de l'individu malintentionné ou du programme malveillant dans le système.

Dans les systèmes Windows, tout programme qui s'infiltré dans le système et intercepte les fonctions système (Windows API) est considéré comme rootkit. L'interception et la modification de fonctions API de bas niveau permet avant tout à ce genre de programme de bien masquer sa présence dans le système. De plus, en général, un rootkit masque la présence dans le système de n'importe quel processus, dossier ou fichier sur le disque ou clé de registre décrit dans sa configuration. De nombreux rootkits installent leurs pilotes et services dans le système (ils sont aussi invisibles).

## P

### PAQUET DE MISE A JOUR

Paquet de fichiers pour la mise à jour des modules de l'application. L'application de Kaspersky Lab copie les paquets de mise à jour depuis les serveurs de mises à jour de Kaspersky Lab, puis les installe et les applique automatiquement.

### PARAMETRES DE LA TACHE

Les paramètres de fonctionnement de l'application, spécifiques à chaque type de tâches.

### PHISHING

Type d'escroquerie sur Internet qui consiste à envoyer aux victimes potentielles des messages électroniques, prétendument envoyés en général par une banque, dans le but d'obtenir des informations confidentielles.

### POINTS

Points octroyés par Kaspersky Lab aux utilisateurs qui participent à la campagne "Protège ton ami". Un utilisateur obtient des points lorsqu'il publie un lien vers un produit de Kaspersky Lab sur un réseau social ou dans un message et si un de ces amis télécharge la distribution et active l'application via ce lien.

### PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Lors de la détection d'une activité suspecte du processus de confiance, Kaspersky Internet Security exclut ce processus depuis la liste des processus de confiance et bloque ses actions.

### PROFIL DE L'UTILISATEUR

Informations générales sur la participation de l'utilisateur à la campagne "Protège ton ami". Le profil de l'utilisateur contient la popularité de l'utilisateur, le nombre de points bonus octroyés à l'utilisateur, le lien vers la page de téléchargement de Kaspersky Internet Security et les codes d'activation offerts à l'utilisateur.

### PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter : HTTP, FTP et NNTP.

## Q

### QUARANTAINE

Le stockage spécial dans lequel l'application place les copies de sauvegarde des fichiers, modifiés ou supprimés lors de la réparation. Les copies des fichiers sont conservées au format spécial et ne représentent aucun danger pour l'ordinateur.

## S

### SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Internet.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

### SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Il contient des informations relatives au système de fichiers du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et de les réparer en cas d'infection.

### SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Serveurs HTTP de Kaspersky Lab d'où l'application de Kaspersky Lab récupère la mise à jour des bases et des modules de l'application.

### SIGNATURE NUMERIQUE

Bloc de données cryptées qui fait partie d'un document ou d'une application. La signature numérique permet d'identifier l'auteur du document ou de l'application. Afin de pouvoir créer une signature numérique, l'auteur du document ou de l'application doit posséder un certificat numérique qui confirme l'identité de l'auteur.

La signature numérique permet de vérifier la source et l'intégrité des données et offre une protection contre les faux.

## T

### TECHNOLOGIE ICHECKER

La technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases de l'application et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases de l'application, l'archive sera analysée à nouveau.

Limitations technologiques d'iChecker :

- La technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse.
- La technologie prend en charge le nombre limité de formats.

### TRAÇAGES

Exécution de débogage de l'application au cours duquel un arrêt a lieu après l'exécution de chaque étape afin d'en afficher les résultats.

## **TACHE**

Fonctions exécutées par l'application de Kaspersky Lab sous la forme des tâches, par exemple : Protection en temps réel des fichiers, Analyse complète de l'ordinateur, Mise à jour des bases.

## **V**

### **VIRUS**

Le programme qui infecte d'autres programmes : y ajoute son propre code pour obtenir l'administration lors du lancement des fichiers infectés. Cette définition simple permet de révéler l'action principale exécutée par le virus - l'infection.

### **VIRUS INCONNU**

Nouveau virus au sujet duquel aucune information ne figure dans les bases. En général, l'application détecte les virus inconnus dans les objets à l'aide de l'analyse heuristique. Ces objets obtiennent l'état potentiellement infecté.

### **VULNERABILITE**

Le manque dans le système d'exploitation ou dans le programme qui peut être utilisé par les éditeurs du logiciel malveillant pour pénétrer dans le système ou dans le programme et pour nuire son intégrité. Un grand nombre de vulnérabilités dans le système fait en sorte que le fonctionnement du système soit fragile parce que les virus, installés dans le système, peuvent amener aux échecs dans le fonctionnement du système et des programmes installés.

# 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 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 logiciels antivirus pour ordinateurs de bureau et ordinateurs portables ainsi que des applications pour la protection des ordinateurs de poche, des smartphones et d'autres appareils nomades.

La société offre également des services pour la protection des postes de travail, des serveurs de fichiers, des serveurs 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 antivirus 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 (Russie), SonicWALL (USA), WatchGuard Technologies (É-U), ZyXEL Communications (Taïwan). De nombreuses technologies novatrices développées par la société sont brevetées.

**Réalisations.** 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 de Kaspersky Lab :

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

Encyclopédie Virus :

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

Laboratoire de virus :

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (uniquement pour l'envoi d'objets suspects sous forme d'archive)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr>

(pour les questions posées aux experts de la lutte contre les virus)

Forum de Kaspersky Lab :

<http://forum.kaspersky.com/index.php?showforum=105>

# INFORMATIONS SUR LE CODE TIERS

Les informations sur le code tiers sont reprises dans le fichier legal\_notices.txt situé dans le dossier d'installation de l'application.

# NOTICE SUR LES MARQUES DE COMMERCE

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

Google Chrome est une marque de Google, Inc.

ICQ est une marque ou une marque de service de ICQ LLC.

Intel et Pentium sont des marques déposées de Intel Corporation aux États-Unis et dans d'autres pays.

Bing, DirectX, Internet Explorer, Microsoft, Windows et Windows Vista – les marques Microsoft Corporation déposées aux États-Unis et aux autres pays.

Mozilla et Firefox sont des marques de Mozilla Foundation.

# INDEX

## A

Activation de l'application .....	30
Activation de l'application	
code d'activation .....	26
licence .....	25
version d'évaluation .....	18
Analyse de sécurité .....	32
Anti-Spam .....	40
Antivirus Courrier .....	40
Application.....	73, 76
Applications sécurisées.....	44

## B

Banque en ligne .....	51
Bases de l'application.....	33

## C

Clavier virtuel .....	47
Code	
code d'activation .....	26
Configuration logicielle .....	14
Configuration matérielle .....	14
Contrat de licence .....	25
Contrôle des Applications	
création de la règle pour l'application .....	42
exclusions.....	42
règles d'accès aux périphériques .....	42
Contrôle Parental .....	55
correspondance.....	61
lancement des applications .....	59
lancement des jeux.....	59
rapport .....	62
réseaux sociaux.....	60
utilisation de l'ordinateur .....	56
utilisation d'Internet.....	57
Courrier indésirable .....	40

## D

Diagnostic .....	32
Disque de dépannage .....	63

## E

Enregistreurs de frappes	
clavier virtuel.....	47
protection de la saisie au clavier.....	50
Etat de la protection .....	32

## F

Filtre Internet .....	54
-----------------------	----

**I**

Installation de l'application ..... 16

**K**

Kaspersky Account ..... 74  
 Kaspersky Gadget..... 70  
 Kaspersky Security Network ..... 71

**L**

Licence  
     code d'activation ..... 26  
     Contrat de licence..... 25

**M**

Menaces de sécurité ..... 32  
 Mise à jour..... 33  
 Mode des Applications sécurisées ..... 44  
 Mode jeux..... 63  
 Mode plein écran de fonctionnement des programmes ..... 63  
 Module d'analyse des liens  
     Antivirus Internet..... 54  
 Modules de l'application ..... 12

**N**

Notifications..... 31

**O**

Objet désactivé ..... 37  
 Outils complémentaires  
     disque de dépannage ..... 63  
     restauration après infection ..... 38

**P**

Problèmes de sécurité..... 32  
 Programmes inconnus ..... 41

**Q**

Quarantaine  
     restauration d'un objet ..... 37

**R**

Rapports..... 70  
 Recherche de vulnérabilités ..... 36  
 Restauration après infection..... 38  
 Restauration de l'objet..... 37  
 Restauration des paramètres par défaut ..... 67  
 Restriction de l'accès à l'application ..... 66

**S**

Source des mises à jour ..... 33  
 Statistiques..... 70  
 Suppression  
     application ..... 22  
 Suppression des traces d'activité ..... 52

**T**

Traçage	
création d'un fichier de trace.....	79
Traçages	
transfert des résultats du traçage .....	80

**V**

Vulnérabilité .....	36
---------------------	----