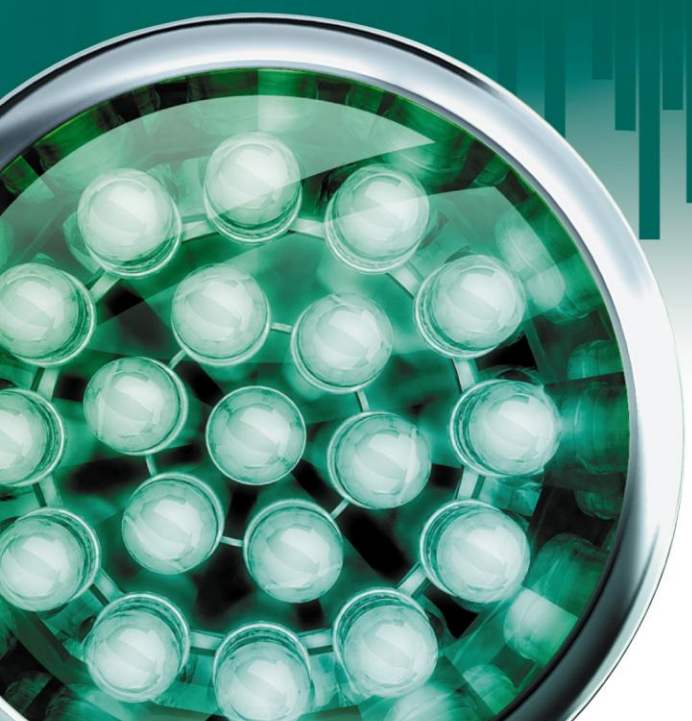
Kaspersky Mobile Security 9.0

GUIDE DE L'UTILISATEUR

VERSION DE L'APPLICATION : 9.0



KASPERSKY lab

Cher utilisateur,

Merci d'avoir choisi notre produit. Nous espérons que cette documentation vous sera utile dans votre travail et vous apportera toutes les réponses sur notre produit logiciel.

Ce document peut être modifié sans préavis. Pour obtenir la dernière version de ce document, reportez-vous au site de Kaspersky Lab à l'adresse http://www.kaspersky.com/fr/docs.

Date d'édition : 24.08.2010

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

CONTRAT DE LICENCE

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À ÊTRE LIÉ(E) PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LÀ À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

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

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

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

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

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

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

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

2.1. Le Titulaire des droits convient par la présente de Vous accorder une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (" l'utilisation ") du Logiciel sur un nombre spécifié d'Ordinateurs pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la " Licence ") et vous acceptez cette Licence :

Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre d'ordinateurs spécifiés dans les licences que vous avez obtenues auprès du Titulaire des droits,

sachant que, sauf disposition contraire du contrat de licence, chaque licence acquise vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acquis sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel ou stipulé dans le contrat additionnel.

2.3. Si le Logiciel a été acquis sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'acquisition de la Licence du Logiciel ou stipulé dans le contrat additionnel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acquis sur un support physique) ou stipulée pendant l'acquisition (si le Logiciel a été acquis sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acquis sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat ou celle stipulée dans le contrat additionnel.

3.3. Si le Logiciel a été acquis sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'acquisition ou celle stipulée dans le contrat additionnel.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone. Si le Titulaire des droits fixe une autre durée pour la période d'évaluation unique applicable, Vous serez informé(e) par notification.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acquis le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

3.10. Si vous avez acheté le logiciel avec un code d'activation valide pour la localisation de la langue parlée dans la région où il a été acquis auprès du détenteur des droits ou de ses partenaires, vous ne pouvez pas activer le logiciel avec le code d'activation prévu pour la localisation d'une autre langue.

3.11. Si vous avez acquis le logiciel prévu pour fonctionner avec un opérateur de télécommunications en particulier, ce logiciel n'est utilisable qu'en association avec l'opérateur indiqué au moment de l'acquisition.

3.12. En cas de restrictions précisées dans les clauses 3.10 et 3.11, vous trouverez des informations concernant ces restrictions sur l'emballage et/ou le site Web du détenteur et/ou de ses partenaires.

4. Assistance technique

L'assistance technique décrite dans la Clause 2.5 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).

Service d'assistance technique : http://support.kaspersky.com

5. Limitations

5.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune pièce du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

5.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans le contrat additionnel.

5.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans le contrat additionnel.

5.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

5.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

5.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

5.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

6. **Garantie limitée et avis de non-responsabilité**

6.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constatation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

6.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.

6.3. Vous reconnaissez, acceptez et convenez que le Titulaire des droits n'est pas responsable ou ne peut être tenu pour responsable de la suppression des données que vous autorisez. Les données mentionnées peuvent inclure des informations personnelles ou confidentielles.

6.4. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

6.5. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.5 de ce Contrat.

6.6. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

6.7. LE LOGICIEL EST FOURNI " TEL QUEL " ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PAR LA LÉGISLATION EN VIGUEUR, LE " COMMON LAW ", LA COUTUME, LES USAGES OU AUTRES) QUANT À

TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

7. Exclusion et Limitation de responsabilité

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

8. Licence GNU et autres licences de tierces parties

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (" Logiciel libre "). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

9. Droits de propriété intellectuelle

9.1 Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de

l'Union européenne et des États-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service du Titulaire des droits et/ou de ses partenaires (les " Marques de commerce "). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

9.2 Vous convenez que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.

9.3 Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

10. Droit applicable ; arbitrage

Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 10 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

11. Délai de recours

Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

12. Intégralité de l'accord ; divisibilité ; absence de renoncement

Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en équité de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

13. Coordonnées du Titulaire des droits

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie
Tél. :+7-495-797-8700
Fax : +7-495-645-7939
E-mail : info@kaspersky.com
Site Internet : www.kaspersky.com

TABLE DES MATIÈRES

KASPERSKY MOBILE SECURITY 9.0

Kaspersky Mobile Security 9.0 protège les appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile contre les menaces connues et nouvelles ainsi que contre les appels et les SMS indésirables. L'application contrôle les SMS et les appels sortants et l'activité de réseau et protège les données confidentielles contre l'accès non autorisé. Chaque type de menace est traité par un composant distinct de l'application. Cela permet de configurer en souplesse les paramètres de l'application en fonction des besoins d'un utilisateur particulier.

Kaspersky Mobile Security 9.0 reprend les composants suivants pour la protection :

- **Protection**. Protège le système de fichiers de l'appareil nomade contre l'infection. Le composant Protection, lancé au démarrage du système d'exploitation, est chargée en permanence dans la mémoire vive de l'appareil et analyse tous les fichiers ouverts, enregistrés et exécutés, y compris sur la carte mémoire. De plus, la Protection recherche la présence éventuelle de virus connus dans tous les fichiers entrants. Il sera possible d'utiliser le fichier uniquement si l'objet est simple ou s'il a pu être réparé.

- **Anti-Virus**. Permet de découvrir et de neutraliser les objets malveillants sur l'appareil. Il faut réaliser l'analyse de l'appareil à intervalles réguliers afin d'éviter la propagation d'objets malveillants qui n'auraient pas été découverts par la Protection.

- **Anti-Spam**. Analyse tous les SMS et appels entrants à la recherche de spam. Le composant peut bloquer tous les SMS et appels qu'il considère indésirable.

- **Contrôle Parental**. Contrôle les SMS et les appels sortants et interdit l'envoi de SMS et / ou la réalisation d'appels vers des numéros prédéfinis.

- **Antivol**. Protège les données de l'appareil contre l'accès non autorisé en cas de perte ou de vol. Le composant permet de verrouiller l'appareil à distance en cas de perte ou de vol, de supprimer les données confidentielles et de contrôler le remplacement de la carte SIM. Il permet également de définir les coordonnées géographiques de l'appareil (si celui-ci est doté d'un récepteur GPS).

- **Contacts personnels**. Dissimule les informations confidentielles de l'utilisateur pendant que l'appareil est utilisé par d'autres personnes. Le composant permet d'afficher ou de masquer toutes les informations liées aux numéros désignés, par exemple les données de la liste de contacts, les échanges de SMS et les entrées du journal des appels. Le composant permet également de dissimuler la réception des appels et de SMS entrants en provenance de numéros sélectionnés.

- **Pare-feu**. Contrôle les connexions de réseau de votre appareil mobile. Le composant permet de définir les connexions qui seront autorisées ou qui seront bloquées.

- **Chiffrement**. Protège les informations que la consultation par des tiers, même s'ils ont accès à l'appareil. Le composant peut crypter un nombre quelconque de dossiers qui ne sont pas définis par le système et enregistrés aussi bien dans la mémoire de l'appareil que sur les cartes mémoire. Les données du dossier sont accessibles uniquement après la saisie d'un code secret.

De plus, l'application propose les fonctions de service suivantes. Elles permettent de maintenir l'actualité de l'application, d'élargir les possibilités de celle-ci et de venir en aide à l'utilisateur durant l'utilisation.

- Mise à jour des bases antivirus de l'application. La fonction permet de tenir à jour les bases antivirus de Kaspersky Mobile Security 9.0.

- État de la protection. Les états des composants de l'application sont affichés. Les informations proposées permettent d'évaluer l'état actuel de la protection de l'appareil.

- Journal des événements. Un journal est tenu pour chaque composant. Ce journal des événements reprend les informations relatives au fonctionnement du composant (par exemple, opération exécutée, données sur l'objet bloqué, rapport sur l'analyse, la mise à jour, etc.).

- Licence. Au moment d'acheter Kaspersky Mobile Security 9.0, vous et Kaspersky Lab signez un contrat de licence qui vous donne le droit d'utiliser l'application, de recevoir les mises à jour des bases antivirus de l'application et de contacter le service d'assistance technique durant une période déterminée. La durée

d'utilisation ainsi que toute autre information requise pour le fonctionnement complet de l'application figurent dans la licence.

Grâce à la fonction **Licence**, vous pouvez obtenir des informations détaillées sur la licence que vous utilisez ainsi que renouveler la licence en cours.

Kaspersky Mobile Security 9.0 ne réalise pas de copies de sauvegarde des données en vue d'une restauration ultérieure.

DANS CETTE SECTION

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Mobile Security, vous pouvez trouver la réponse rapidement dans diverses sources d'informations sur l'application. Vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES DE DONNEES POUR DES CONSULTATIONS INDEPENDANTES

Vous disposez des informations suivantes sur le programme :

- la page de l'application sur le site de Kaspersky Lab ;
- la page du logiciel, sur le site du Support Technique (Base de connaissances) ;
- aide électronique et astuces ;
- documentation.

Page sur le site Web de Kaspersky Lab

http://www.kaspersky.com/fr/mobile_downloads

Sur cette page vous allez retrouver les informations générales sur Kaspersky Mobile Security 9.0, ses possibilités et ses particularités. Vous pouvez également acheter Kaspersky Mobile Security 9.0 dans notre boutique en ligne.

Page de l'application sur le site du Support Technique (Base de connaissances)

http://support.kaspersky.fr/

Cette page contient des articles publiés par les experts du Service d'assistance technique.

Ils contiennent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'acquisition, l'installation et l'utilisation de Kaspersky Mobile Security 9.0. Ces articles sont regroupés par sujet, par exemple " Utilisation des fichiers de licence ", " Mise à jour des bases " ou " Elimination des échecs ". Les articles répondent non seulement à des questions sur Kaspersky Mobile Security 9.0, mais aussi sur d'autres produits Kaspersky Lab ; ils peuvent contenir des informations générales récentes du Service d'assistance technique.

Système d'aide en ligne

En cas de question sur une fenêtre ou sur un onglet spécifiques de Kaspersky Mobile Security 9.0, vous disposez de l'aide contextuelle.

Pour accéder à l'aide contextuelle, ouvrez l'onglet correspondant et sélectionnez **Aide**.

Documentation

Le Guide de l'utilisateur contient des informations détaillées sur les fonctions de l'application, comment l'utiliser, avec des conseils et des recommandations de configuration.

Des fichiers de documentation au format PDF sont fournis dans le paquet du produit Kaspersky Mobile Security 9.0 (CD d'installation).

Vous pouvez télécharger les fichiers numériques de la documentation depuis le site de Kaspersky Lab.

CONTACTER LE DEPARTEMENT COMMERCIAL

En cas de questions sur le choix, l'achat ou le renouvellement de la licence de Kaspersky Mobile Security 9.0, vous pouvez contacter nos spécialistes du Département commercial via les numéros téléphoniques suivants :

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Le service est offert en russe et en anglais.

Vous pouvez transmettre vos questions au Département commercial à l'adresse de messagerie info@kaspersky.fr.

PUBLIER DES MESSAGES DANS LE FORUM SUR LES APPLICATIONS DE KASPERSKY LAB

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.com.

Le forum permet de lire les conversations existantes, d'ajouter des commentaires, de créer de nouvelles rubriques et il dispose d'une fonction de recherche.

NOUVEAUTES DE KASPERSKY MOBILE SECURITY 9.0

Voici une présentation détaillées des nouveautés de Kaspersky Mobile Security 9.0.

Nouveautés au niveau de la protection :

- L'accès au programme est régi par un mot de passe.
- Kaspersky Mobile Security 9.0 propose un nouveau composant intitulé Contacts personnels qui empêche l'accès non autorisé aux données personnelles de l'utilisateur lorsque l'appareil est utilisé temporairement par d'autres personnes. Ce composant dissimule les données et les événements associés à une liste définie de numéros. Le composant Contacts personnels ne dévoile jamais son activité, si bien que rien n'indique l'existence de données cachées sur l'appareil
- La version actualisée du module Chiffrement permet de bloquer l'accès à un nombre quelconque de dossiers de la mémoire de l'appareil ou d'une carte mémoire. Il conserve les données confidentielles sous une forme chiffrée et bloque l'accès automatiquement à l'issue d'une période définie.
- L'application adopte une nouvelle démarche pour l'administration de l'appareil : l'utilisateur peut activer et désactiver n'importe quel composant selon la fonctionnalité requise.
- Il est désormais possible d'acheter le code d'activation ou de renouveler la licence directement depuis l'appareil nomade.

SPECIFICATIONS MATERIELLES ET LOGICIELLES

Kaspersky Mobile Security 9.0 peut être installé sur des appareils mobiles avec l'un des systèmes d'exploitation suivants :

- Symbian OS 9.1, 9.2, 9.3 et 9.4 Series 60 UI.
- Microsoft Windows Mobile 5.0, 6.0, 6.1, 6.5.

KIT DE DISTRIBUTION

Vous pouvez acquérir Kaspersky Mobile Security 9.0 par Internet (le kit de distribution et la documentation du programme sont au format numérique). Vous pouvez également acquérir Kaspersky Mobile Security 9.0 revendeurs de téléphonie mobile. Pour des détails sur les méthodes d'achat et le kit de distribution, contactez notre Département commercial à l'adresse info@kaspersky.fr.

KASPERSKY MOBILE SECURITY 9.0 POUR SYMBIAN OS

Cette section décrit le fonctionnement de Kaspersky Mobile Security 9.0 sur des Smartphone équipés de Symbian OS version 9.1, 9.2, 9.3 et 9.4 Séries 60 UI.

DANS CETTE SECTION

INSTALLATION DE KASPERSKY MOBILE SECURITY 9.0

L'installation de l'application sur l'appareil nomade s'effectue en plusieurs étapes.

Pour installer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Connectez l'appareil nomade à l'ordinateur.

   Pour les appareils nomades de la marque Nokia, il est conseillé d'utiliser l'application Nokia PC Suite ou Nokia Ovi Suite.

2. Exécutez une des opérations suivantes :

   - Si vous avez acheté l'application sur un cédérom, lancez l'installation automatique de Kaspersky Mobile Security 9.0 depuis ce cédérom.

   - Si vous avez obtenu le fichier d'installation via Internet, copiez-le sur l'appareil nomade. Pour ce faire, appliquez l'une des méthodes suivantes :

     - utilisez l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;

     - utilisez une carte d'extension mémoire.

     Puis lancez l'installation avec l'une des méthodes suivantes :

     - depuis l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;

     - En ouvrant l'archive sis de la distribution sur l'appareil nomade.

   L'écran de confirmation de l'installation s'ouvre.

3. Pour confirmer l'installation de l'application, cliquez sur **Oui**.

4. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.

   Si la langue du système d'exploitation ne correspond pas à la langue de Kaspersky Mobile Security 9.0, un message s'affiche. Pour continuer l'installation de l'application dans la langue actuelle, cliquez sur **OK**.

5. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. L'installation de Kaspersky Mobile Security 9.0. est lancée. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.

6. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade en cliquant sur **OK**.

7. Pour terminer l'installation, redémarrez l'appareil.

   L'application sera installée avec les paramètres recommandés par les experts de Kaspersky Lab.

DÉSINSTALLATION DE L'APPLICATION

Pour supprimer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Déchiffrez les données sur votre appareil si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security 9.0 (cf. la rubrique " Déchiffrement des données " à la page 98).

2. Désactivez Contacts personnels (cf. rubrique " Présentation des modes de Contacts personnels " à la page 86).

3. Fermez Kaspersky Mobile Security 9.0. Pour ce faire, choisissez **Options** → **Quitter** (cf. ill. ci-après).

Figure 1 : Quitter le logiciel.

4. Désinstallation de Kaspersky Mobile Security 9.0. Pour ce faire, exécutez les actions suivantes :

   a. Ouvrez le menu principal de l'appareil.

   b. Sélectionnez le dossier **Applications** → **Install.** (voir figure suivante).

Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

Figure 2 : chemin d'accès aux applications installées

c. Dans la liste des applications, sélectionnez **KMS 9.0**, puis choisissez **Options** → **Désinstaller** (cf. ill. ci-après).

Figure 3: suppression de l'application

d. Pour confirmer la suppression de l'application, cliquez sur **Oui**.

e. Saisissez le code secret puis cliquez sur **OK**.

f. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :

- Si vous souhaitez conserver les paramètres de l'application et les objets en quarantaine, cochez la case en regard des paramètres requis, puis cliquez sur **OK** (cf. ill. ci-après).

- Pour supprimer complètement une application, cliquez sur **Annuler**.

Figure 4 : liste des paramètres à sauvegarder

5. Redémarrez l'appareil pour terminer la suppression de l'application.

MISE A JOUR DE L'APPLICATION

Vous pouvez mettre à jour Kaspersky Mobile Security 9.0 en installant la version la plus récente de cette génération (par exemple, réaliser la mise à jour de la version 9.0 à la version 9.2).

Si vous utilisez Kaspersky Mobile Security 8.0, vous pouvez passer à la version Kaspersky Mobile Security 9.0.

Pour mettre l'application à jour, procédez comme suit :

1. Désactivez le chiffrement - déchiffrez toutes les données (cf. rubrique " Déchiffrement des données " à la page 98).
2. Désactivez Contacts personnels (cf. rubrique " Présentation des modes de Contacts personnels " à la page 86).
3. Quittez la version actuelle de Kaspersky Mobile Security. Pour ce faire, choisissez **Options** → **Quitter**.
4. Copiez le fichier d'installation de l'application sur l'appareil nomade. Pour ce faire, appliquez l'une des méthodes suivantes :
   - depuis le site Internet de Kaspersky Lab ;
   - utilisez l'application Nokia PC Suite ou Nokia Ovi Suite (pour les appareils nomades Nokia) ;
   - utilisez une carte d'extension mémoire.
5. Exécutez le fichier d'installation de Kaspersky Mobile Security 9.0 sur l'appareil.
6. Confirmez l'installation de l'application en cliquant sur le bouton **Oui**.
7. Visualisation des informations complémentaires de l'application : nom, version, certificats. Cliquez ensuite sur **Suite**.
8. Confirmez la mise à jour de l'application en appuyant sur **OK**.
9. Saisissez le code secret défini dans la version antérieure de l'application.
10. Lisez attentivement le contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **OK**. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**. L'installation sera suspendue.
11. Confirmez qu'aucun autre logiciel antivirus n'est installé sur l'appareil nomade. Pour ce faire, cliquez sur **OK**.
12. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :
    - Si vous souhaitez conserver les paramètres de l'application et les objets en quarantaine, cochez la case en regard des paramètres requis, puis cliquez sur **OK**.
    - Pour supprimer complètement une application, cliquez sur **Annuler**.

    L'installation de Kaspersky Mobile Security 9.0. est lancée
13. Pour terminer l'installation, redémarrez l'appareil.

    Si la durée de validité de la licence actuelle n'est pas écoulée, alors l'application sera activée automatiquement. Si la durée de validité de l'application est écoulée, activez l'application (cf. rubrique " Activation de l'application " à la page 23).

Pour passer de Kaspersky Mobile Security 8.0 à la version 9.0, procédez comme suit :

1. Déchiffrez toutes les données si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security 8.0.
2. Fermez Kaspersky Mobile Security 8.0. Pour ce faire, choisissez **Options** → **Quitter**.
3. Désinstallation de Kaspersky Mobile Security 8.0. Pour ce faire, exécutez les actions suivantes :
   a. Ouvrez le menu principal de l'appareil.
   b. Sélectionnez le dossier **Applications** → **Install.**

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

   c. Dans la liste des applications, sélectionnez **KMS 8.0**, puis choisissez **Options** → **Désinstaller**.
   d. Pour confirmer la suppression de l'application, cliquez sur **Oui**.
   e. Supprimez complètement les paramètres de Kaspersky Mobile Security 8.0 car ils sont incompatibles avec les paramètres de la version 9.0. Pour ce faire, cliquez sur **Annuler**.
4. Redémarrez l'appareil pour terminer la suppression de Kaspersky Mobile Security 8.0.
5. Passez à l'installation de Kaspersky Mobile Security 9.0 (cf. rubrique " Installation de Kaspersky Mobile Security 9.0 " à la page 18).

   Si la licence pour Kaspersky Mobile Security 8.0 est toujours valide, activez la version 9.0 à l'aide du code d'activation de la version 8.0 (cf. rubrique " Activation de l'application " à la page 23).

PREMIERS PAS

Cette section reprend les informations sur la préparation de Kaspersky Mobile Security 9.0 (activation et définition du code secret), le lancement de l'application, la mise à jour des bases antivirus et la recherche de virus.

DANS CETTE SECTION

ACTIVATION DU LOGICIEL

Avant de pouvoir utiliser Kaspersky Mobile Security 9.0, il faut l'activer.

Afin de pouvoir activer Kaspersky Mobile Security 9.0, la connexion à Internet doit être configurée sur l'appareil.

Avant d'activer l'application, assurez-vous que la date et l'heure système sont correctes.

Vous pouvez activer l'application d'une des manières suivantes :

- **Activer la version d'évaluation**. Lors de l'activation de la version d'évaluation de l'application, l'utilisateur reçoit une licence d'évaluation gratuite. La durée de validité de la licence d'évaluation est affichée à l'écran après l'activation. Une fois la durée de la licence d'évaluation écoulée, les possibilités de l'application sont réduites. Seules les fonctions suivantes sont accessibles :

  - activation du logiciel ;
  - administration de la licence de l'application ;
  - aide de Kaspersky Mobile Security 9.0 ;
  - désactivation de Chiffrement ;
  - désactivation de Contacts personnels.

  Il est impossible d'activer une deuxième fois la version d'évaluation.

- **Activer la version commerciale**. L'activation de la version commerciale s'opère à l'aide du code d'activation obtenu à l'achat de l'application. Dans le cadre de l'activation de la version commerciale, l'application obtient une licence commerciale qui permet d'utiliser toutes les fonctions de l'application. La durée de validité de la licence apparaît à l'écran de l'appareil. Une fois la licence parvenue à échéance, les fonctionnalités de l'application sont restreintes et la mise à jour de l'application n'a plus lieu.

  Vous pouvez obtenir le code d'activation d'une des manières suivantes :

  - en ligne, en passant de l'application Kaspersky Mobile Security 9.0 au site Web de Kaspersky Lab dédiés aux appareils mobiles ;
  - dans la boutique en ligne de Kaspersky Lab (http://kaspersky.telechargement.fr/cata_home.html)
  - chez un revendeur de Kaspersky Lab.

- **Activer l'abonnement**. Lors de l'activation de l'abonnement, l'application reçoit une licence commerciale à abonnement. La durée de validité de la licence à abonnement est limitée à 30 jours. Dans le cadre de l'abonnement, l'application renouvelle la licence tous les 30 jours. Lors du renouvellement de la licence, la somme définie lors de l'activation de l'abonnement est débitée de votre compte personnel pour l'utilisation de l'application. Le paiement s'opère via l'envoi d'un SMS payant. Une fois que la somme a été débitée, l'application reçoit une nouvelle licence à abonnement du serveur d'activation. Toutes les fonctions sont à nouveau accessibles. Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9.0. Dans ce cas, à l'échéance de la validité de la licence, les fonctionnalités de l'application sont réduites. Les bases antivirus de l'application ne sont pas actualisées.

DANS CETTE SECTION

ACTIVATION DE LA VERSION D'ÉVALUATION

Pour activer la version d'évaluation de Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran **KMS 9.0** s'ouvre.

4. Sélectionnez **Options** → **Version d'évaluation** (cf. ill. ci-après).

Figure 5: activation de la version d'évaluation de l'application

5. Confirmez la connexion à Internet en cliquant sur **Oui**.
6. Sélectionnez le point d'accès pour la connexion au serveur, puis appuyez sur **OK**.

   Le programme envoie une requête au serveur d'activation de Kaspersky Lab puis télécharge et installe la licence.

   Si des erreurs se sont produites lors de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, contactez le service d'assistance technique.

7. Passez à la saisie du code secret (cf. rubrique " Saisie du code secret " à la page 29).

ACTIVATION DE LA VERSION COMMERCIALE

Pour activer la version commerciale de l'application à l'aide du code d'activation, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.

2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran **KMS 9.0** s'ouvre.

4. Sélectionnez **Options** → **Saisie du code**.

   L'écran d'activation de Kaspersky Mobile Security 9.0 s'ouvre.

5. Saisissez le code dans les 4 champs contigus. Le code d'activation est composé de lettres en alphabet latin et de chiffres et n'est pas sensible à la casse. Une fois le code d'activation saisi, choisissez l'option **Options** → **Activer** (cf. ill. ci-après).

Figure 6: activation de la version commerciale de l'application

6. Confirmez la connexion à Internet en cliquant sur **Oui**.

7. Sélectionnez le point d'accès pour la connexion au serveur d'activation de Kaspersky Lab.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab. Si le code d'activation est correct, l'application reçoit une licence.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société où vous avez acheté le code d'activation de Kaspersky Mobile Security 9.0.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

8. Passez à la saisie du code secret (cf. rubrique " Saisie du code secret " à la page 29).

ACTIVATION DE L'ABONNEMENT A KASPERSKY MOBILE SECURITY 9.0

L'activation de l'abonnement requiert l'existence d'une connexion à Internet sur l'appareil.

Pour activer l'abonnement à Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran **KMS 9.0** s'ouvre.

4. Sélectionnez **Options** → **Achat rapide** (cf. ill. ci-après).

Figure 7 : activation de l'abonnement

   L'écran d'activation de Kaspersky Mobile Security 9.0 s'ouvre.

5. Pour confirmer l'activation de l'abonnement à Kaspersky Mobile Security 9.0, appuyez sur **Oui**.
6. Sélectionnez le point d'accès via lequel l'application va se connecter au serveur d'activation de Kaspersky Lab, puis cliquez sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement est accessible, alors les conditions générales de l'abonnement sont présentées.

   Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode d'activation de l'application.

7. Lisez les conditions générales de l'abonnement et si vous les acceptez, cliquez sur **Oui**.

L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9.0 vous prévient lorsque l'abonnement est activé.

Si le solde de votre compte n'est pas suffisant pour envoyer le SMS payant, l'activation de l'abonnement est annulée.

Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Non**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir le mode d'activation de l'application.

8. Passez à la saisie du code secret (cf. rubrique " Saisie du code secret " à la page 29).

ACHAT DU CODE D'ACTIVATION EN LIGNE

Pour acheter le code d'activation de l'application en ligne, procédez comme suit :

1. Ouvrez le menu principal de l'appareil.
2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

   L'écran **KMS 9.0** s'ouvre.

4. Sélectionnez **Options** → **Acheter en ligne**.

   L'écran **Acheter en ligne** s'ouvre.

5. Appuyez sur **Select.** (cf. ill. ci-dessous).

Figure 8: achat du code d'activation en ligne

Le site Web de Kaspersky Lab pour les appareils mobiles s'ouvre. Vous pouvez y commander un code d'activation en ligne.

6. Suivez les instructions.

7. Une fois que vous aurez acheté le code d'activation, passez à l'activation de la version commerciale de l'application (cf. rubrique " Activation de la version commerciale " à la page 25).

SAISIE DU CODE SECRET

Après l'activation de l'application, vous serez invité à saisir le code secret de l'application. Le *code secret de l'application* permet d'éviter l'accès non autorisé aux paramètres de l'application. Vous pourrez modifier ultérieurement le code secret de l'application définit.

Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder à l'application ;
- Pour accéder aux données cryptées ;
- Pour l'envoi d'une instruction SMS dans le but de lancer à distance les fonctions suivante : verrouillage de l'appareil, suppression des données, SIM-Surveillance, Localisation, Contacts personnels ;
- Pour supprimer l'application.

Mémorisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Mobile Security 9.0, ni obtenir l'accès aux données chiffrées, ni supprimer l'application.

Le code secret de l'application est composé de chiffres. Il doit être composé d'au moins 4 chiffres.

Pour saisir le code secret, procédez comme suit :

1. Une fois l'application activée, saisissez les chiffres qui constituent votre code dans le champ **Saisissez le nouveau code** saisissez les chiffres qui constituent votre code.

2. Tapez de nouveau ce code dans la zone **Confirmation du code**.

   La robustesse du code saisi est vérifiée automatiquement.

3. Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche et l'application demande une confirmation. Pour utiliser le code, cliquez sur **Oui**. Pour définir un nouveau code, cliquez sur **Non**.

4. Pour commencer à utiliser le programme, appuyez sur **OK**.

DÉMARRAGE DU LOGICIEL

Pour lancer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Ouvrez le menu principal de l'appareil.

2. Sélectionnez le dossier **Applications** → **Install.** → **KMS 9.0**.

   Le dossier d'installation de l'application peut varier en fonction du modèle d'appareil nomade.

3. Lancez l'application. Pour ce faire, choisissez **Options** → **Ouvrir**.

L'écran **KMS 9.0** s'ouvre.

4. Saisissez le code secret puis cliquez sur **OK**.

La fenêtre d'état de la protection de Kaspersky Mobile Security 9.0 (cf. la rubrique " Fenêtre d'état de la protection " à la page 38) apparaît à l'écran. Pour passer aux fonctions de l'application, appuyez sur **OK**.

MISE A JOUR DES BASES DU PROGRAMME

Kaspersky Mobile Security 9.0 recherche les menaces à l'aide des bases antivirus de l'application qui contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les moyens de les neutraliser. On y retrouve également les descriptions d'autres objets indésirables. Il se peut que les bases livrées avec Kaspersky Mobile Security 9.0 soient dépassées au moment de l'installation.

Il est conseillé d'actualiser les bases antivirus dès après l'installation de l'application.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur l'appareil.

- *Pour lancer la mise à jour des bases manuellement, procédez comme suit :*

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Sélectionnez l'option **Mise à jour**.

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

RECHERCHE DE VIRUS SUR L'APPAREIL

Une fois l'application installée, il est conseillé de lancer l'analyse complète de l'appareil mobile à la recherche d'éventuels objets malveillants.

La première analyse s'opère selon les paramètres définis préalablement par les experts de Kaspersky Lab.

- *Pour lancer l'analyse complète de l'appareil, procédez comme suit :*

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyser** s'ouvre.

2. Sélectionnez l'option **Analyser tout**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez afficher des informations générales sur le logiciel, ainsi que les détails de version et de copyright.

- *Pour consulter les informations relatives à l'application,*

  sous l'onglet **Avancé**, choisissez l'option **Infos logiciel**.

GESTION DE LA LICENCE

Dans le cadre de l'octroi de licences pour l'utilisation des applications de Kaspersky Lab, il est important de comprendre les notions suivantes :

- Le contrat de licence ;
- La licence.

Ces notions sont liées les unes aux autres et forment un ensemble unique.

Examinons chacune d'entre elles en détail.

La rubrique présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Mobile Security 9.0 et de la renouveler.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le *contrat de licence* est un contrat conclu entre d'une part une personnalité physique ou juridique détenant une copie légale de Kaspersky Mobile Security 9.0 et Kaspersky Lab d'autre part. Ce contrat est proposé avec chaque application de Kaspersky Lab. Il présente en détail les droits et les restrictions d'utilisation de Kaspersky Mobile Security 9.0.

Conformément aux termes du contrat de licence, vous avez le droit de détenir une copie de l'application après avoir acheté et installé celle-ci.

Kaspersky Lab est également ravi de vous proposer les services complémentaires suivants :

- Assistance technique ;
- la mise à jour des bases antivirus de Kaspersky Mobile Security 9.0;
- Mise à jour des modules logiciels de Kaspersky Mobile Security 9.0.

Pour pouvoir l'obtenir, vous devez acheter et activer une licence (cf. la rubrique " Présentation des licences de Kaspersky Mobile Security 9.0 " à la page 31).

PRESENTATION DES LICENCES DE KASPERSKY MOBILE SECURITY 9.0

La *licence* est un droit octroyé pour l'utilisation de Kaspersky Mobile Security 9.0 et des services complémentaires (cf. rubrique " Présentation du contrat de licence " à la page 31) offerts par Kaspersky Lab ou ses partenaires.

Chaque licence se définit par sa durée de validité et son type.

La *durée de validité de la licence* désigne la période pendant laquelle vous pouvez bénéficier des services complémentaires :

- Assistance technique ;
- Mise à jour des bases antivirus et des modules de l'application.

Le volume des services proposés dépend du type de licence.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Mobile Security 9.0.

  La licence d'évaluation peut être utilisée une seule fois uniquement.

  La licence d'évaluation vous permet de contacter le service d'assistance technique uniquement pour les questions relatives à l'activation de l'application ou à l'achat de la licence commerciale. Une fois la licence d'évaluation expirée, Kaspersky Mobile Security 9.0 arrête de fonctionner. Pour pouvoir continuer à utiliser l'application, il faut l'activer (cf. rubrique " Activation de la version commerciale " à la page 25).

- *Commerciale* : licence payante avec une durée de validité définie (par exemple, un an) octroyée à l'achat de Kaspersky Mobile Security 9.0.

  Toutes les fonctionnalités de l'application et les services complémentaires sont accessibles pendant la période de validité de la licence commerciale.

  Une fois que la licence commerciale a expiré, certaines fonctionnalités de Kaspersky Mobile Security 9.0 deviennent inaccessibles et les bases antivirus de l'application ne seront plus actualisées. Sept jours avant l'expiration de la licence, l'application affichera une notification. Vous aurez ainsi le temps de renouveler la licence.

- *Commerciale avec abonnement* : licence payante offrant une possibilité de renouvellement automatique ou manuel. La licence à abonnement est proposée aux prestataires de services.

  L'abonnement a une validité limitée (30 jours). Une fois que l'abonnement expire, il peut être renouvelé manuellement ou automatiquement. Le mode de renouvellement de l'abonnement dépend de la législation en vigueur et de l'opérateur de téléphonie mobile. L'abonnement est renouvelé automatiquement si le prépaiement du prestataire de service a été réalisé.

  Lors du renouvellement de l'abonnement, le montant défini dans les conditions générales de l'abonnement est débité de votre compte personnel. La somme est débitée de votre compte personnel via un SMS payant envoyé au numéro du prestataire de service.

  Si l'abonnement n'est pas renouvelé, Kaspersky Mobile Security 9.0 ne réalise plus la mise à jour des bases antivirus de l'application et les fonctionnalités de l'application sont limitées.

  Si vous choisissez l'abonnement, vous pouvez activer la licence commerciale via le code d'activation. Dans ce cas, l'abonnement sera automatiquement annulé.

  Vous pouvez activer un abonnement si vous utilisez une licence commerciale. Si au moment d'activer l'abonnement vous aviez déjà activé la licence à durée déterminée, cette licence sera remplacée par une licence à abonnement.

AFFICHAGE DES INFORMATIONS DE LICENCE

Vous pouvez consulter les informations suivantes sur la licence : le numéro de licence, le type, le nombre de jours restant avant l'expiration, la date d'activation et le numéro de série de l'appareil.

➧ *Pour consulter les informations sur la licence, procédez comme suit :*

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Infos licence** dans l'onglet Informations (cf. ill. suivante).

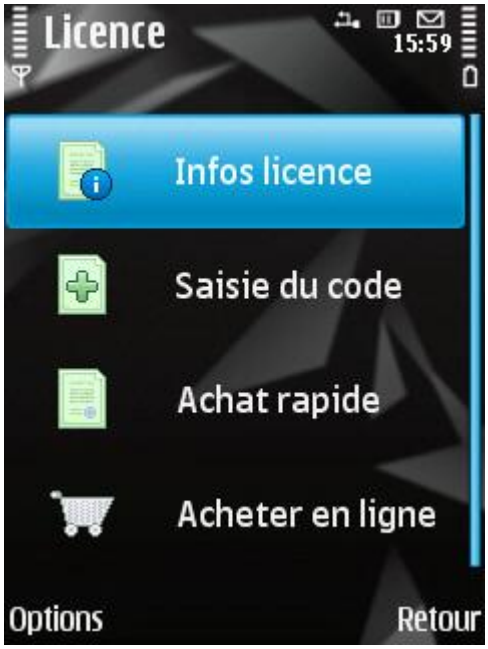


Figure 9 : Affichage des informations de licence

L'écran **Infos licence** s'ouvre

RENOUVELLEMENT DE LA LICENCE

Kaspersky Mobile Security 9.0 permet de renouveler la durée de validité de la licence de l'application.

Vous pouvez renouveler la licence d'une des méthodes suivantes :

- saisir le code d'activation : activation de la licence à l'aide d'un code d'activation. Le code d'activation est disponible à l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html ou chez un distributeur Kaspersky Lab.
- acheter le code d'activation en ligne. Accédez au site Web ouvert sur votre appareil mobile et achetez le code d'activation en ligne.
- s'abonner à Kaspersky Mobile Security 9.0. Activez l'abonnement afin de renouveler la durée de validité de la licence tous les 30 jours.

Pour pouvoir actualiser les bases de l'application sur l'appareil mobile, la connexion à Internet doit être configurée.

DANS CETTE SECTION

RENOUVELLEMENT DE LA LICENCE A L'AIDE DU CODE D'ACTIVATION

Pour renouveler la licence à l'aide du code d'activation, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Sélectionnez l'option **Saisie du code**.

   L'écran **Saisie du code** apparaît.

3. Saisissez dans l'ordre le code d'activation reçu dans les quatre champs, puis choisissez **Options** → **Activer** (cf. ill. ci-après).

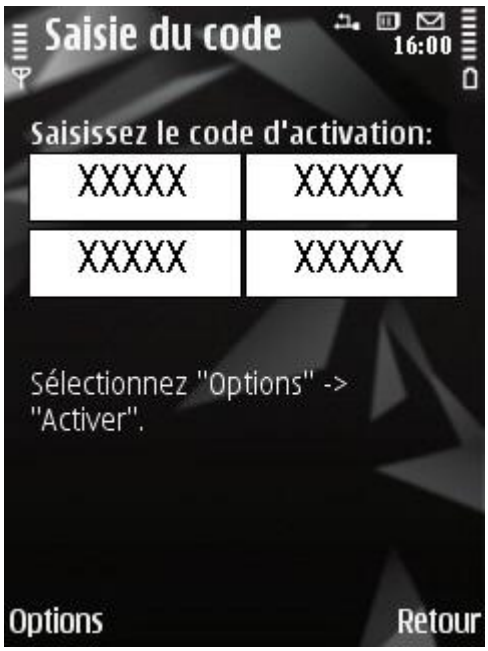


Figure 10 : renouvellement de la licence à l'aide d'un code d'activation

4. Si l'application demande un point d'accès, sélectionnez le type de connexion requis dans la liste proposée.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées sur l'écran.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade.

5. A la fin, cliquez sur **OK**.

RENOUVELLEMENT DE LA LICENCE EN LIGNE

Pour renouveler l'application en ligne, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Renouveler en ligne** (cf. ill. ci-dessous).

   Si la validité de la licence est écoulée, l'option du menu deviendra **Acheter en ligne**.

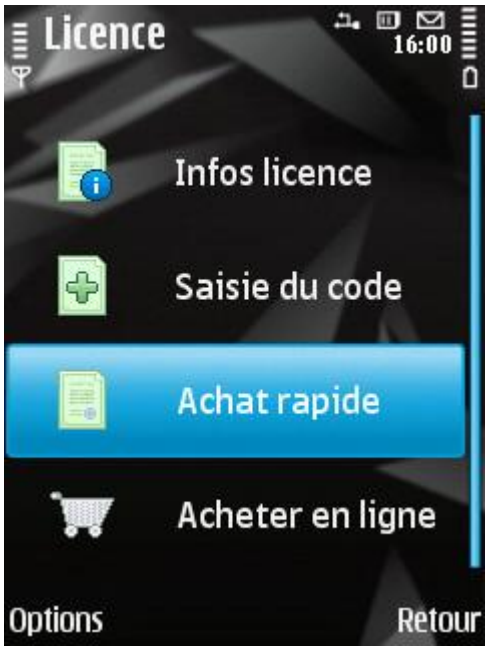


Figure 11: renouvellement de la licence en ligne

   L'écran **Acheter en ligne** s'ouvre.

3. Appuyez sur **Ouvrir**.

   Cette action entraîne l'ouverture d'un site où vous serez invité à commander le renouvellement de la licence.

   Si la durée de validité de la licence est écoulée, alors le site Web de Kaspersky Lab pour appareils mobiles s'ouvre. Vous pouvez y acheter le code d'activation en ligne.

4. Suivez les instructions.

5. Une fois l'achat du code d'activation terminé, saisissez le code d'activation obtenu (cf. la rubrique " Renouvellement de la licence à l'aide d'un code d'activation " à la page 34).

RENOUVELLEMENT DE LA LICENCE A L'AIDE DE L'ACTIVATION DE L'ABONNEMENT

Vous pouvez activer l'abonnement à Kaspersky Mobile Security 9.0. Dans le cadre de l'abonnement, Kaspersky Mobile Security 9.0 renouvelle la validité de la licence tous les 30 jours. Lors de chaque renouvellement de la licence, le montant défini dans les conditions générales de l'abonnement est débité de votre compte personnel.

L'activation de l'abonnement à Kaspersky Mobile Security 9.0, requiert une connexion à Internet.

Pour activer l'abonnement à Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Achat rapide**.

   L'écran **Activation** s'ouvre.

3. Pour confirmer l'activation de l'abonnement à Kaspersky Mobile Security 9.0, appuyez sur **Oui**.

4. Sélectionnez le point d'accès via lequel l'application va se connecter au serveur d'activation de Kaspersky Lab, puis cliquez sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement est accessible, alors les conditions générales de l'abonnement sont présentées.

   Si le service d'abonnement n'est pas offert, l'application vous en informe. L'activation de l'abonnement sera annulée.

5. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9.0 en cliquant sur **Oui**.

   L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9.0 vous prévient lorsque l'abonnement est activé.

   Si le solde de votre compte n'est pas suffisant pour envoyer le SMS payant, l'activation de l'abonnement est annulée.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

   Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Non**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir le mode de renouvellement de la licence.

6. A la fin, cliquez sur **OK**.

REFUS DE L'ABONNEMENT

Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9.0. Dans ce cas Kaspersky Mobile Security 9.0 ne renouvelle pas la validité de la licence tous les 30 jours. À l'échéance de la licence en cours de validité, les fonctionnalités de l'application sont réduites et les bases antivirus de l'application ne sont pas mises à jour.

Si l'abonnement est annulé, sachez que vous pouvez le reprendre (cf. rubrique " Renouvellement de l'abonnement " à la page 37).

Pour refuser l'abonnement à Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Ann. abon.** (voir figure suivante).

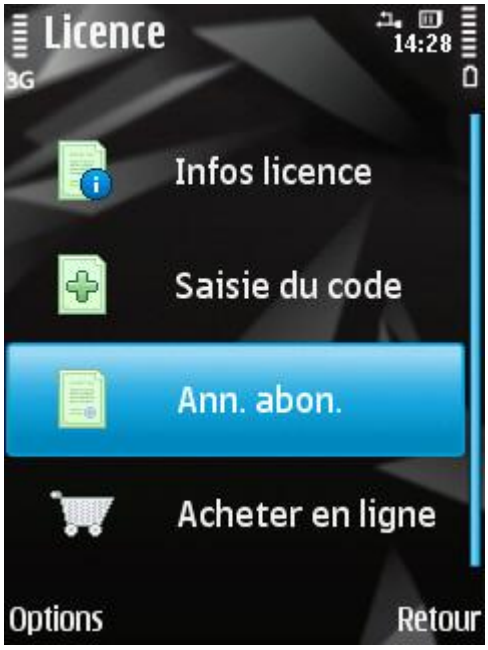


Figure 12 : refus de l'abonnement

Kaspersky Mobile Security 9.0 vous signale que l'abonnement a été annulé

RENOUVELLEMENT DE L'ABONNEMENT

Si vous aviez refusé l'abonnement, vous avez la possibilité de le renouveler. Dans ce cas Kaspersky Mobile Security 9.0 renouvellera à nouveau la validité de la licence de l'application tous les 30 jours.

En cas de renouvellement de l'abonnement, le montant requis sera débité de votre compte personnel uniquement si la licence actuelle expire dans moins de trois jours.

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

1. Sélectionnez **Avancé**, choisissez l'option **Licence**.

   L'écran **Licence** s'ouvre.

2. Choisissez l'option **Achat rapide**.

Si la licence actuelle est échue, Kaspersky Mobile Security 9.0 propose d'activer à nouveau l'abonnement.

Si la licence actuelle est toujours valide, alors Kaspersky Mobile Security 9.0 renouvelle l'abonnement et quand la licence actuelle arrive à échéance, il la renouvelle tous les 30 jours.

INTERFACE DE L'APPLICATION

L'interface de Kaspersky Mobile Security 9.0 est simple et conviviale. Cette section présente des informations sur les principaux composants de l'interface.

ICONE DE PROTECTION

L'icône de la protection indique l'état de fonctionnement de l'application. Si l'icône est activée (en couleur), cela signifie que la protection est activée. Si l'icône est inactive (grise), cela indique que la protection est suspendue et que tous ses composants sont désactivés.

Par défaut, l'icône de la protection ne s'affiche pas à l'écran de l'appareil. Vous pouvez modifier les paramètres d'affichage de l'icône (cf. la rubrique " Affichage de l'icône de protection " à la page 111).

VOIR AUSSI

FENETRE D'ETAT DE LA PROTECTION

L'état des composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection.

Il existe trois états possibles pour chaque composant. Chacun d'entre eux est associé à une couleur définie, comme les feux de circulation. Le vert signifie que la protection de l'appareil est assurée au niveau requis. Le jaune et le rouge indiquent qu'il y a différents types de menaces contre la sécurité. Les menaces sont non seulement les applications malveillantes, mais également les bases antivirus de l'application dépassée, certains composants désactivés, les paramètres minimes de fonctionnement de l'application, etc.

La fenêtre de l'état de la protection est accessible directement après le lancement de l'application et reprend les informations suivantes :

- **Protection** : état de la protection en temps réel (cf. la rubrique " Protection en temps réel " à la page 41).

  L'icône verte de l'état indique que la protection est activée et assurée au niveau requis. Les bases antivirus de l'application sont à jour.

  L'icône jaune signale que la mise à jour des bases antivirus n'a plus eu lieu depuis quelques jours.

  L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil. Par exemple, la protection est désactivée. Il se peut que les bases de l'application n'ait plus été actualisées plus de 15 jours.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. la rubrique " Filtrage de l'activité de réseau. Pare-feu " à la page 93).

  L'icône verte de l'état signifie que le composant est activé. Le niveau de protection du pare-feu a été sélectionné.

  Une icône rouge indique que le filtrage de l'activité de réseau n'a pas lieu.

- **Antivol** : état de la protection de l'appareil en cas de vol ou de perte (cf. la rubrique " Protection des données en cas de perte ou de vol de l'appareil " à la page 75).

  L'icône verte signifie que les fonctions de l'Antivol dont le nom apparaît sous l'état du composant sont activées.

  L'icône rouge indique que toutes les fonctions d'antivol sont désactivées.

- **Contacts personnels** : état de la protection des données confidentielles (cf. la rubrique " Dissimulation des informations confidentielles " à la page 85).

  L'icône verte de l'état signifie que le composant est activé. Les données confidentielles sont masquées.

L'icône jaune prévient l'utilisateur que le composant est désactivé. Les données personnelles sont visibles et peuvent être consultées.

- **Licence** : durée de validité de la licence (cf. la rubrique " Administration des licences " à la page 30).

  L'icône verte d'état indique que la licence est encore valide pendant plus de 14 jours.

  L'icône jaune indique que la licence est valide pour moins de 14 jours.

  L'icône rouge indique que la validité de la licence est écoulée.

Figure 13: Fenêtre de l'état de la protection

Vous pouvez aussi passer à la fenêtre de l'état de la protection en choisissant l'option **Menu** → **Etat de la protection**.

Par défaut, la fenêtre de l'état de la protection s'affiche directement après le lancement de l'application. Vous pouvez modifier ses paramètres d'affichage (cf. la rubrique " Affichage de la fenêtre d'état " à la page 110).

VOIR AUSSI

Affichage de la fenêtre d'état 110

ONGLETS DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et accessibles sur les onglets de l'application. Chaque onglet permet d'accéder aux paramètres du composant sélectionné et aux tâches de la protection.

Kaspersky Mobile Security 9.0 propose les onglets suivants :

- **Anti-Virus :** protection du système de fichiers, analyse à la demande et actualisation des bases antivirus de l'application.
- **Contacts personnels** : dissimulation des données confidentielles sur l'appareil.
- **Antivol** : blocage de l'appareil et suppression des informations en cas de vol ou de perte.

- **Chiffrement** : protection des données sur l'appareil grâce au chiffrement des données.
- **Anti-Spam** : filtrage des SMS et des appels entrants non sollicités.
- **Contrôle Parental** : contrôle des SMS et des messages sortants.
- **Pare-feu** : protection de réseau de l'application.
- **Avancé** : paramètres généraux de l'application, informations sur l'application, sur les bases antivirus utilisées et sur la licence.

Par défaut, les onglets de l'application sont accessibles après la consultation de la fenêtre sur l'état de la protection (cf. la rubrique " Fenêtre d'état de la protection " à la page 38).

Vous pouvez naviguer entre les onglets d'une des manières suivantes :

- A l'aide du joystick de l'appareil ;
- Via le menu **Options** → **Ouvrir onglet**.

MENU DE L'APPLICATION

Le menu de l'application permet de passer à l'exécution des principales actions. Le menu contient les options suivantes (cf. ill. ci-après) :

- **Sélection** : sélection de la fonction, de l'instruction ou du paramètre.
- **Ouvrir l'onglet** : passage à la sélection du composant de l'application.
- **Etat de protection** : ouverture de la fenêtre de l'état de la protection.
- **Aide** : affichage de l'aide contextuelle de Kaspersky Mobile Security 9.0.
- **Infos logiciel** : affichage de l'écran reprenant les informations sur l'application.
- **Quitter** : arrêt de Kaspersky Mobile Security 9.0.

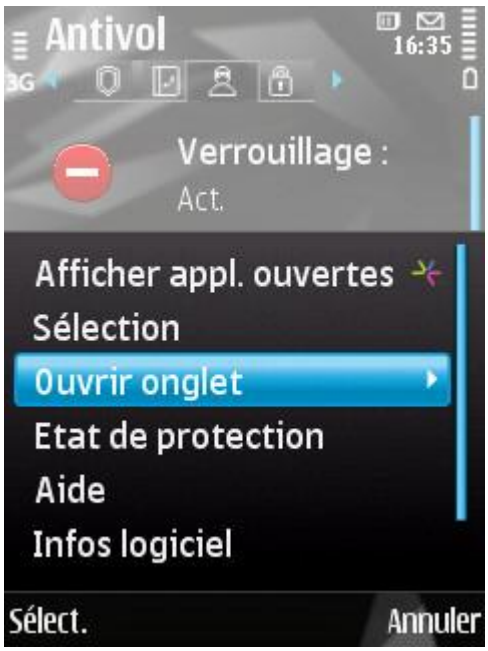


Figure 14: menu de l'application

➡ *Pour ouvrir le menu de l'application,*

sélectionnez **Options**.

Pour naviguer dans le menu de l'application, utilisez le joystick de l'appareil ou le stylet.

PROTECTION DU SYSTEME DE FICHIERS

La rubrique présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. Elle explique comment activer / suspendre la Protection et la configurer.

DANS CETTE SECTION

PRESENTATION DE LA PROTECTION

La protection se charge en même temps que le système d'exploitation et s'exécute dans la mémoire de l'appareil, pour analyser tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte toutes les tentatives d'accès aux fichiers de la part de l'utilisateur ou d'un autre programme.

2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés comparant aux bases antivirus de données utilisées par le logiciel. Les bases antivirus de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

3. Après l'analyse, Kaspersky Mobile Security 9.0 peut appliquer les actions suivantes :

   - quand du code malveillant est découvert dans le fichier, l'application le bloque et agit conformément aux paramètres définis ;

   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Les informations sur les résultats de l'analyse sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

ACTIVATION ET DESACTIVATION DE LA PROTECTION

Lorsque la protection est activée, toutes les actions exécutées dans le système sont placées sous un contrôle permanent. La protection contre les objets malveillants utilisent les ressources de l'application. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

Les spécialistes de Kaspersky Lab recommandent vivement de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

L'état actuel de la protection est repris sur l'onglet **Anti-Virus** à côté de l'option de menu **Protection**.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

- *Pour désactiver la protection, procédez de la manière suivante :*

  1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

     L'écran **Protection** s'ouvre.

  2. Pour le paramètre **Mode de protection**, choisissez la valeur **Act.** (cf. ill. ci-après).

Figure 15 : activation de la protection

  3. Appuyez sur **Précédent** pour enregistrer les modifications.

- *Pour désactiver la protection, procédez de la manière suivante :*

  1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

     L'écran **Protection** s'ouvre.

  2. Attribuez la valeur **Désact.** au paramètre **Mode de protection**.

  3. Appuyez sur **Précédent** pour enregistrer les modifications.

CONFIGURATION DE LA ZONE DE PROTECTION

Kaspersky Mobile Security 9.0 analyse par défaut les fichiers de tous les types. Pour réduire la durée de l'analyse, vous pouvez définir les types d'objets à analyser.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

- *Pour sélectionner le type d'objet à analyser, procédez comme suit :*

  1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

L'écran **Protection** s'ouvre.

2. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tous les types.
   - **Exécutables** : analyse uniquement les fichiers exécutables des applications (par exemple, fichiers au format *.exe, *.sis, *.mdl, *.app).

Figure 16: sélection des objets à analyser

3. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9.0 met les objets malveillants découverts en quarantaine. Vous pouvez modifier l'action qui sera exécutée par l'application en cas de découverte d'un objet malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer la réponse du logiciel en présence d'un objet malveillant découvert, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Définissez l'action que l'application exécutera en cas de découverte d'un objet malveillant. Pour ce faire, attribuez une valeur au paramètre **Action Anti-Virus** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.
   - **Quarantaine** : place en quarantaine les objets malveillants.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

Figure 17: réponse de l'application sur l'objet malveillant détecté

3. Appuyez sur **OK** pour enregistrer les modifications.

RESTAURATION DES PARAMETRES DE PROTECTION PAR DEFAUT

La protection fonctionne par défaut selon les paramètres recommandés par les experts de Kaspersky Lab. En cas de configuration de la protection, sachez qu'il est toujours possible de revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de protection par défaut, procédez comme suit :

1. Sélectionnez **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez **Options** → **Restaurer**.

ANALYSE DE L'APPAREIL

La section reprend les informations sur la recherche des objets malveillants qui permet d'identifier et de neutraliser les menaces sur votre appareil. La section décrit également comment lancer la tâche d'analyse, comment programmer l'exécution de la tâche, comme sélectionner les objets à analyser et comment définir l'action que l'application exécutera sur la menace identifiée.

DANS CETTE SECTION

PRESENTATION DE L'ANALYSE DE L'APPAREIL

L'analyse de l'appareil permet d'identifier et de neutraliser les objets malveillants sur votre appareil. Kaspersky Mobile Security 9.0 est capable de réaliser une analyse complète ou partielle du système de fichiers de l'appareil. Autrement dit, il peut analyser uniquement le contenu de la mémoire intégrée de l'appareil, uniquement les messages ou un dossier en particulier (y compris les dossiers sur les cartes mémoire).

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Mobile Security 9.0 analyse les fichiers d'un type défini (cf. la rubrique " Sélection des types de fichiers à analyser " à la page 48).

2. Le fichier est analysé à la recherche d'objets malveillants. Kaspersky Mobile Security 9.0 identifie les objets malveillants à l'aide des bases antivirus de l'application. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Après l'analyse, Kaspersky Mobile Security 9.0 peut appliquer les actions suivantes :

   - Si un objet malveillant a été découvert dans le fichier, Kaspersky Mobile Security 9.0 exécute l'action définie (cf. la rubrique " Sélection des actions à appliquer sur les objets identifiés " à la page 49) ;

   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

La tâche d'analyse est lancée manuellement ou automatiquement selon un horaire défini (cf. rubrique " Exécution de l'analyse programmée " à la page 47).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer l'analyse manuellement, par exemple lorsqu'aucune autre tâche n'est exécutée sur l'appareil.

Pour lancer manuellement une analyse antivirus, procédez de la manière suivante :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyser** s'ouvre.

2. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

- **Analyser tout.** : analyse tout le système de fichiers de l'appareil. Les objets suivants sont analysés par défaut : mémoire de l'appareil et carte mémoire.

- **Analyser dossier** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte mémoire. En cas de sélection de l'option **Analyser dossier**, un écran reprenant le système de fichiers de l'appareil s'ouvre. Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick. Pour lancer l'analyse d'un dossier, sélectionnez le dossier souhaité puis choisissez **Options →·Analyser**.

- **Analyser RAM** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.

- **Analyser msgs.** : analyse les messages reçus via SMS, MMS ou Bluetooth.

Figure 18: sélection de la zone d'analyse

Une fois l'analyse lancée, la fenêtre du processus d'analyse s'ouvre. Elle indique l'état actuel de l'analyse : le nombre d'objets analysés, le chemin d'accès à l'objet en cours d'analyse et un indicateur des résultats de l'analyse en pour cent (cf. ill. ci-dessous).

Figure 19: état de l'analyse de l'appareil

Si Kaspersky Mobile Security 9.0 découvre un objet infecté, il exécute l'action conformément aux paramètres d'analyse définis (cf. la rubrique " Sélection des actions à appliquer sur les objets identifiés " à la page 49).

Par défaut, si l'application Kaspersky Mobile Security 9.0 découvre une menace, elle tente de la réparer. Si la réparation est impossible, l'application place l'objet découvert en quarantaine.

Une fois l'analyse terminée, des statistiques générales reprenant les informations suivantes s'affichent :

- Le nombre d'objets analysés ;
- Le nombre de virus découverts, placés en quarantaine et supprimés ;
- Le nombre d'objets ignorés (par exemple, lorsque le fichier est bloqué par le système d'exploitation ou lorsque le fichier n'est pas un fichier exécutable alors que l'analyse porte uniquement sur les fichiers exécutables) ;
- L'heure de l'analyse.

Pour économiser la batterie, le rétro éclairage de l'écran est désactivé par défaut pendant l'analyse. Vous pouvez modifier les paramètres du rétro éclairage de l'écran (cf. la rubrique " Gestion du rétro éclairage " à la page 109).

EXECUTION DE L'ANALYSE PROGRAMMEE

Kaspersky Mobile Security 9.0 permet de planifier des analyses de l'appareil qui s'exécuteront automatiquement à des heures programmées à l'avance. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, l'action définie par le paramètre d'analyse est exécutée sur cet objet.

Par défaut, l'exécution d'analyse programmée est désactivée.

➧ *Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :*

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

L'écran **Analyser** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez une valeur au paramètre **Analyse auto** (cf. ill. ci-après) :

   - **Désact.** : désactive le démarrage de l'analyse planifiée.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Spécifiez le **Jour d'analyse** et l'**Heure d'analyse auto**.
   - **Chaque jour** : l'analyse s'exécutera tous les jours. Spécifiez l'**Heure d'analyse**. dans le champ de saisie.

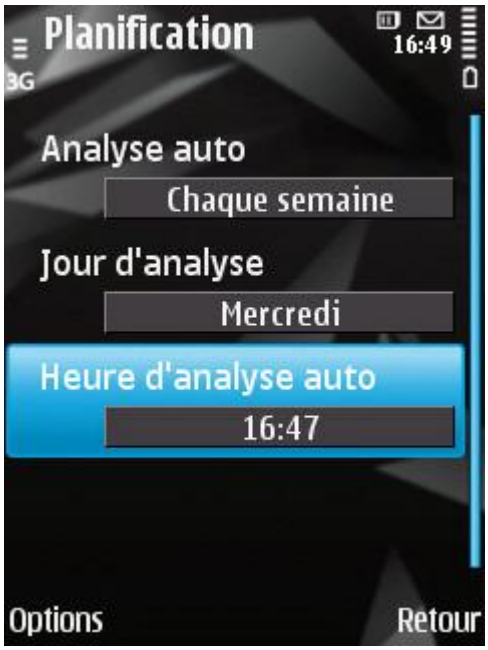


Figure 20 : planification d'une analyse

4. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DU TYPE D'OBJET A ANALYSER

Kaspersky Mobile Security 9.0 analyse par défaut tous les objets qui se trouvent sur l'appareil et sur les cartes mémoire. Pour réduire la durée de l'analyse, vous pouvez sélectionner des types d'objets à analyser, c'est-à-dire définir quels formats de fichiers seront soumis à la recherche d'un éventuel code malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour sélectionner un objet à analyser, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyser** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Choisissez la valeur du paramètre **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers** : analyse les fichiers de tout type et décompacte et analyse le contenu des archives. L'application analyse les archives des formats suivants : *.zip, *.jar, *.jad, *.sis et *.sisx.

   - **Exécutables** : analyse uniquement les fichiers exécutables des applications au format *.exe, *.dll, *.mdl, *.app, * .rdl, *.prt, *.pxt, *.ldd, *.pdd ou *.class. Dans ce cas, les archives ne sont ni décompactées, ni analysées.

Figure 21: sélection du type d'objet à analyser.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9.0 met les objets infectés découverts en quarantaine. Vous pouvez configurer les actions appliquées quand il détecte un objet malveillant.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer la réponse du programme, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Définissez l'action à exécuter sur les objets malveillants. Pour ce faire, attribuez une valeur au paramètre **Action Anti-Virus** (cf. ill. ci-après) :

   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.

   - **Quarantaine** : place en quarantaine les objets malveillants détectés.

- **Confirmer** : confirme l'action auprès de l'utilisateur. En cas de découverte d'une menace, une fenêtre de confirmation de l'action s'ouvre.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

- **Tenter de réparer** : répare les objets malveillants. Si la réparation est impossible, l'action définie pour le paramètre **Si la réparation échoue** est exécutée.

Figure 22 : sélection de l'action appliquée à un objet malveillant

4. Si vous avez choisi l'option **Tenter de réparer**, définissez la deuxième action de l'application qui sera exécutée lorsque la réparation de l'objet ne sera pas possible. Pour ce faire, attribuez une valeur au paramètre **Si la réparation échoue** (cf. ill. ci-après) :

    - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.

    - **Quarantaine** : place en quarantaine les objets malveillants.

    - **Interroger** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

Figure 23: sélection de l'action à exécuter sur les objets malveillants si la réparation est impossible

5. Appuyez sur **Précédent** pour enregistrer les modifications.

CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. Pour pouvoir analyser le contenu d'une archive, il faut absolument la décompacter. Ceci peut ralentir considérablement la vitesse de l'analyse de l'appareil.

Le décompactage des archives est désactivé par défaut. L'application analyse les archives des formats suivants : *.zip, *.jar, *.jad, *.sis et *.sisx. Pour accélérer l'analyse, vous pouvez désactiver le décompactage des archives.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour désactiver le décompactage des archives, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyse** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Attribuez au paramètre **Décompresser archives** la valeur **Non** (cf. ill. ci-dessous).

Figure 24: configuration de l'analyse de fichiers compressés

4. Appuyez sur **Précédent** pour enregistrer les modifications.

RESTAURATION DES PARAMETRES D'ANALYSE DE L'APPLICATION PAR DEFAUT

L'analyse de l'appareil fonctionne par défaut selon les paramètres recommandés par les experts de Kaspersky Lab. En cas de configuration de l'analyse de l'appareil, sachez qu'il est toujours possible de revenir aux valeurs recommandées pour les paramètres.

Pour restaurer les paramètres de l'analyse par défaut, procédez comme suit :

1. Sélectionnez **Analyser** dans l'onglet **Anti-Virus**.

   L'écran **Analyser** s'ouvre.

2. Choisissez l'option **Objets/action**.

   L'écran **Objets et actions** s'ouvre.

3. Sélectionnez **Options** → **Restaurer**.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La rubrique présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. Elle décrit également comment manipuler les objets en quarantaine, à savoir comment consulter, restaurer ou supprimer les objets qui se trouvent dans ce dossier.

DANS CETTE SECTION

À PROPOS DE LA QUARANTAINE

La quarantaine est un dossier défini dans lequel Kaspersky Mobile Security 9.0 place les objets potentiellement malveillants.

Les objets malveillants peuvent être découverts et placés en quarantaine pendant l'analyse de l'appareil ou par la protection.

Les objets placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil. Ensuite, ces objets pourront être supprimés ou restaurés.

AFFICHAGE DES OBJETS EN QUARANTAINE

Vous pouvez consulter les objets qui sont dans la quarantaine. Le nom complet de l'objet et la date à laquelle il a été découvert sont repris.

Vous pouvez également consulter des informations complémentaires sur l'objet infecté sélectionné : chemin d'accès à l'objet sur l'appareil avant sa mise en quarantaine et nom de la menace.

- *Pour afficher la liste des objets en quarantaine,*

  sous l'onglet **Quarantaine** dans l'onglet **Anti-Virus**.

L'écran **Quarantaine** s'ouvre et présente la liste des objets contenus (cf. ill. ci-après).

Figure 25 : liste des objets en quarantaine

- *Pour consulter les informations relatives à l'objet sélectionné,*

  choisissez le menu **Options** → **Détails**.

  L'écran propose les informations suivantes sur l'objet : chemin d'accès au fichier où l'application l'a trouvé sur l'appareil et nom de la menace.

RESTAURATION D'OBJETS DE LA QUARANTAINE

Si vous êtes convaincu que l'objet placé en quarantaine ne constitue pas une menace pour l'appareil, vous pouvez le restaurer depuis la quarantaine. L'objet restauré sera remis dans on répertoire d'origine.

- *Pour restaurer un objet depuis la quarantaine, procédez comme suit :*

  1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

     L'écran **Quarantaine** s'ouvre.

  2. Sélectionnez l'objet que vous souhaitez restaurer, puis choisissez l'option **Options** → **Restaurer**.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

Il est possible de supprimer un objet ou l'ensemble des éléments repris dans la quarantaine.

- *Pour supprimer un objet de la quarantaine, procédez comme suit :*

  1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

     L'écran **Quarantaine** s'ouvre.

  2. Choisissez l'objet que vous souhaitez supprimer, puis sélectionnez l'option **Options** → **Supprimer**.

L'objet sélectionné sera supprimé.

Pour supprimer tous les objets de la quarantaine, procédez comme suit :

1. Sélectionnez **Quarantaine** dans l'onglet **Anti-Virus**.

   L'écran **Quarantaine** s'ouvre.

2. Sélectionnez **Options** → **Tout supprimer**.

Tous les objets en quarantaine seront éliminés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

La section présente le composant Anti-Spam qui filtre les SMS et les appels entrants sur la base des listes noire ou blanche. Elle décrit également comment composer les listes noire et blanche, comment sélectionner l'action réalisée par Anti-Spam sur les SMS et les appels entrants et comment configurer le fonctionnement du composant.

DANS CETTE SECTION

A PROPOS DU COMPOSANT ANTI-SPAM

Anti-Spam protège l'appareil contre la réception de SMS et d'appels non sollicités. Anti-Spam filtre les SMS et les appels entrants sur la base de listes noire ou blanche.

Les listes contiennent les enregistrements. Chacun de ces enregistrements peut contenir les paramètres suivants :

- Type de données (SMS, appels, SMS et appels) soumis au filtrage (paramètre obligatoire) ;
- Numéro d'où proviennent les données ;
- Texte que peut contenir le SMS.

Anti-Spam filtre les SMS et les appels sur la base du régime (cf. la rubrique " Présentation des modes de l'Anti-Spam " à la page 56). Anti-Spam analyse, sur la base du régime, chaque SMS ou appel entrant puis détermine si ce SMS ou cet appel est sollicité ou non. L'analyse se termine dès que l'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

L'algorithme Anti-Spam se déroule de la manière suivante par défaut :

1. Analyse du SMS entrant pour voir si le texte ou le numéro de téléphone figurent dans :

a. La liste noire. Si la liste contient un enregistrement dont le numéro ou le texte correspond aux données du SMS entrant, ce dernier est considéré comme indésirable et bloqué. L'application supprime le SMS bloqué.

b. La liste blanche. Si la liste contient un enregistrement dont le numéro ou le texte correspond aux données du SMS entrant, ce dernier est considéré comme désirable et est autorisé.

2. Analyse des appels et des SMS uniquement sur la base du numéro :

a. La liste noire. Si la liste contient un enregistrement dont le numéro correspond au numéro de l'appelant (pas de texte dans l'enregistrement), alors l'appel ou le SMS est considéré comme du spam et est bloqué. L'application supprime le SMS bloqué.

b. La liste blanche. Si la liste contient un enregistrement dont le numéro correspond au numéro de l'appelant (pas de texte dans l'enregistrement), alors l'appel ou le SMS est considéré comme acceptable et est autorisé.

3. Analyse des messages uniquement sur la base du texte :

a. La liste noire. Si la liste contient un enregistrement dont le texte correspond aux données du SMS entrant (le numéro ne figure pas dans l'enregistrement), alors ce SMS est considéré comme du spam et est bloqué. L'application supprime le SMS bloqué.

b. La liste blanche. Si la liste contient un enregistrement dont le texte correspond aux données du SMS entrant (le numéro ne figure pas dans l'enregistrement), alors ce SMS est considéré comme normal et est autorisé.

4. Sélection de l'action. Si aucune équivalence n'est trouvée dans la liste noire ou dans la liste blanche, Anti-Spam laisse passer par défaut les appels et les SMS et propose de choisir une action dans la fenêtre de notification. La notification présente en plus des informations complémentaires. S'agissant d'un appel reçu, la notification reprend le numéro de l'appelant. Dans le cas des SMS, la notification reprend le numéro de l'expéditeur et le contenu.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique " Journaux du logiciel " à la page 106).

PRESENTATION DES MODES DE L'ANTI-SPAM

Le mode Anti-Spam détermine la règle selon laquelle les SMS et les appels sont filtrés.

Les modes de fonctionnement Anti-Spam disponibles :

- **Les deux listes**. Dans ce mode, l'Anti-Spam remet les SMS et accepte les appels en provenance de numéros de la liste blanche et bloque ceux en provenance de numéros de la liste noire. Après la réception d'un appel ou d'un message en provenance d'un numéro qui ne figure dans aucune des deux listes, l'Anti-Spam propose une action à choisir : accepter le SMS/l'appel sans ajouter le numéro de téléphone de l'abonné à la liste ou ajouter le numéro de téléphone à la liste noire ou à la liste blanche.

  Ce mode est sélectionné par défaut.

- **Liste noire**. Dans ce mode, l'Anti-Spam bloque les SMS et les appels en provenance de numéros de la liste noire. L'Anti-Spam accepte les SMS et les appels en provenance d'autres numéros. L'Anti-Spam supprime les numéros bloqués.

- **Liste blanche**. Dans ce mode, l'Anti-Spam accepte les SMS et les appels en provenance de numéros de la liste blanche. L'Anti-Spam bloque les SMS et les appels en provenance d'autres numéros. L'Anti-Spam supprime les numéros bloqués.

- **Désactivé**. Dans ce mode, l'Anti-Spam est désactivé. L'Anti-Spam ne filtre pas les SMS et les appels.

Vous pouvez modifier le mode de l'Anti-Spam (cf. la rubrique " Modification du mode de l'Anti-Spam " à la page 57). Le mode actuel de l'Anti-Spam s'affiche sur l'onglet **Anti-Spam** à côté de l'option **Mode**.

MODIFICATION DU MODE DE L'ANTI-SPAM

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier le mode de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Mode** dans l'onglet **Anti-Spam**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une valeur pour le paramètre **Mode de l'Anti-Spam** (cf. ill. ci-dessous).

Figure 26: modification du mode de l'Anti-Spam

3. Appuyez sur **Précédent** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à l'Anti-Spam pour bloquer les SMS et les appels entrants.

La liste reprend les numéros de téléphone et les expressions dont la présence dans un message indique son appartenance au spam.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique " Journaux du logiciel " à la page 106).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste noire de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

   L'écran **Liste noire** s'ouvre.

2. Choisissez l'option **Options** → **Ajouter entrée** (cf. ill. ci-après).

Figure 27: ajout d'un enregistrement à la liste noire.

3. Définissez les paramètres suivants (cf. ill. ci-après) :

   - **Bloquer tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va bloquer :
     - **Appels et SMS :** bloque les appels et les SMS entrants.

- **Appels seuls :** bloque uniquement les appels entrants.
- **SMS seuls** : bloque uniquement les SMS entrants.

- **Depuis le numéro** : numéro de téléphone dont les SMS et/ou les appels seront bloqués. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenants le texte** : mots/expressions clés qui indiquent que le SMS reçu est du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

Figure 28: paramètres de l'enregistrement

4. Appuyez sur **Précédent** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez modifier les valeurs de tous les paramètres de la liste noire des numéros interdits.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste noire de l'Anti-Spam, exécutez les opérations suivantes :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Options** → **Modifier entrée**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Bloquer tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va bloquer :

     - **Appels et SMS :** bloque les appels et les SMS entrants.

- **Appels seuls :** bloque uniquement les appels entrants.
- **SMS seuls** : bloque uniquement les SMS entrants.

- **Depuis le numéro** : numéro de téléphone dont les SMS et/ou les appels seront bloqués. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).
- **Contenant le texte** : mots/expressions clés qui indiquent que le SMS reçu est du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste.

Pour supprimer un enregistrement de la liste noire de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer entrée**.

SUPPRESSION DE TOUTES LES ENTREES

Pour supprimer tous les enregistrements de la liste noire de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Anti-Spam**.

   L'écran **Liste noire** s'ouvre.

2. Choisissez l'option du menu **Options** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer la liste blanche qui servira à Anti-Spam pour autoriser les SMS et les appels entrants.

La liste reprend les numéros de téléphone des expéditeurs et les expressions que vous ne considérez pas comme du spam

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

   L'écran **Liste blanche** s'ouvre.

2. Choisissez l'option **Options** → **Ajouter entrée** (cf. ill. ci-après).

Figure 29: ajout d'un enregistrement à la liste blanche

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Autoriser tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va autoriser :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seuls :** autorise uniquement les appels entrants.
     - **SMS seuls** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone dont les SMS et/ou les appels sont acceptés. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenant le texte** : mots/expressions clés qui indiquent que le SMS reçu n'est pas du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

Figure 30: paramètres de l'enregistrement

4. Appuyez sur **Précédent** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste blanche de l'Anti-Spam, exécutez les opérations suivantes :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Options** → **Modifier entrée**.

3. Modifier les paramètres requis de l'enregistrement :

   - **Autoriser tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va autoriser :
     - **Appels et SMS :** autorise les appels et les SMS entrants.
     - **Appels seuls :** autorise uniquement les appels entrants.
     - **SMS seuls** : autorise les messages SMS entrants uniquement.
   - **Depuis le numéro** : numéro de téléphone dont les SMS et/ou les appels sont acceptés. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenant le texte** : mots/expressions clés qui indiquent que le SMS reçu n'est pas du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Pour supprimer un enregistrement de la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer entrée**.

SUPPRESSION DE TOUS LES ENREGISTREMENTS DE LA LISTE BLANCHE

Pour supprimer tous les enregistrements de la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Anti-Spam**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez **Options** → **Tout supprimer**.

REACTION AUX SMS ET APPELS DE CONTACTS QUI NE FIGURENT PAS DANS LE REPERTOIRE TELEPHONIQUE

Si le mode **Les deux listes** ou **Liste blanche** (cf. la rubrique " **Présentation des modes de l'Anti-Spam** " à la page 147) de l'Anti-Spam a été sélectionné, vous pouvez définir la réaction du composant face aux SMS ou aux appels de personnes dont le numéro ne figure pas dans le répertoire téléphonique. L'Anti-Spam permet d'élargir la liste blanche en y introduisant les numéros des contacts.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour définir la réaction de l'Anti-Spam face aux numéros ne figurant pas dans le répertoire téléphonique de l'appareil, procédez comme suit :

1. Sélectionnez **Mode** dans l'onglet **Anti-Spam**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Autoriser contacts** (cf. ill. ci-après) :

   - Pour que l'Anti-Spam considère un numéro du répertoire téléphonique comme un ajout à la liste blanche, sélectionnez la valeur **Oui** ;

- Pour que l'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini de l'Anti-Spam, choisissez la valeur **Non**.

Figure 31: réaction de l'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

3. Appuyez sur **Précédent** pour enregistrer les modifications.

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode **Les deux listes** ou **Liste noire** (cf. la rubrique " **Présentation des modes de l'Anti-Spam** " à la page 147) de l'Anti-Spam a été sélectionné, vous pouvez enrichir la liste noire en incluant tous les numéros sans chiffres (composés de lettres). Alors l'Anti-Spam pourra bloquer les SMS en provenance de numéros sans chiffres.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour définir la réaction de l'Anti-Spam en cas de réception d'un SMS en provenance d'un numéro sans chiffres, procédez comme suit :

1. Sélectionnez **Mode** dans l'onglet **Anti-Spam**.

   L'écran **Mode** s'ouvre.

2. Choisissez la valeur du paramètre **Non numériques** (cf. ill. ci-après) :

   - Pour que l'Anti-Spam supprime automatiquement les SMS en provenance de numéros sans chiffres, sélectionnez l'option **Bloquer** ;

- Pour que l'Anti-Spam filtre les SMS en provenance de numéros sans chiffres uniquement sur la base du mode sélectionné pour l'Anti-Spam, sélectionnez la valeur **Autoriser**.

Figure 32: configuration des actions exécutées par l'Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres.

3. Appuyez sur **Précédent** pour enregistrer les modifications.

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Le mode par défaut activé pour l'Anti-Spam est **Les deux listes** (cf. la rubrique " **Modes du composant Anti-Spam** " à la page 147). L'Anti-Spam analyse les SMS entrants sur la base des listes blanche et noire.

Si le numéro de l'appelant ne figure ni dans la liste blanche, ni dans la liste noire, l'Anti-Spam vous prévient et vous demande quelle sera l'action à réaliser sur les SMS entrants.

Vous pouvez choisir une des actions suivantes à exécuter sur le SMS (cf. ill. ci-après) :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, choisissez **Options** → **Ajouter à la liste noire**.

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste blanche, choisissez **Options** → **Ajouter à la liste blanche**.

- Pour accepter le SMS sans consigner le numéro de téléphone de l'appelant dans aucune des listes, appuyez sur **Ignorer**.

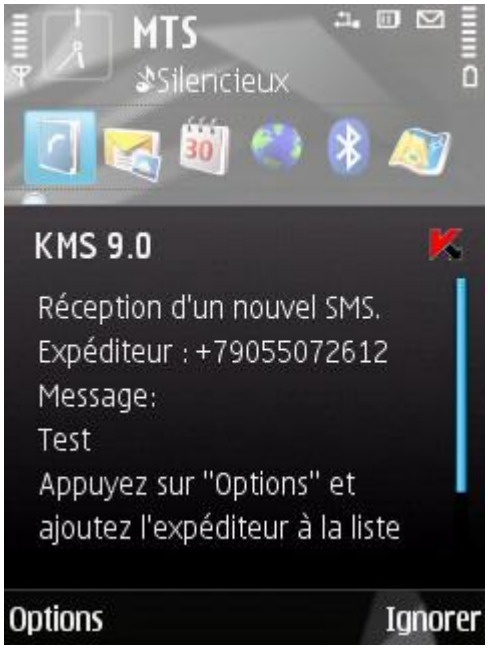


Figure 33: notification de l'Anti-Spam sur le SMS reçu

Les informations sur les SMS bloqués sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Le mode par défaut activé pour Anti-Spam est **Les deux listes** (cf. la rubrique " **Modes du composant Anti-Spam** " à la page 147). Anti-Spam analyse les appels entrants sur la base des listes blanche et noire.

Si le numéro de l'appelant ne figure ni dans la liste blanche, ni dans la liste noire, Anti-Spam vous le signalera après l'appel et proposera une action à exécuter sur les appels entrants.

Vous pouvez choisir une des actions suivantes pour le numéro de l'appelant (cf. ill. ci-après) :

- Pour ajouter le numéro de téléphone de l'appelant à la liste noire, choisissez **Options** → **Ajouter à la liste noire**.

- Pour ajouter le numéro de téléphone de l'appelant à la liste blanche, choisissez **Options** → **Ajouter à la liste blanche**.

- Choisissez **Ignorer** si vous ne souhaitez pas consigner le numéro de l'appelant dans aucune des listes.

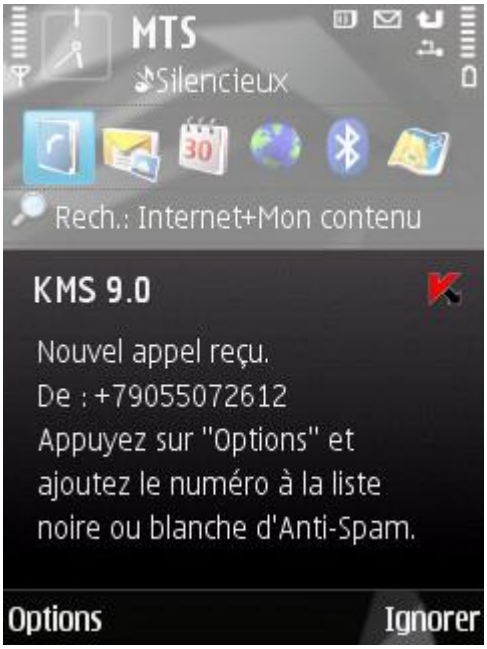


Figure 34: notification de l'Anti-Spam sur l'appel reçu

Les informations sur les appels bloqués sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

RESTRICTIONS SUR LES APPELS ET LES SMS SORTANTS. CONTROLE PARENTAL

Cette section présente le composant Contrôle Parental qui permet de restreindre les appels et les SMS sortants à certains numéros. Elle explique également comment composer des listes de numéros interdits ou autorisés et configurer les paramètres du Contrôle Parental.

DANS CETTE SECTION

À PROPOS DU CONTROLE PARENTAL

Contrôle Parental permet de contrôler les appels et les SMS sortants sur la base de listes noire et blanche de numéros de téléphone. Le fonctionnement du composant dépend du mode.

En mode **Liste noire**, le Contrôle Parental interdit l'envoi de SMS et la réalisation d'appels vers les numéros de la liste noire. L'envoi de SMS et la réalisation d'appels vers les autres numéros est autorisée. En mode **Liste blanche**, le

Contrôle Parental autorise l'envoi de SMS et la réalisation d'appels uniquement vers les numéros de la liste blanche. L'envoi de SMS et la réalisation d'appels vers les autres numéros sont interdits par le Contrôle Parental. En mode **Désact.** , le Contrôle Parental ne contrôle pas les SMS et les appels sortants.

Le Contrôle Parental interdit les SMS envoyés uniquement à l'aide des outils standards de l'appareil. Le Contrôle Parental autorise l'envoi de SMS via des logiciels tiers.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

MODES DU CONTROLE PARENTAL

Le mode du Contrôle Parental définit la règle selon laquelle le contrôle des SMS et des appels sortants est effectué.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Désactivé** : désactive Contrôle Parental. Ne pas contrôler les SMS et les appels sortants.

  Ce mode est sélectionné par défaut.

- **Liste noire** : interdit l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste noire. Tous les autres SMS et appels sont autorisés.

- **Liste blanche** : autorise l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste blanche. Tous les autres SMS et appels sont interdits.

Vous pouvez changer le mode du Contrôle Parental (cf. la rubrique " Modification du mode du contrôle parental " à la page 68).

Le mode sélectionné de Contrôle Parental apparaît sur l'onglet **Contrôle Parental** à côté de l'option de menu **Mode**.

MODIFICATION DU MODE DU CONTROLE PARENTAL

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier le mode de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Contrôle Parental**, choisissez l'option **Mode**.

   L'écran **Mode** s'ouvre.

2. Sélectionnez un des modes proposés pour Contrôle Parental (cf. ill. ci-après).

Figure 35 : modification du mode du Contrôle Parental

3. Appuyez sur **OK** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à Contrôle Parental pour bloquer les SMS et les appels sortants. La liste reprend les numéros de téléphone vers lesquels l'envoi de SMS et la réalisation d'appels seront interdits.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Contrôle Parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle Parental**.

   L'écran **Liste noire** s'ouvre.

2. Choisissez l'option **Options** → **Ajouter entrée** (cf. ill. ci-après).

Figure 36: ajout d'un enregistrement à la liste noire.

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
     - **Appels et SMS :** bloque les appels et les SMS sortants.
     - **Appels seuls :** bloque uniquement les appels sortants.
     - **SMS seuls** : interdit les SMS sortants uniquement.

- **Numéro de téléphone :** numéro de téléphone vers lequel l'envoi de SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

Figure 37: paramètres de l'enregistrement

4. Appuyez sur **Précédent** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Vous pouvez modifier les valeurs de tous les paramètres de la liste noire des numéros interdits.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier une entrée dans liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle Parental**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Options** → **Ajouter entrée**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
     - **Appels et SMS :** bloque les appels et les SMS sortants.
     - **Appels seuls :** bloque uniquement les appels sortants.
     - **SMS seuls** : interdit les SMS sortants uniquement.
   - **Numéro de téléphone :** numéro de téléphone vers lequel l'envoi de SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des

caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste.

Pour supprimer un enregistrement de la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle Parental**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer entrée**.

SUPPRESSION DE TOUS LES ENREGISTREMENTS DE LA LISTE NOIRE

Pour supprimer tous les enregistrements de la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste noire** dans l'onglet **Contrôle Parental**.

   L'écran **Liste noire** s'ouvre.

2. Sélectionnez **Options** → **Tout supprimer**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer une liste blanche sur la base de laquelle Contrôle Parental autoriser l'envoi de SMS/la réalisation d'appels.

La liste reprend les numéros de téléphone vers lesquels Contrôle Parental autorise l'envoi de SMS et la réalisation d'appels.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

DANS CETTE SECTION

AJOUT D'UNE ENTREE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Contrôle Parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour ajouter un enregistrement à la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle Parental**.

   L'écran **Liste blanche** s'ouvre.

2. Choisissez l'option **Options** → **Ajouter entrée** (cf. ill. ci-après).

Figure 38: ajout d'un enregistrement à la liste blanche

3. Définissez les paramètres suivants pour le nouvel enregistrement (cf. ill. ci-après) :

   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :
     - **Appels et SMS :** autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle Parental pour l'envoi de SMS/la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

Figure 39: paramètres de l'enregistrement

4. Appuyez sur **Précédent** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour modifier un enregistrement de la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle Parental**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement que vous souhaitez modifier, puis choisissez l'option **Options** → **Modifier entrée**.

3. Modifiez les paramètres requis de l'enregistrement :

   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :

     - **Appels et SMS :** autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle Parental pour l'envoi de SMS/la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

4. Appuyez sur **Précédent** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste blanche. Vous pouvez supprimer ce numéro de la liste composée.

Pour supprimer un enregistrement de la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle Parental**.

   L'écran **Liste blanche** s'ouvre.

2. Sélectionnez dans la liste l'enregistrement qu'il faut absolument supprimer, puis choisissez l'option **Options** → **Supprimer entrée**.

SUPPRESSION DE TOUTES LES ENTREES

Pour supprimer tous les enregistrements de la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Liste blanche** dans l'onglet **Contrôle Parental**.

   L'écran **Liste blanche** s'ouvre.

2. Dans le menu **Options** → **Tout supprimer**.

La liste est désormais vide.

PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL

La section présente les informations sur le composant Antivol chargé de la protection sophistiquées de données personnelles en cas de vol ou de perte de l'appareil et qui facilite la recherche de celui-ci. Elle explique également comment activer/désactiver les fonctions de l'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la protection en cas de vol ou de perte de l'appareil.

DANS CETTE SECTION

À PROPOS DU COMPOSANT ANTIVOL

Antivol protège les données enregistrées sur l'appareil contre l'accès non autorisé. Cette fonction peut être utile en cas de perte ou de vol de l'appareil. Antivol permet de verrouiller à distance l'appareil et de supprimer les données qu'il renferme.

Ce composant dispose des fonctions suivantes :

- **Verrouillage** : permet de verrouiller l'appareil à la demande de l'utilisateur et de définir le texte qui apparaîtra à l'écran de l'appareil verrouillé.
- **Suppression** : permet de supprimer les données personnelles de l'utilisateur (tous les contacts, les messages, les photos, le calendrier, les journaux, les paramètres de connexion au réseau), les données de la carte mémoire et les fichiers des dossiers sélectionnés.
- **SIM-Surveillance** : permet, en cas de remplacement de la carte SIM, d'envoyer vers le numéro de téléphone et/ou l'adresse électronique défini le nouveau numéro ainsi que de bloquer l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.
- **Localisation** : permet de récupérer les coordonnées géographiques de l'appareil volé par SMS sur un autre appareil ou dans une adresse de messagerie spécifiée.

  Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré.

Afin de pouvoir utiliser chaque fonction de l'Antivol, il faut se souvenir du code secret défini au premier lancement de Kaspersky Mobile Security 9.0.

Toutes les fonctions de l'Antivol sont désactivées après l'installation de Kaspersky Mobile Security 9.0.

De plus, Kaspersky Mobile Security 9.0 permet de lancer à distance la fonction Antivol via l'envoi d'instruction SMS vers un autre appareil (cf. la rubrique " Lancement à distance de la fonction Antivol " à la page 84).

L'état du fonctionnement actuel de chaque fonction apparaît sur l'onglet **Antivol** à côté du nom de la fonction.

Les informations sur le fonctionnement du composant sont conservées dans le journal du composant (cf. la rubrique " Journaux de l'application " à la page 106).

VERROUILLAGE DE L'APPAREIL

Après la réception d'une instruction SMS spéciale, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données qu'il renferme. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Cette fonction ne verrouille pas l'appareil mais active la possibilité de le verrouiller à distance.

Pour modifier les valeurs des paramètres, utilisez le joystick de votre appareil ou sélectionnez **Options** → **Modifier**.

Pour activer la fonction de verrouillage, procédez comme suit :

1. Sélectionnez **Antivol**, choisissez l'option **Verrouillage**.

   L'écran **Verrouillage** s'ouvre.

2. Attribuez la valeur **Act.** pour le paramètre **Mode de verrouillage**.

3. Pour afficher un message à l'écran de l'appareil verrouillé, choisissez le paramètre **Texte lors du verr.** et remplissez le champ **Entrez le texte** (cf. ill. ci-après). Quand l'appareil sera verrouillé, le texte par défaut " Appareil verrouillé " s'affichera.

   Pour ne pas afficher le message, choisissez le paramètre **Texte lors du verr.**, puis supprimer le contenu du champ **Entrez le texte** et appuyez sur **OK**.

Figure 40: paramètres de la fonction Verrouillage

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Pour verrouiller un autre appareil, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction **Envoi d'une instruction**. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Saisissez l'instruction **Verrouillage** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 41: verrouillage à distance de l'appareil.

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour composer le SMS à l'aide des fonctions standard de rédaction de SMS du téléphone,

envoyez à l'appareil un SMS avec le texte `block:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction SMS spéciale, la fonction Suppression permet de supprimer les informations suivantes sur l'appareil :

- Les données personnelles de l'utilisateur (tous les contacts, les messages, les photos, le calendrier et les paramètres de connexion au réseau). Qui plus est, Antivol supprime les contacts enregistrés dans le répertoire téléphonique de l'appareil et sur la carte SIM ;

- Les données de la carte mémoire ;

- Les données dans le dossier **C:\Data** et dans d'autres dossiers dans la liste **Dossiers à supprimer**.

Cette fonction ne supprime pas les données enregistrées sur l'appareil mais active la possibilité de le faire après la réception de l'instruction SMS.

Pour activer la fonction de suppression des données, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Choisissez l'option **Mode Suppr. des donn.** et choisissez la valeur **Act.** (cf. ill. ci-dessous).

4. Sélectionnez les données qui seront supprimées dès la réception de l'instruction SMS spéciale par l'appareil :

   - Pour supprimer les données personnelles, attribuez la valeur **Oui** au paramètre **Supprimer données** ;
   - Pour supprimer les fichiers du dossier **C:\Data** et de la liste **Dossiers à supprimer**, attribuez la valeur **Oui** au paramètre **Supprimer les dossiers**.

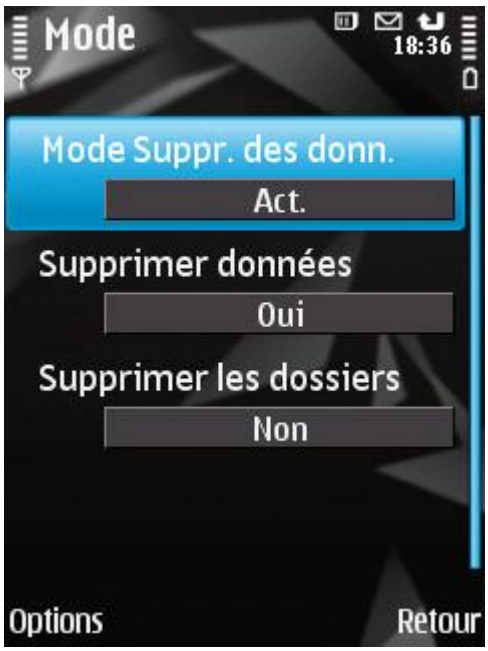


Figure 42: paramètres de la fonction de suppression de données

5. Appuyez sur **Précédent** pour enregistrer les modifications.

6. Passez à la constitution de la liste **Dossiers à supprimer** (cf. rubrique " **Composition de la liste des objets à supprimer** " à la page 80).

La suppression des données personnelles de l'appareil peut être réalisée d'une des manières suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Choisissez l'instruction **Suppression** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 43 : Suppression de données personnelles

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour composer le SMS avec les fonctions standards de messagerie SMS de votre téléphone :

envoyez à l'autre appareil un SMS contenant le texte `wipe:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil récepteur). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception de l'instruction SMS spéciale.

Pour que l'Antivol supprime les dossiers de la liste après la réception de l'instruction SMS spéciale, assurez-vous que la valeur **Oui** est attribuée au paramètre **Supprimer les dossiers** dans le menu **Mode** de l'onglet **Antivol**.

Pour ajouter un dossier à la liste des dossiers à supprimer, procédez comme suit :

1. Sous l'onglet **Antivol**, sélectionnez **Suppression**

L'écran **Suppression** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Choisissez l'option **Options** → **Ajouter un dossier** (cf. ill. ci-après).

Figure 44: ajout d'un dossier

4. Choisissez le dossier souhaité dans l'arborescence, puis cliquez sur **OK**.

   Le dossier sera ajouté à la liste.

5. Appuyez sur **Précédent** pour enregistrer les modifications.

Pour supprimer un dossier de la liste, procédez comme suit :

1. Sélectionnez sous l'onglet **Antivol** l'option **Suppre ssion**

   L'écran **Suppression** s'ouvre.

2. Choisissez l'option **Suppr. doss.**

   L'écran **Dossiers à supprimer** s'ouvre.

3. Sélectionnez un dossier dans la liste, puis choisissez l'option **Options** → **Supprimer le dossier**.

4. Pour confirmer la suppression, cliquez sur **Oui**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

SIM-Surveillance permet, en cas de remplacement de la carte SIM, d'envoyer le nouveau numéro de téléphone au numéro et/ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil.

Pour activer la fonction SIM-Surveillance et contrôler le remplacement de la carte SIM sur l'appareil, procédez comme suit :

1. Sélectionnez SIM-Surveillance dans l'onglet **Antivol**.

   L'écran **SIM-Surveillance** s'ouvre.

2. Choisissez l'option **Mode de SIM-Surveillance** et attribuez la valeur **Act**.

3. Configurez les paramètres suivants de SIM-Surveillance (cf. ill. ci-après) :

   - **Adresse courriel**. Pour recevoir un message électronique indiquant le nouveau numéro de téléphone de votre appareil, saisissez ici une adresse électronique.

   - **Numéro de téléphone**. Pour envoyer automatiquement un message au sujet du nouveau numéro de téléphone, saisissez le numéro de téléphone vers lequel le message sera envoyé. Ces numéros peuvent commencer par un chiffre ou par le signe " + " et ne peuvent contenir que des chiffres.

   - **Au rempl. de SIM**. Pour verrouiller l'appareil en cas de remplacement ou de mise en marche de l'appareil sans sa carte SIM, choisissez la valeur **Verrouiller**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret. Par défaut, le verrouillage de l'appareil est désactivé.

   - **Texte en cas de verrouillage**. Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Entrez le texte**. Le texte " Appareil verrouillé " est saisi par défaut.

Figure 45: paramètres de la fonction SIM-Surveillance

4. Appuyez sur **Précédent** pour enregistrer les modifications.

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Localisation détermine les coordonnées géographiques de l'appareil et les envoie par SMS ou courrier électronique à l'appareil à l'origine de la demande.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. L'activation du récepteur a lieu automatiquement après la réception de l'instruction SMS.

La réception des coordonnées est possible uniquement si l'appareil se trouve dans une zone couverte par les satellites. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver seront lancées à intervalles réguliers.

Pour activer la fonction Localisation, procédez comme suit :

1. Sous l'onglet **Antivol**, choisissez l'option **Localisation**.

   L'écran **Localisation** s'ouvre.

2. Attribuez la valeur **Act**. au paramètre **Mode de localisation**.

3. Dans le champ **Adresse courriel**, saisissez l'adresse électronique à laquelle les coordonnées géographiques de l'appareil seront envoyées (cf. ill. ci-après).

Figure 46: paramètres de la fonction Localisation

4. Appuyez sur **Précédent** pour enregistrer les modifications.

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. Votre appareil recevra à l'insu de l'utilisateur un SMS et l'application enverra les coordonnées de l'appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. Votre appareil recevra un SMS et l'application enverra les coordonnées de l'appareil.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sélectionnez **Avancé** et choisissez l'option **Instr. env.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Choisissez l'instruction **Localisation**, puis cliquez sur **Suivant** (cf. ill. ci-après).

Figure 47 : détermination des coordonnées de l'appareil

3. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

4. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Pour composer le SMS avec les fonctions standards de messagerie SMS de votre téléphone :

envoyez à l'autre appareil un SMS contenant le texte `find:<code>` (où `<code>` est le code secret de l'application défini sur l'autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Le SMS contenant les coordonnées géographiques de l'appareil sera envoyé au numéro de téléphone à l'origine de l'envoi de l'instruction SMS et à une adresse électronique, si celle-ci a été définie dans les paramètres de la fonction Localisation.

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

L'application permet d'envoyer une instruction spéciale par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Mobile Security. L'instruction par SMS se présente sous la forme d'un SMS crypté qui contient le code secret de l'appareil auquel est envoyé le SMS. La réception de l'instruction passera inaperçue sur l'autre appareil.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Sélectionnez une des fonctions proposées à lancer à distance (cf. ill. ci-après) :

- **Verrouillage** (cf. la rubrique " **Verrouillage** " à la page 77).
- **Suppression** (cf. la rubrique " **Suppression de données personnelles** " à la page 78).
- **Localisation**.
- **Contacts personnels** (cf. rubrique " **Présentation des modes de Contacts personnels** " à la page 86).

Figure 48: lancement à distance de la fonction Antivol

La fonction doit être activée sur l'appareil qui reçoit l'instruction par SMS.

4. Cliquez sur **Suivant**.
5. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.
6. Entrez le code secret spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

La section présente le composant Contacts personnels. Le composant permet de dissimuler les données confidentielles de l'utilisateur pendant que l'appareil est utilisé temporairement par une autre personne.

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

Le composant Contacts personnels masque les informations confidentielles sur la base de la liste des contacts créée qui reprend les numéros confidentiels. Pour les numéros confidentiels, le composant masque les informations suivantes : contacts du répertoire, SMS entrants, sortants et transmis et entrées du journal des appels. Le composant masque également les informations entrantes : SMS et appels entrants. Le composant bloque le signal de réception d'un nouveau SMS et le masque dans la liste des SMS reçus. Le composant bloque l'appel d'un numéro confidentiel et n'affiche pas les informations relatives à sa réception. L'interlocuteur entendra la tonalité de ligne occupée. Pour voir les appels et SMS reçus pendant la période où le composant Contacts personnels était activé, désactivez-le. Quand vous activerez à nouveau le composant Contacts personnels, il masquera les informations consultées.

Vous pouvez configurer l'activation de la dissimulation des données confidentielles automatiquement ou à distance depuis un autre appareil mobile.

Vous ne pouvez désactiver la fonction de dissimulation des informations confidentielles que depuis l'application.

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. la rubrique " Journaux de l'application " à la page 106).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

Vous pouvez gérer le mode de fonctionnement de Contacts personnels. Le mode détermine si la fonction de dissimulation des données confidentielles est activée ou non.

La dissimulation est désactivée par défaut.

Les modes suivants sont prévus pour Contacts personnels :

- **Afficher** : les données confidentielles sont affichées. Les paramètres de Contacts personnels peuvent être modifiés.
- **Masquer** : les données confidentielles sont masquées. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique (cf. rubrique " Activation automatique de la dissimulation des informations confidentielles " à la page 87) de la dissimulation des données personnelles ou son activation à distance depuis un autre appareil (cf. rubrique " Activation de la dissimulation des informations confidentielles à distance " à la page 88).

L'état actuel de dissimulation des informations confidentielles figure sur l'onglet **Contacts personnels** à côté de l'option de menu **Mode**.

La modification du mode de fonctionnement du composant Contacts personnels peut prendre un certain temps.

MODIFICATION DU MODE DE CONTACTS PERSONNELS

Le mode du composant Contacts personnels peut être modifié d'une des manières suivantes :

- Depuis l'interface de l'application ;
- A l'aide d'un code secret lorsque l'appareil est en mode d'attente actif.

Pour modifier le mode de Contacts personnels, procédez comme suit :

1. Sélectionnez **Contacts personnels**, sélectionnez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Attribuez une valeur au paramètre **Mode Contacts perso.** (cf. ill. ci-après).

Figure 49: modification du mode de Contacts personnels

3. Appuyez sur **Précédent** pour enregistrer les modifications.

Pour modifier le mode du composant Contacts personnels à l'aide du code secret lorsque l'appareil est en mode d'attente actif,

saisissez ***code secret#**.

Une notification apparaîtra à l'écran pour indiquer la modification du mode du composant Contacts personnels.

ACTIVATION AUTOMATIQUE DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES

Vous pouvez configurer l'activation automatique de la dissimulation des informations confidentielles après un certain temps. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour activer automatiquement la dissimulation des informations confidentielles à l'issue d'une période déterminée, procédez comme suit :

1. Sous l'onglet **Contacts personnels**, choisissez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, choisissez une des valeurs prédéfinies pour le paramètre **Masquer automatiq.** (cf. ill. ci-après).

   - **Sans délai**.
   - **1 minute**.
   - **5 minutes**.
   - **15 minutes**.
   - **1 heure**.
   - **Désact.**

Figure 50: paramètres de lancement automatique de Contacts personnels

3. Appuyez sur **Précédent** pour enregistrer les modifications.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Mobile Security 9.0 permet d'activer à distance depuis un autre appareil mobile la dissimulation des informations confidentielles. Pour ce faire, il faut avant tout activer la fonction qui autorise l'activation à distance de la dissimulation des informations.

Pour autoriser l'activation à distance de la dissimulation des informations confidentielles, procédez comme suit :

1. Sélectionnez **Contacts personnels**, sélectionnez l'option **Mode**.

   L'écran **Mode Contacts perso.** apparaît.

2. Attribuez la valeur **Oui** au paramètre **Masquer par SMS** (cf. ill. ci-après).

Figure 51 : paramètres d'activation à distance du composant Contacts personnels

3. Appuyez sur **Précédent** pour enregistrer les modifications.

Vous pouvez activer à distance la dissimulation des informations confidentielles d'une des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. La réception du SMS par votre appareil passera inaperçu et déclenchera la dissimulation des informations confidentielles.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra le SMS et les informations confidentielles seront masquées.

Pour activer à distance la dissimulation des informations confidentielles à l'aide d'une instruction spéciale envoyée par SMS, procédez comme suit :

1. Sous l'onglet **Avancé**, sélectionnez l'option **Instr. env.**.

   L'écran d'envoi de l'instruction SMS spéciale s'ouvre.

2. Cliquez sur **Démarrer**.

3. Choisissez l'instruction **Contacts personnels** et cliquez sur **Suivant** (cf. ill. ci-après).

Figure 52 : lancement à distance de Contacts personnels

4. Saisissez le numéro de l'appareil auquel vous envoyez l'instruction SMS, puis cliquez sur **Suivant**.

5. Saisissez le code secret de l'application spécifié sur l'appareil destinataire de l'instruction SMS et appuyez sur **Envoi**.

Quand l'appareil aura reçu l'instruction par SMS, la dissimulation des informations confidentielles sera activée automatiquement.

- *Pour activer à distance la dissimulation des informations confidentielles à l'aide de la fonction standard de rédaction de SMS, procédez comme suit :*

  envoyez à l'appareil un SMS contenant le texte `hide:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil récepteur). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

La liste des contacts contient les numéros confidentiels dont les informations et les événements sont masqués par le composant Contacts personnels. La liste des numéros peut être enrichie manuellement, via importation depuis les contacts ou depuis la carte SIM

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter à la Liste de contacts des numéros de téléphone et des contacts quelconques, des données enregistrées sur la carte SIM ou dans le répertoire téléphonique de l'appareil.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour ajouter un enregistrement à la Liste de contacts, procédez comme suit :

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.

2. Exécutez une des opérations suivantes (cf. ill. ci-après) :

   - Pour ajouter un numéro quelconque, choisissez l'option **Options** → **Ajouter entrée** → **Numéro**. Dans l'écran **Numéro** qui s'ouvre, remplissez le champ **Saisissez le numéro**. Après avoir saisi, cliquez sur **OK**.

   - Pour ajouter un numéro depuis le répertoire téléphonique, choisissez l'option **Options** → **Ajouter entrée** → **Contacts**. Dans l'écran **Contacts** qui apparaît, sélectionnez le contact requis dans le répertoire via le menu **Options** → **Sélectionner**. Après avoir saisi, cliquez sur **OK**.

   - Pour ajouter un numéro enregistré sur la carte SIM, choisissez **Options** → **Ajouter entrée** → **Contact de la carte SIM**. Sur l'écran **Contact de la carte SIM** qui apparaît, choisissez le numéro requis dans la liste des numéros de la carte SIM à l'aide de l'option **Options** → **Sélectionner**. Après avoir saisi, cliquez sur **OK**.

Figure 53: ajout d'un enregistrement à la liste des contacts protégés

3. Appuyez sur **Précédent** pour enregistrer les modifications.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Seuls les numéros qui ont été saisis manuellement dans la liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans le répertoire ou dans la liste des numéros de la carte SIM.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

- *Pour modifier le numéro dans la Liste de contacts, procédez comme suit :*

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez le numéro à modifier dans la Liste de contacts, puis choisissez **Options** → **Modifier entrée**.

   Le numéro de téléphone du contact sélectionné apparaît à l'écran.

3. Modifiez les données dans le champ **Saisissez le numéro**.

4. Une fois la modification terminée, cliquez sur **OK**.

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro ou effacer tout le contenu de la Liste de contacts.

- *Pour supprimer un numéro de la Liste de contacts, procédez comme suit :*

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez le numéro dans la liste, puis choisissez **Options** → **Supprimer entrée**.

3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

- *Pour purger la Liste de contacts, procédez comme suit :*

1. Sélectionnez **Contacts personnels** l'option **Liste de contacts**.

   L'écran **Liste de contacts** apparaît.

2. Sélectionnez **Options** → **Tout supprimer**.

3. Confirmez la suppression. Pour ce faire, cliquez sur **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

La fonction Contacts personnels masque par défaut les informations suivantes pour les numéros qui figurent dans la liste des contacts : contacts, SMS et entrées du journal des appels. Vous pouvez choisir les informations et les événements que la fonction Contacts personnels va dissimuler pour les numéros confidentiels.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

- *Pour choisir les informations et les événements à masquer pour les numéros confidentiels, procédez comme suit :*

1. Sélectionnez sous l'onglet **Contacts personnels** l'option **Obj. à masquer**.

L'écran **Objets à masquer** apparaît.

2. Sélectionnez les objets qui seront masqués pour les numéros confidentiels. Attribuez à chaque paramètre souhaité la valeur **Masquer** via l'option **Options** → **Modifier**. Il est possible de masquer les informations suivantes et les événements (cf. ill. ci-après) :

   - **Contacts** : toutes les informations relatives aux numéros confidentiels sont masquées dans le répertoire téléphonique.
   - **Messages** : tous les SMS entrants/sortants des numéros confidentiels sont masqués.
   - **Enreg. des appels** : accepte les appels en provenance des numéros confidentiels mais les masque et n'affiche pas les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).
   - **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité " occupé "). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.
   - **SMS entrants** : n'indique pas la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.

Figure 54: Sélection des objets cachés

3. Appuyez sur **Précédent** pour enregistrer les modifications.

FILTRAGE DE L'ACTIVITE DE RESEAU PARE-FEU

La section présente des informations sur le composant Pare-feu qui contrôle les connexions entrantes et sortantes sur votre périphérique. De plus, elle décrit comment activer/désactiver le composant et sélectionner le niveau de protection requis.

DANS CETTE SECTION

À PROPOS DU PARE-FEU

Le Pare-feu analyse toutes les connexions de réseau sur votre appareil. Il bloque ou autorise l'activité de réseau sur la base du niveau de protection sélectionné.

Le Pare-feu est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.0.

Pour connaître toutes les connexions bloquées, utilisez les notifications du Pare-feu (cf. la rubrique " Notification sur les tentatives de connexion " à la page 95).

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section " Journaux de l'application " à la page 106).

PRESENTATION DES NIVEAUX DE SECURITE DU PARE-FEU

Le fonctionnement du Pare-feu repose sur les niveaux de protection. Le niveau de sécurité permet de spécifier quels protocoles réseau sont autorisés, ou au contraire interdits, pour le transfert de données.

Les niveaux de sécurité suivants sont prévus :

- **Désact.** : autorisation de la moindre activité de réseau. Ce niveau de sécurité est choisi par défaut.
- **Les connexions entrantes sont interdites** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Les connexions sortantes des protocoles SSH, HTTP, HTTPS, IMAP, SMTP, POP3 sont autorisées** : toutes les connexions entrantes sont bloquées. La réception et l'envoi de courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Bloq. tout** : blocage de la moindre activité de réseau, à l'exception de la mise à jour des bases antivirus de l'application et du renouvellement de la licence.

Vous pouvez modifier le niveau de sécurité du Pare-feu (cf. la rubrique " Sélection du niveau de protection du Pare-feu " à la page 94). Le mode actuel est indiqué sur l'onglet Pare-feu à côté de l'option de menu **Mode**.

SELECTION DU NIVEAU DE SECURITE DU PARE-FEU

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour sélectionner le niveau de protection du Pare-feu, procédez comme suit :

1. Sélectionnez **Pare-feu**, choisissez l'option **Mode**.

L'écran **Mode** s'ouvre.

2. Sélectionnez un des niveaux de sécurité proposé (cf. ill. ci-après).

Figure 55: sélection du niveau de sécurité du Pare-feu

3. Appuyez sur **Précédent** pour enregistrer les modifications.

NOTIFICATION SUR LES TENTATIVES DE CONNEXION

Pare-feu bloque toutes les connexions interdites sur la base du mode de sécurité sélectionné (cf. la rubrique " Sélection du niveau de sécurité du Pare-feu " à la page 94). Pour que Pare-feu vous signale les connexions bloquées sur l'appareil, utilisez la fonction de notification du Pare-feu.

➧ *Pour recevoir des notifications sur les tentatives de connexions interdites par le niveau de sécurité choisi pour le Pare-feu, procédez comme suit :*

1. Sous l'onglet **Pare-feu**, choisissez l'option **Notification**.

2. Attribuez la valeur **Avertir** au paramètre **En cas de verrouillage** (cf. ill. ci-après).

Figure 56: configuration des notifications du Pare-feu

3. Appuyez sur **OK** pour enregistrer les modifications.

CHIFFREMENT DES DONNEES PERSONNELLES

Cette section fournit des informations sur le composant Chiffrement qui protège les données confidentielles sur votre appareil. De plus, la rubrique décrit comment activer/désactiver le composant et chiffrer/déchiffrer les dossiers sélectionnés.

DANS CETTE SECTION

À PROPOS DU CHIFFREMENT

Le composant Chiffrement protège les données sur l'appareil contre la consultation par des tiers même s'ils ont pu accéder à l'appareil nomade. Le composant permet de chiffrer n'importe quel nombre de dossiers qui ne sont pas du système.

Afin de déchiffrer les données, il faut saisir le code secret. Une fois que la période définie après le passage de l'appareil en mode d'économie de l'énergie est écoulée (cf. la rubrique " Interdiction d'accès aux données chiffrées " à la page 99), l'accès aux données sera bloqué automatiquement.

Le contenu du dossier est chiffré dès l'exécution de la commande **Chiffrer** après quoi les données sont chiffrées ou déchiffrées " au vol " au fur et à mesure que des données sont ajoutées, extraites ou consultées dans le dossier.

Le composant Chiffrement est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.0.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

CHIFFREMENT DES DONNEES

Le composant Chiffrement permet de chiffrer un nombre quelconque de dossiers non systèmes qui se trouvent dans la mémoire de l'appareil ou sur une carte mémoire.

La liste de tous les dossiers chiffrés ou déchiffrés antérieurement est accessible sur l'onglet **Chiffrement** via l'option **Liste des dossiers**.

Vous pouvez également chiffrer directement tous les dossiers qui se trouvent dans la liste des dossiers.

Pour chiffrer les données, procédez comme suit :

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Choisissez l'option **Options** → **Ajouter un dossier** (cf. ill. ci-après).

Figure 57: chiffrement des données

   L'écran reprenant l'arborescence du système de fichiers de l'appareil apparaît.

3. Sélectionnez le dossier qu'il faut absolument chiffrer, puis lancer le processus de chiffrement du dossier sélectionné. Pour ce faire, choisissez **Options** → **Chiffrer**.

   Pour vous déplacer dans le système de fichiers, utilisez le stylet ou les boutons du joystick de votre appareil : **Haut**, **Bas** – pour vous déplacer à l'intérieur du dossier sélectionné ; **Gauche**, **Droit** – pour monter ou descendre de niveau par rapport au dossier courant.

4. Appuyez sur **OK**.

   Le dossier chiffré sera ajouté à la liste des dossiers.

Une fois que la procédure de chiffrement sera terminée, l'option **Chiffrer** du menu **Options** deviendra **Déchiffrer**.

Après le chiffrement, les donnée sont déchiffrées et chiffrées automatiquement lorsque vous manipulez des données depuis un dossier chiffré, lorsque vous les extrayez du dossier chiffré ou y placer de nouvelles données.

- *Pour chiffrer directement tous les dossiers de la liste, procédez comme suit :*

1. Sélectionnez **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Options** → **Actions compl.** → **Tout chiffrer**.

3. Appuyez sur **OK**.

DÉCHIFFREMENT DES DONNÉES

Il est possible de déchiffrer complètement les données préalablement chiffrées (cf. la rubrique " Chiffrement de données " à la page 97) Vous pouvez déchiffrer un seul dossier ou tous les dossiers chiffrés sur l'appareil.

- *Pour déchiffrer un dossier chiffré, procédez comme suit :*

1. Sous l'onglet **Chiffrement**, sélectionnez l'option **Liste des doss.**.

   L'écran **Liste des dossiers** apparaît. Il reprend la liste de tous les dossiers chiffrés et déchiffrés antérieurement.

2. Sélectionnez dans la liste le dossier que vous voulez déchiffrer, puis choisissez l'option **Options** → **Déchiffrer** (cf. ill. ci-après).

Figure 58: déchiffrement des données

3. Cliquez sur **OK** à la fin du déchiffrement des données.

Une fois que la procédure de déchiffrement sera terminée, l'option **Déchiffrer** du menu **Options** du dossier sélectionné deviendra **Chiffrer**. Vous pouvez à nouveau utiliser le chiffrement de données (cf. la rubrique " Chiffrement de données " à la page 97).

Pour déchiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sous l'onglet **Chiffrement**, choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

2. Sélectionnez **Options** → **Actions compl.** → **Tout déchiffrer**.

3. Appuyez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le chiffrement permet de bloquer l'accès aux données chiffrées de manière instantanée ou à l'issue d'une période définie après le passage de l'appareil en mode d'économie d'énergie.

Par défaut, l'accès aux données chiffrées est bloqué directement après que le rétroéclairage de l'écran se coupe.

Vous pouvez définir la durée pendant laquelle les données chiffrées resteront accessibles après le passage de l'appareil en mode d'économie d'énergie. Pour manipuler les données chiffrées par la suite, il faudra saisir le code secret.

Vous pouvez également verrouiller momentanément l'accès aux données chiffrées et demander la saisie du code secret.

Pour bloquer l'accès au dossier après l'écoulement d'une durée définie, procédez comme suit :

1. Sélectionnez sous l'onglet **Chiffrement** l'option **Interdiction de l'accès**.

   L'écran **Interdiction de l'accès** s'ouvre.

2. Définissez la durée après le passage de l'appareil en mode de veille pendant laquelle les données seront accessibles. Pour ce faire, choisissez une des valeurs proposées (cf. ill. ci-après) :

   - **Sans délai**.
   - **1 minute**.
   - **5 minutes**.
   - **15 minutes**.

- **1 heure**.

Figure 59: blocage de l'accès aux données chiffrées

3. Appuyez sur **OK** pour enregistrer les modifications.

Pour interdire directement l'accès aux données chiffrées et activer la saisie du code secret,

appuyez simultanément sur les touches " 0 " et " 1 " de l'appareil.

MISE A JOUR DES BASES DU PROGRAMME

La section présente la mise à jour des bases antivirus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

DANS CETTE SECTION

À PROPOS DE LA MISE A JOUR DES BASES

La recherche d'application malveillante s'opère à l'aide de base de données qui contiennent les descriptions de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus.

Il est conseillé d'actualiser régulièrement les bases antivirus de l'application. Si plus de 15 jours se sont écoulés depuis la dernière mise à jour, les bases antivirus de l'application sont considérées comme étant fortement dépassées. Dans ces conditions, il est impossible de garantir la fiabilité de la protection.

Kaspersky Mobile Security 9.0 télécharge la mise à jour de l'application depuis les serveurs de mises à jour de Kaspersky Lab. Il s'agit de sites Internet spéciaux où sont hébergés les mises à jour des bases pour toutes les applications de Kaspersky Lab.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur l'appareil.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. Les bases antivirus de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial de Kaspersky Lab.

2. Kaspersky Mobile Security 9.0 exécute une des actions suivantes :

   - Si les bases antivirus de l'application que vous utilisez sont à jour, un message d'informations apparaît à l'écran.

   - Si les bases antivirus installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

     Une fois la mise à jour terminée, la connexion est automatiquement coupée. Si la connexion était déjà établie avant la mise à jour, elle reste alors disponible pour d'autres opérations.

Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres de la connexion à Internet ne sont pas définis automatiquement, configurez-les (cf. la rubrique " Configuration des paramètres de connexion à Internet " à la page 105).

Vous pouvez lancer la tâche de mise à jour manuellement à n'importe quel moment, si l'appareil n'est pas occupé par l'exécution d'autres tâches ou programmer l'exécution de la mise à jour.

En cas d'itinérance vous pouvez désactiver la mise à jour des bases antivirus de Kaspersky Mobile Security 9.0 pour réduire les dépenses.

La date d'édition des bases antivirus figure dans la fenêtre d'état de la protection (cf. la rubrique " Fenêtre de l'état de la protection " à la page 38). Les informations détaillées sur les bases antivirus utilisées sont accessibles sous l'onglet **Avancé** dans l'option du menu **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

AFFICHAGE D'INFORMATIONS SUR LES BASES

Vous pouvez consulter les informations sur les bases antivirus de l'application installées. Les données suivantes sont accessibles : date de la dernière mise à jour, date d'édition des bases et nombre d'enregistrements dans la base.

- *Pour consulter les informations relatives aux bases antivirus installées,*

  sous l'onglet **Avancé**, choisissez l'option **Infos des bases** (cf. ill. ci-après).

Figure 60: informations relatives aux bases de l'application installées

LANCEMENT MANUEL DE LA MISE A JOUR

Vous pouvez lancer manuellement la mise à jour des bases antivirus de l'application.

- *Pour lancer la mise à jour des bases manuellement, procédez comme suit :*

  1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

     L'écran **Mise à jour** s'ouvre.

2. Sélectionnez **Mise à jour** (cf. ill. ci-après).

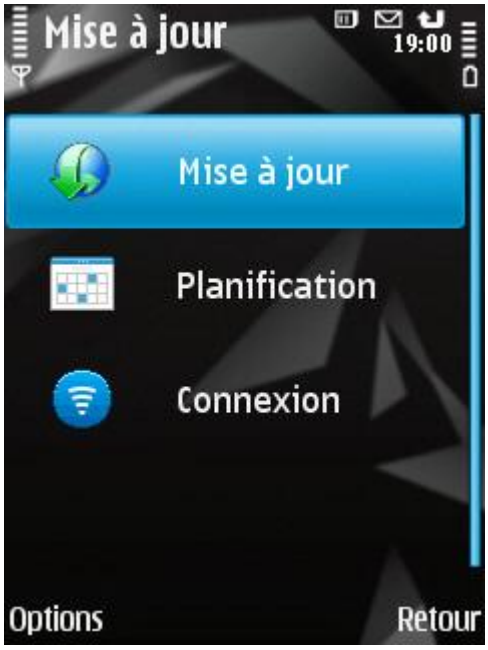


Figure 61: lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

LANCEMENT PROGRAMME DE LA MISE A JOUR

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Pour votre confort, vous pouvez configurer l'exécution automatique de la mise à jour des bases antivirus de l'application.

Vous pouvez également configurer les paramètres de mise à jour automatique si vous vous trouvez par exemple en itinérance (cf. la rubrique" Mise à jour en itinérance " à la page 104).

Pour configurer la mise à jour automatique des bases du logiciel, procédez de la manière suivante :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez au paramètre **Mise à jour auto** une des valeurs proposées (cf. ill. ci-après) :

   - **Désact.** : la mise à jour programmée des bases antivirus de l'application n'aura pas lieu.
   - **Chaque semaine** : actualise les bases antivirus de l'application une fois par semaine. Sélectionnez ensuite une des valeurs pour les paramètres **Jour de mise à jour** et **Heure de mise à jour**.

- **Chaque jour** : actualise les bases antivirus chaque jour. Saisissez ensuite la valeur pour le paramètre **Heure de mise à jour**.

Figure 62: Paramètres de la mise à jour automatique

4. Appuyez sur **Précédent** pour enregistrer les modifications.

MISE A JOUR EN ITINERANCE

Si vous êtes en itinérance, vous pouvez désactiver la mise à jour programmée des bases antivirus de l'application. La mise à jour manuelle reste disponible dans le mode normal.

Pour désactiver la mise à jour programmée des bases antivirus de l'application en cas d'itinérance, procédez comme suit :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Choisissez l'option **Planification**.

   L'écran **Planification** s'ouvre.

3. Attribuez la valeur **Non** au paramètre **Autoriser en itinérance** (cf. ill. ci-après).

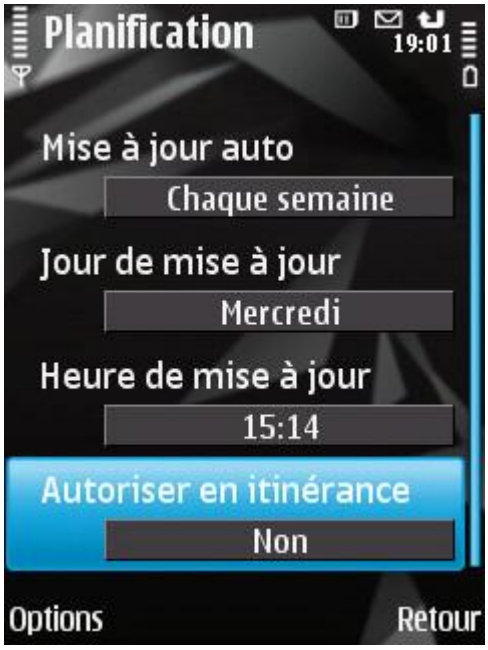


Figure 63 : configuration des mises en jour en itinérance

4. Appuyez sur **Précédent** pour enregistrer les modifications.

CONFIGURATION DES PARAMETRES DE CONNEXION A INTERNET

Pour se connecter à Internet, Kaspersky Mobile Security 9.0 utilise un point d'accès défini par défaut.

Les paramètres du point d'accès sont communiqués par le fournisseur.

Si Kaspersky Mobile Security 9.0 n'a pas défini automatiquement les paramètres de connexion, configurez-les.

Pour configurer les paramètres de connexion à Internet, procédez comme suit :

1. Sélectionnez **Mise à jour** sous l'onglet **Anti-Virus**.

   L'écran **Mise à jour** s'ouvre.

2. Sélectionnez l'option **Connexion**.

3. Sélectionnez le point d'accès utilisé pour vous connecter au serveur de mise à jour. Pour ce faire, sélectionnez la valeur du paramètre **Point d'accès**, puis appuyez sur **OK** (cf. ill. ci-après) :

La liste reprendra tous les points d'accès définis sur l'appareil nomade.

Figure 64: paramètres de connexion à Internet

4. Appuyez sur **Précédent** pour enregistrer les modifications.

JOURNAUX DU LOGICIEL

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus, etc.)

DANS CETTE SECTION

À PROPOS DES JOURNAUX

Les journaux reprennent les enregistrements sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Mobile Security 9.0. Les enregistrements sont triés par l'heure de l'événement et classés dans l'ordre chronologique.

Il existe un journal des événements pour chaque composant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

Pour consulter les enregistrements dans le journal du composant, procédez comme suit :

1. Sous l'onglet du composant requis, choisissez l'option **Journal**.

Le journal du composant sélectionné s'ouvre (cf. ill. ci-après).

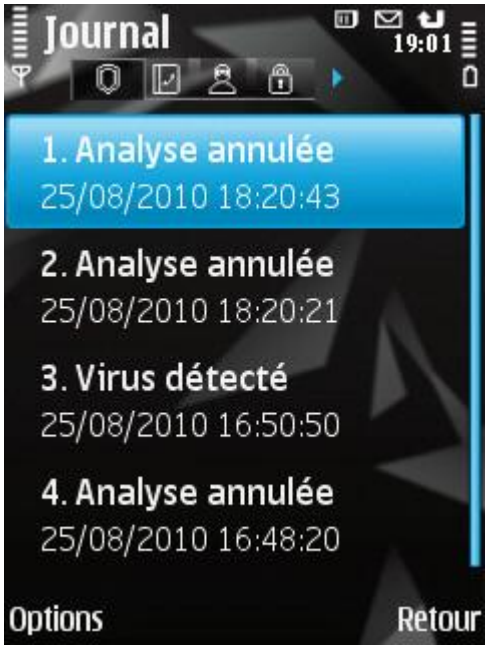


Figure 65: journal du composant sélectionné

2. Naviguez dans le journal à l'aide du stylet ou des boutons du joystick : **Haut** et **Bas** pour consulter les événements dans le journal en cours et **Gauche** et **Droite** pour consulter les événements dans les journaux des autres composants.

Pour afficher des informations détaillées sur les enregistrements du journal,

sélectionnez l'enregistrement requis, puis choisissez **Options** → **Afficher les informations**.

SUPPRESSION D'EVENEMENTS DANS LES JOURNAUX

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Mobile Security 9.0 seront supprimées.

Pour supprimer tous les événements des journaux, procédez comme suit :

1. Sous l'onglet de n'importe quel composant, choisissez l'option **Journal**.

   L'écran **Journal** s'ouvre.

2. Sélectionnez **Options** → **Effacer le journal**.

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section offre des informations sur les possibilités complémentaires de Kaspersky Mobile Security 9.0 : comment modifier le code secret, administrer les notifications sonores de l'application, le rétroéclairage et comment activer/désactiver l'affichage des astuces, de l'icône de la protection ou de la fenêtre d'état de la protection.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret de l'application défini après l'installation.

Pour changer le code secret de l'application, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Choisissez le paramètre **Changer le code**.

3. Saisissez le code actuel dans le champ **Saisissez le code**, puis cliquez sur **OK**.

4. Saisissez le nouveau code dans le champ **Saisissez le nouveau code**, puis cliquez sur **OK**.

5. Saisissez à nouveau le code dans le champ **Confirmation du code**, puis cliquez sur **OK**.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Mobile Security 9.0 affiche par défaut des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Mobile Security 9.0.

Pour configurer l'affichage des astuces, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :

   - **Afficher** : affiche l'astuce avant de configurer les paramètres de la fonction sélectionnée.

   - **Masquer** : aucune astuce n'est affichée.

3. Appuyez sur **Précédent** pour enregistrer les modifications.

NOTIFICATIONS SONORES

Divers événements définis peuvent survenir durant l'utilisation de l'application : découverte d'un objet infecté ou d'un virus, expiration de la licence, etc. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Par défaut, Kaspersky Mobile Security 9.0 active la notification sonore uniquement selon le mode défini de l'appareil.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour administrer les notifications sonores de l'application, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Notifications sonores** (cf. ill. ci-après) :

   - **Toujours** : utilise les notifications sonores quel que soit le profil sélectionné de l'utilisateur.
   - **Selon le mode** : utilise la notification sonore en fonction du mode sélectionné pour l'appareil.
   - **Désactiver** : n'utilise pas les notifications sonores.

Figure 66 : contrôle des notifications sonores

3. Appuyez sur **Précédent** pour enregistrer les modifications.

CONTROLE DU RETRO ECLAIRAGE

Quand l'application exécute une tâche de protection, l'appareil puise dans son autonomie. Pour épargner la batterie durant l'exécution des tâches, l'application permet de désactiver automatiquement le rétroéclairage de l'écran.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer le rétroéclairage de l'écran pendant l'exécution des tâches, procédez comme suit :

1. Sélectionnez **Avancé**, choisissez l'option **Configuration**.

   L'écran **Configuration** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Rétro éclairage** (cf. ill. ci-après) :

   - **Selon le mode** : utilise le rétroéclairage en fonction du mode sélectionné pour l'appareil.
   - **Activé** : utilise toujours le rétroéclairage de l'écran.

Figure67 : contrôle du rétroéclairage

3. Appuyez sur **Précédent** pour enregistrer les modifications.

AFFICHAGE DE LA FENETRE D'ETAT

Vous pouvez activer ou désactiver l'affichage de la fenêtre d'état de protection au démarrage de l'application.

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour configurer l'affichage de la fenêtre d'état au démarrage de l'application, procédez comme suit.

1. Sélectionnez **Paramètres** dans l'onglet **Avancé**.

   L'écran **Paramètres** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Fenêtre d'état** (cf. ill. ci-après) :

   - **Afficher** : affiche la fenêtre d'état.

- **Masquer** : n'affiche pas la fenêtre d'état.

Figure68 : configuration de l'affichage de la fenêtre d'état

3. Appuyez sur **Précédent** pour enregistrer les modifications.

AFFICHAGE DE L'ICONE DE PROTECTION

Pour voir l'état de la protection, vous pouvez configurer l'affichage de l'icône de la protection sur l'écran de l'appareil mobile (cf. la rubrique " Icône de la protection " à la page 38).

Les valeurs des paramètres peuvent être modifiées à l'aide du stylet, joystick de l'appareil ou via l'option **Options** → **Modifier**.

Pour modifier les paramètres d'affichage de l'icône de la protection, procédez comme suit.

1. Sélectionnez l'option **Protection** sous l'onglet **Anti-Virus**.

   L'écran **Protection** s'ouvre.

2. Sélectionnez une des valeurs proposées pour le paramètre **Icône de protection** (cf. ill. ci-après) :

   - **Afficher partout** : affiche l'icône de la protection sur l'écran de l'appareil.
   - **Menu uniquement** : affiche l'icône de la protection uniquement lorsque le menu de l'appareil ou le menu de Kaspersky Mobile Security 9.0 est ouvert.

- **Ne pas afficher** : n'affiche pas l'icône de la protection.

Figure 69: paramètres d'affichage de l'icône de la protection

3. Appuyez sur **OK** pour enregistrer les modifications.

KASPERSKY MOBILE SECURITY 9.0 POUR MICROSOFT WINDOWS MOBILE

Cette section présente une description de l'utilisation de Kaspersky Mobile Security 9.0 pour les appareils nomades fonctionnant sous un des systèmes d'exploitation suivant :

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0, 6.1, 6.5.

DANS CETTE SECTION

INSTALLATION DE KASPERSKY MOBILE SECURITY 9.0

L'installation de l'application sur l'appareil nomade s'effectue en plusieurs étapes.

Avant de lancer l'installation, il est conseillé de quitter toutes les autres applications sur l'appareil nomade.

Pour installer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Connectez l'appareil nomade à l'ordinateur à l'aide de l'application Microsoft ActiveSync.

2. Exécutez une des opérations suivantes :

   - Si vous avez acheté l'application sur un cédérom, lancez l'installation automatique de Kaspersky Mobile Security 9.0 depuis ce cédérom.

   - Si vous avez obtenu le fichier d'installation via Internet, copiez-le sur l'appareil nomade. Pour ce faire, appliquez l'une des méthodes suivantes :

     - depuis le site Internet de Kaspersky Lab ;

     - avec l'application Microsoft ActiveSync ;

     - avec une carte d'extension mémoire.

     Exécutez l'installation (ouvrez le fichier CAB de la distribution dans l'appareil mobile).

3. Lisez le texte du contrat de licence conclu entre vous et Kaspersky Lab. Si vous acceptez les dispositions du contrat, cliquez sur **OK**. Kaspersky Mobile Security 9.0 sera installé dans l'appareil. Si vous n'êtes pas d'accord avec les dispositions du contrat de licence, cliquez sur **Annuler**.

4. Choisissez la langue de l'interface de Kaspersky Mobile Security 9.0, puis cliquez sur **OK**.

5. Pour terminer l'installation, redémarrez l'appareil. Pour ce faire, cliquez sur **Redémarrer**.

   L'application sera installée avec les paramètres recommandés par les experts de Kaspersky Lab.

DÉSINSTALLATION DE L'APPLICATION

Pour supprimer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Décryptez les données sur votre périphérique, si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security (cf. la rubrique " Déchiffrement des données " à la page 191).

2. Désactivez Contacts personnels (cf. la rubrique " Activation/désactivation du composant Contacts personnels " à la page 179).

3. Fermez Kaspersky Mobile Security 9.0. Pour ce faire, choisissez **Menu** → **Quitter**.

4. Désinstallation de Kaspersky Mobile Security 9.0. Pour ce faire, exécutez les actions suivantes :

   a. Cliquez sur **Démarrer** → **Configuration**.

b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système** (voir figure suivante).

*Figure 70: Onglet **Système***

c. Sélectionnez **Kaspersky Mobile Security** dans la liste des applications installées puis cliquez sur **Supprimer** (cf. ill. ci-après).

Figure 71: sélection de l'application à supprimer

d. Confirmez la suppression de l'application en cliquant sur le bouton **Oui** dans la fenêtre qui s'ouvre.

e. Saisissez le code secret puis cliquez sur **OK**.

f. Indiquez s'il faut conserver ou non les paramètres de l'application et les objets en quarantaine (cf. ill. ci-après) :

- Pour sauvegarder la configuration de l'application ou les objets en quarantaine, appuyez sur **Conserver**.
- Pour supprimer complètement une application, cliquez sur **Supprimer**.

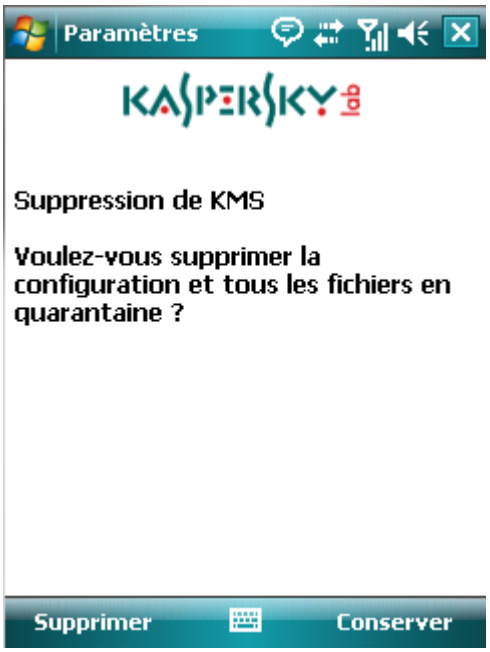


Figure 72: suppression des paramètres de l'application

5. Redémarrez l'appareil pour terminer la suppression de l'application.

MISE A JOUR DE L'APPLICATION

Vous pouvez mettre à jour Kaspersky Mobile Security 9.0 en installant la version la plus récente de cette génération (par exemple, réaliser la mise à jour de la version 9.0 à la version 9.2).

Si vous utilisez Kaspersky Mobile Security 8.0, vous pouvez passer à la version Kaspersky Mobile Security 9.0.

Pour mettre l'application à jour, procédez comme suit :

1. Désactivez le chiffrement - déchiffrez toutes les données (cf. rubrique " Déchiffrement des données " à la page 191).
2. Désactivez Contacts personnels (cf. la rubrique " Activation/désactivation du composant Contacts personnels " à la page 179).
3. Quittez la version actuelle de Kaspersky Mobile Security. Pour ce faire, choisissez **Menu** → **Quitter**.
4. Copiez le fichier d'installation de l'application sur l'appareil. Pour ce faire, appliquez l'une des méthodes suivantes :
   - depuis le site Internet de " Kaspersky Lab " ;
   - avec l'application Microsoft ActiveSync ;
   - avec une carte d'extension mémoire.
5. Exécutez le fichier d'installation de Kaspersky Mobile Security 9.0 sur l'appareil.

6. Lisez attentivement le contrat de licence. Si vous êtes d'accord avec tous les termes, appuyez sur **J'accepte**. Vous serez d'abord invité à supprimer la version de l'application installée.

7. Pour confirmer la suppression de la version antérieure, cliquez sur **OK**.

8. Saisissez le code secret.

9. Indiquez s'il faut utiliser ou non les paramètres de l'application et de l'objet pour la quarantaine :

   - Pour sauvegarder la configuration de l'application ou les objets en quarantaine, appuyez sur **Conserver**.

   - Pour supprimer complètement une application, cliquez sur **Supprimer**.

10. Pour terminer la suppression, redémarrez l'appareil. Pour ce faire, cliquez sur **Redémarrer**.

11. Après le redémarrage de l'appareil, lancez l'installation de Kaspersky Mobile Security 9.0 (cf. la rubrique " Installation de Kaspersky Mobile Security 9.0 " à la page 113).

    Si la durée de validité de la licence actuelle n'est pas écoulée, alors l'application sera activée automatiquement. Si la durée de validité de la licence est écoulée, activez l'application (cf. rubrique " Activation de l'application " à la page 118).

Pour passer de Kaspersky Mobile Security 8.0 à la version 9.0, procédez comme suit :

1. Déchiffrez toutes les données si elles avaient été chiffrées à l'aide de Kaspersky Mobile Security 8.0.

2. Fermez Kaspersky Mobile Security 9.0. Pour ce faire, choisissez **Menu** → **Quitter**.

3. Désinstallation de Kaspersky Mobile Security 9.0. Pour ce faire, exécutez les actions suivantes :

   a. Cliquez sur **Démarrer** → **Configuration**.

   b. Sélectionnez **Suppr. de progr.** dans l'onglet **Système**.

   c. Sélectionnez **Kaspersky Mobile Security** dans la liste des applications installées puis cliquez sur **Supprimer**.

   d. Confirmez la suppression de l'application en cliquant sur le bouton **Oui** dans la fenêtre qui s'ouvre.

   e. Saisissez le code secret défini dans la version antérieure de l'application, puis cliquez sur **OK**.

   f. Supprimez complètement les paramètres de Kaspersky Mobile Security 8.0 car ils sont incompatibles avec les paramètres de la version 9.0. Pour ce faire, cliquez sur **Supprimer**.

4. Redémarrez l'appareil pour terminer la suppression de Kaspersky Mobile Security 8.0.

5. Passez à l'installation de Kaspersky Mobile Security 9.0 (cf. rubrique " Installation de Kaspersky Mobile Security 9.0 " à la page 113).

6. Passez à l'activation de l'application (cf. rubrique " Activation de l'application " à la page 118).

   Si la licence pour Kaspersky Mobile Security 8.0 est toujours valide, activez la version 9.0 à l'aide du code d'activation de la version 8.0.

PREMIERS PAS

Cette section reprend les informations sur la préparation de Kaspersky Mobile Security 9.0 (activation et définition du code secret), le lancement de l'application, la mise à jour des bases antivirus et la recherche de virus.

DANS CETTE SECTION

ACTIVATION DU LOGICIEL

Avant de pouvoir utiliser Kaspersky Mobile Security 9.0, il faut l'activer.

Afin de pouvoir activer Kaspersky Mobile Security 9.0, la connexion à Internet doit être configurée sur l'appareil.

Avant d'activer l'application, assurez-vous que la date et l'heure système sont correctes.

Vous pouvez activer l'application d'une des manières suivantes :

- **Activer la version d'évaluation**. Lors de l'activation de la version d'évaluation de l'application, l'utilisateur reçoit une licence d'évaluation gratuite. La durée de validité de la licence d'évaluation est affichée à l'écran après l'activation. Une fois la durée de la licence d'évaluation écoulée, les possibilités de l'application sont réduites. Seules les fonctions suivantes sont accessibles :

  - activation du logiciel ;
  - administration de la licence de l'application ;
  - aide de Kaspersky Mobile Security 9.0 ;
  - désactivation de Chiffrement ;
  - désactivation de Contacts personnels.

  Il est impossible d'activer une deuxième fois la version d'évaluation.

- **Activer la version commerciale**. L'activation de la version commerciale s'opère à l'aide du code d'activation obtenu à l'achat de l'application. Dans le cadre de l'activation de la version commerciale, l'application obtient une licence commerciale qui permet d'utiliser toutes les fonctions de l'application. La durée de validité de la licence apparaît à l'écran de l'appareil. Une fois la licence parvenue à échéance, les fonctionnalités de l'application sont restreintes et la mise à jour de l'application n'a plus lieu.

  Vous pouvez obtenir le code d'activation d'une des manières suivantes :

  - en ligne, en passant de l'application Kaspersky Mobile Security 9.0 au site Web de Kaspersky Lab dédiés aux appareils mobiles ;
  - dans la boutique en ligne de Kaspersky Lab (http://kaspersky.telechargement.fr/cata_home.html)

- chez un revendeur de Kaspersky Lab.

- **Activer l'abonnement**. Lors de l'activation de l'abonnement, l'application reçoit une licence commerciale à abonnement. La durée de validité de la licence à abonnement est limitée à 30 jours. Dans le cadre de l'abonnement, l'application renouvelle la licence tous les 30 jours. Lors du renouvellement de la licence, la somme définie lors de l'activation de l'abonnement est débitée de votre compte personnel pour l'utilisation de l'application. Le paiement s'opère via l'envoi d'un SMS payant. Une fois que la somme a été débitée, l'application reçoit une nouvelle licence à abonnement du serveur d'activation. Toutes les fonctions sont à nouveau accessibles. Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9.0. Dans ce cas, à l'échéance de la validité de la licence, les fonctionnalités de l'application sont réduites. Les bases antivirus de l'application ne sont pas actualisées.

DANS CETTE SECTION

ACTIVATION DE LA VERSION D'ÉVALUATION

Pour activer la version d'évaluation de Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Choisissez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9.0** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

   L'écran **Activation** s'ouvre.
3. Sélectionnez **Version d'évaluation**.
4. Confirmez la connexion à Internet en cliquant sur **Oui**.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence.

   Si des erreurs se sont produites lors de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, contactez le service d'assistance technique.
5. Passez à la saisie du code secret de l'application (cf. rubrique " Saisie du code secret " à la page 121).

ACTIVATION DE LA VERSION COMMERCIALE

Pour activer la version commerciale de l'application à l'aide du code d'activation, procédez comme suit :

1. Choisissez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9.0** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

   L'écran **Activation** s'ouvre.
3. Choisissez l'option **Saisie du code**.

   L'écran d'activation de Kaspersky Mobile Security 9.0 apparaît (cf. ill. ci-dessous).

4. Saisissez le code d'activation obtenu dans les quatre champs, puis cliquez sur **Suivant**.

Figure 73: activation de la version commerciale de l'application

5. Confirmez la connexion à Internet en cliquant sur **Oui**.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade. Dans ce cas, vérifiez que le code d'activation saisi est correct, puis contactez la société où vous avez acheté le code d'activation de Kaspersky Mobile Security 9.0.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer les licences, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

6. Passez à la saisie du code secret de l'application (cf. rubrique " Saisie du code secret " à la page 121).

ACTIVATION DE L'ABONNEMENT A KASPERSKY MOBILE SECURITY 9.0

L'activation de l'abonnement requiert l'existence d'une connexion à Internet sur l'appareil.

Pour activer l'abonnement à Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9.0** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

   L'écran **Activation** s'ouvre.
3. Sélectionnez **Achat rapide**.
4. Confirmez la connexion à Internet en cliquant sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement. Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode d'activation de l'application.

Si le service d'abonnement est disponible, alors l'écran **Activation** s'affiche et présente les conditions générales de l'abonnement.

5. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9.0 en cliquant sur **Suivant**.

   L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9.0 vous prévient lorsque l'abonnement est activé.

   Si le solde de votre compte n'est pas suffisant pour envoyer le SMS payant, l'activation de l'abonnement est annulée.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

   Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Annuler**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir le mode d'activation de l'application.

6. Passez à la saisie du code secret (cf. rubrique " Saisie du code secret " à la page 121).

ACHAT DU CODE D'ACTIVATION EN LIGNE

Pour acheter le code d'activation de l'application en ligne, procédez comme suit :

1. Sélectionnez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9.0** et lancez l'application à l'aide du stylet ou du bouton central du joystick.

   L'écran **Activation** s'ouvre.

3. Sélectionnez **Acheter en ligne**.

   L'écran **Acheter en ligne** s'ouvre.

4. Appuyez sur **Ouvrir**.

   Le site Web de Kaspersky Lab pour les appareils mobiles s'ouvre. Vous pouvez y commander le renouvellement de la licence.

5. Suivez les instructions.
6. Une fois que vous aurez acheté le code d'activation, passez à l'activation de la version commerciale de l'application (cf. rubrique " Activation de la version commerciale " à la page 119).

SAISIE DU CODE SECRET

Après l'activation de l'application, vous serez invité à saisir le code secret de l'application. Le *code secret de l'application* permet d'éviter l'accès non autorisé aux paramètres de l'application. Vous pourrez modifier ultérieurement le code secret de l'application définit.

Il faut saisir le code secret de l'application dans les cas suivants :

- Pour accéder à l'application ;
- Pour accéder aux données cryptées ;
- Pour l'envoi d'une instruction à l'aide d'un SMS spécial dans le but de lancer à distance les fonctions suivante : verrouillage de l'appareil, suppression des données, SIM-Surveillance, Localisation, Contacts personnels ;

- Pour supprimer l'application.

Mémorisez le code secret de l'application. Si vous oubliez le code secret, vous ne pourrez plus gérer les fonctions de Kaspersky Mobile Security 9.0, ni obtenir l'accès aux données chiffrées, ni supprimer l'application.

Le code secret de l'application est composé de chiffres. Il doit être composé d'au moins 4 chiffres.

Pour saisir le code secret, procédez comme suit :

1. Apres l'activation de l'application dans la zone **Saisissez le nouveau code**, tapez les chiffres de votre code, appuyez sur OK.
2. Tapez de nouveau ce code dans la zone **Confirmer**.

   La robustesse du code saisi est vérifiée automatiquement.
3. Si la robustesse du code est jugée insuffisante, un message d'avertissement s'affiche et l'application demande une confirmation. Pour utiliser le code, cliquez sur **OK**. Pour définir un nouveau code, cliquez sur **Non**.
4. A la fin, cliquez sur **OK**.

DÉMARRAGE DU LOGICIEL

Pour installer Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Choisissez **Démarrer** → **Programmes**.
2. Sélectionnez **KMS 9.0** et lancez l'application à l'aide du stylet ou du bouton central du joystick.
3. Saisissez le code secret de l'application et cliquez sur **OK**.

La fenêtre d'état de la protection offerte par Kaspersky Mobile Security 9.0 (cf. la rubrique " Fenêtre d'état de la protection " à la page 131) apparaît à l'écran. Pour passer aux fonctions de l'application, appuyez sur **Menu**.

MISE A JOUR DES BASES DU PROGRAMME

Kaspersky Mobile Security 9.0 recherche les menaces à l'aide des bases antivirus de l'application qui contiennent la description de tous les programmes malveillants connus à ce jour ainsi que les moyens de les neutraliser. On y retrouve également les descriptions d'autres objets indésirables. Il se peut que les bases antivirus livrées avec Kaspersky Mobile Security 9.0 soient dépassées au moment de l'installation.

Il est conseillé d'actualiser les bases antivirus dès après l'installation de l'application.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur l'appareil.

Pour lancer la mise à jour des bases antivirus de l'application, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.
2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.
3. Sélectionnez l'option **Mise à jour**.

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

RECHERCHE DE VIRUS SUR L'APPAREIL

Une fois l'application installée, il est conseillé de lancer l'analyse complète de l'appareil mobile à la recherche d'éventuels objets malveillants.

La première analyse s'opère selon les paramètres définis préalablement par les experts de Kaspersky Lab.

Pour lancer l'analyse complète de l'appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez **Analyse complète**.

INFORMATIONS SUR LE PROGRAMME

Vous pouvez afficher des informations générales sur le logiciel, ainsi que les détails de version et de copyright.

Pour consulter les informations sur l'application, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Infos logiciel** (cf. ill. ci-après).

Figure 74: informations sur l'application

GESTION DE LA LICENCE

Dans le cadre de l'octroi de licences pour l'utilisation des applications de Kaspersky Lab, il est important de comprendre les notions suivantes :

- Le contrat de licence ;
- La licence.

Ces notions sont liées les unes aux autres et forment un ensemble unique.

Examinons chacune d'entre elles en détail.

La rubrique présente également des informations sur la manière de consulter les informations relatives à la licence de Kaspersky Mobile Security 9.0 et de la renouveler.

DANS CETTE SECTION

PRESENTATION DU CONTRAT DE LICENCE

Le *contrat de licence* est un contrat conclu entre d'une part une personnalité physique ou juridique détenant une copie légale de Kaspersky Mobile Security et Kaspersky Lab d'autre part. Ce contrat est proposé avec chaque application de Kaspersky Lab. Il présente en détail les droits et les restrictions d'utilisation de Kaspersky Mobile Security 9.0.

Conformément aux termes du contrat de licence, vous avez le droit de détenir une copie de l'application après avoir acheté et installé celle-ci.

Kaspersky Lab est également ravi de vous proposer les services complémentaires suivants :

- Assistance technique ;
- la mise à jour des bases antivirus de Kaspersky Mobile Security 9.0;
- Mise à jour des modules logiciels de Kaspersky Mobile Security 9.0.

Pour pouvoir l'obtenir, vous devez acheter et activer une licence (cf. la rubrique " Présentation des licences de Kaspersky Mobile Security 9.0 " à la page 124).

PRESENTATION DES LICENCES DE KASPERSKY MOBILE SECURITY 9.0

La *licence* est un droit octroyé pour l'utilisation de Kaspersky Mobile Security 9.0 et des services complémentaires (cf. rubrique " Présentation du contrat de licence " à la page 124) offerts par Kaspersky Lab ou ses partenaires.

Chaque licence se définit par sa durée de validité et son type.

La *durée de validité de la licence* désigne la période pendant laquelle vous pouvez bénéficier des services complémentaires :

- Assistance technique ;

- Mise à jour des bases antivirus et des modules de l'application.

Le volume des services proposés dépend du type de licence.

Les types de licence suivants existent :

- *Evaluation* : licence gratuite dont la validité est limitée, par exemple 30 jours, et qui permet de découvrir Kaspersky Mobile Security.

  La licence d'évaluation peut être utilisée une seule fois uniquement.

  La licence d'évaluation vous permet de contacter le service d'assistance technique uniquement pour les questions relatives à l'activation de l'application ou à l'achat de la licence commerciale. Une fois la licence d'évaluation expirée, Kaspersky Mobile Security 9.0 arrête de fonctionner. Pour pouvoir continuer à utiliser l'application, il faut l'activer (cf. rubrique " Activation de la version commerciale " à la page 119).

- *Commerciale* : licence payante avec une durée de validité définie (par exemple, un an) octroyée à l'achat de Kaspersky Mobile Security 9.0.

  Toutes les fonctionnalités de l'application et les services complémentaires sont accessibles pendant la période de validité de la licence commerciale.

  Une fois que la licence commerciale a expiré, certaines fonctionnalités de Kaspersky Mobile Security 9.0 deviennent inaccessibles et les bases antivirus de l'application ne seront plus actualisées. Sept jours avant l'expiration de la licence, l'application affichera une notification. Vous aurez ainsi le temps de renouveler la licence.

- *Commerciale avec abonnement* : licence payante offrant une possibilité de renouvellement automatique ou manuel. La licence à abonnement est proposée aux prestataires de services.

  L'abonnement a une validité limitée (30 jours). Une fois que l'abonnement expire, il peut être renouvelé manuellement ou automatiquement. Le mode de renouvellement de l'abonnement dépend de la législation en vigueur et de l'opérateur de téléphonie mobile. L'abonnement est renouvelé automatiquement si le prépaiement du prestataire de service a été réalisé.

  Lors du renouvellement de l'abonnement, le montant défini dans les conditions générales de l'abonnement est débité de votre compte personnel. La somme est débitée de votre compte personnel via un SMS payant envoyé au numéro du prestataire de service.

  Si l'abonnement n'est pas renouvelé, Kaspersky Mobile Security 9.0 ne réalise plus la mise à jour des bases antivirus de l'application et les fonctionnalités de l'application sont limitées.

  Si vous choisissez l'abonnement, vous pouvez activer la licence commerciale via le code d'activation. Dans ce cas, l'abonnement sera automatiquement annulé.

  Vous pouvez activer un abonnement si vous utilisez une licence commerciale. Si au moment d'activer l'abonnement vous aviez déjà activé la licence à durée déterminée, cette licence sera remplacée par une licence à abonnement.

AFFICHAGE DES INFORMATIONS DE LICENCE

Vous pouvez consulter les informations suivantes sur la licence : le numéro de licence, le type, le nombre de jours restant avant l'expiration, la date d'activation et le numéro de série de l'appareil.

Pour consulter les informations sur la licence, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Licence**.

L'écran **Licence** s'ouvre.

3. Sélectionnez **Infos licence** dans l'onglet.

RENOUVELLEMENT DE LA LICENCE

Kaspersky Mobile Security 9.0 permet de renouveler la durée de validité de la licence de l'application.

Vous pouvez renouveler la licence d'une des méthodes suivantes :

- saisir le code d'activation : activation de la licence à l'aide d'un code d'activation. Le code d'activation est disponible à l'achat sur le site http://kaspersky.telechargement.fr/cata_home.html ou chez un distributeur Kaspersky Lab.
- acheter le code d'activation en ligne. Accédez au site Web ouvert sur votre appareil mobile et achetez le code d'activation en ligne.
- s'abonner à Kaspersky Mobile Security 9.0. Activez l'abonnement afin de renouveler la durée de validité de la licence tous les 30 jours.

Pour pouvoir actualiser les bases de l'application sur l'appareil mobile, la connexion à Internet doit être configurée.

DANS CETTE SECTION

RENOUVELLEMENT DE LA LICENCE A L'AIDE DU CODE D'ACTIVATION

Pour renouveler la licence à l'aide du code d'activation, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

3. Choisissez l'option **Renouveler**.

   L'écran **Renouveler** s'ouvre.

4. Saisissez le code d'activation obtenu dans les quatre champs, puis cliquez sur **Suivant** (cf. ill. ci-après).

Figure 75 : renouvellement de la licence à l'aide d'un code d'activation

5. Confirmez la connexion à Internet en cliquant sur **Oui**.

   L'application envoie une requête au serveur d'activation de Kaspersky Lab et reçoit la licence. Après avoir reçu la licence, les informations relatives à celle-ci sont affichées sur l'écran.

   Si le code que vous avez saisi est incorrect pour une raison quelconque, le message de circonstance apparaîtra à l'écran de l'appareil nomade.

6. A la fin, cliquez sur **OK**.

RENOUVELLEMENT DE LA LICENCE EN LIGNE

Pour renouveler l'application en ligne, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

3. Choisissez l'option **Renouveler en ligne**. Si la validité de la licence est écoulée, l'option du menu deviendra **Acheter en ligne**.

   L'écran **Renouveler en ligne** s'ouvre.

4. Appuyez sur **Ouvrir** (cf. ill. ci-dessous).

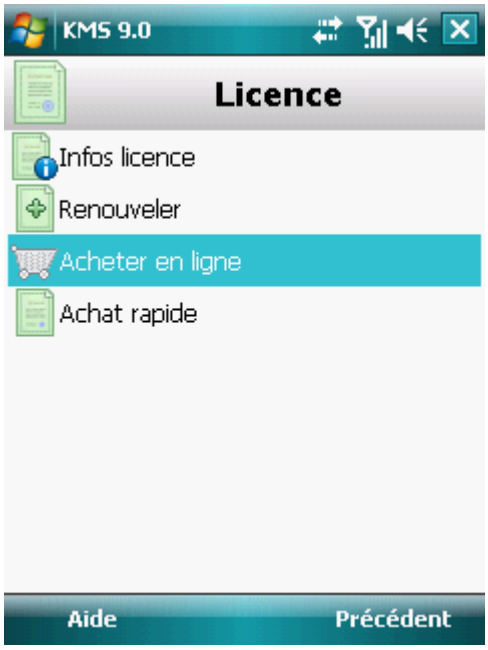


Figure 76: renouvellement de la licence en ligne

Cette action entraîne l'ouverture d'un site où vous serez invité à commander le renouvellement de la licence.

Si la durée de validité de la licence est écoulée, alors le site Web de Kaspersky Lab pour appareils mobiles s'ouvre. Vous pouvez y acheter le code d'activation en ligne.

5. Suivez les instructions.

6. Une fois que la commande du renouvellement de la licence aura été passée, saisissez le code d'activation reçu (cf. rubrique " Renouvellement de la licence à l'aide d'un code d'activation " à la page 126).

RENOUVELLEMENT DE LA LICENCE A L'AIDE DE L'ACTIVATION DE L'ABONNEMENT

Vous pouvez activer l'abonnement à Kaspersky Mobile Security 9.0 avant l'expiration de la version d'évaluation de l'application. Dans le cadre de l'abonnement, Kaspersky Mobile Security 9.0 renouvelle la validité de la licence tous les mois. Lors de chaque renouvellement de la licence, le montant défini dans les conditions générales de l'abonnement est débité chaque mois de votre compte personnel.

L'activation de l'abonnement à Kaspersky Mobile Security 9.0, requiert une connexion à Internet.

Pour activer l'abonnement à Kaspersky Mobile Security 9.0, procédez de la manière suivante :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

Choisissez l'option **Achat rapide** (cf. ill. ci-après).

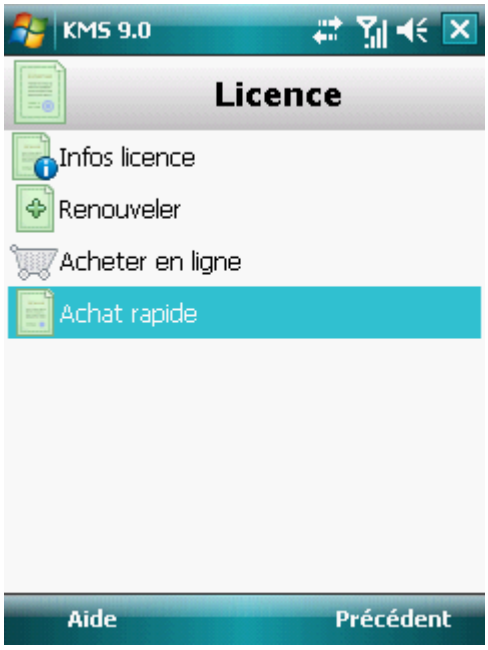


Figure 77 : activation de l'abonnement

3. Confirmez la connexion à Internet en cliquant sur **Oui**.

   L'application vérifie si votre opérateur de téléphonie mobile a accès au service d'abonnement.

   Si le service d'abonnement est disponible, alors l'écran **Activation** s'affiche et présente les conditions générales de l'abonnement.

   Si le service d'abonnement n'est pas offert, l'application vous le signale et revient à l'écran où vous pourrez choisir un autre mode de renouvellement de la licence.

4. Lisez les conditions de l'abonnement, puis confirmez l'activation de l'abonnement à Kaspersky Mobile Security 9.0 en cliquant sur **Suivant**.

   L'application envoie un SMS payant, puis reçoit la licence depuis le serveur d'activation de Kaspersky Lab. Kaspersky Mobile Security 9.0 vous prévient lorsque l'abonnement est activé.

   Si le solde de votre compte n'est pas suffisant pour envoyer le SMS payant, l'activation de l'abonnement est annulée.

   Si des erreurs se sont produites au moment de la connexion au serveur et qu'il n'a pas été possible de récupérer la licence, l'activation sera annulée. Dans ce cas, il est conseillé de vérifier les paramètres de connexion à Internet. Si les erreurs n'ont pas pu être supprimées, contactez le service d'assistance technique.

   Si vous n'acceptez pas les conditions générales de l'abonnement, cliquez sur **Annuler**. L'application annule dans ce cas l'activation et revient à l'écran où vous pouvez choisir un autre mode de renouvellement de la licence.

5. A la fin, cliquez sur **OK**.

REFUS DE L'ABONNEMENT

Vous pouvez refuser l'abonnement à Kaspersky Mobile Security 9.0. Dans ce cas Kaspersky Mobile Security 9.0 ne renouvelle pas la validité de la licence tous les 30 jours. À l'échéance de la licence en cours de validité, les fonctionnalités de l'application sont réduites et les bases antivirus de l'application ne sont pas mises à jour.

Si vous avez refusé l'abonnement, sachez que vous pourrez le reprendre (cf. rubrique " Renouvellement de l'abonnement " à la page 130).

Pour refuser l'abonnement à Kaspersky Mobile Security 9.0, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

3. Choisissez l'option **Annulation de l'abonnement** (cf. ill. ci-après).

Figure 78 : refus de l'abonnement

4. Confirmez le refus de l'abonnement en cliquant sur **Oui**.

Kaspersky Mobile Security 9.0 vous signale que l'abonnement a été annulé.

RENOUVELLEMENT DE L'ABONNEMENT

Si vous aviez refusé l'abonnement (cf. rubrique " Refus de l'abonnement " à la page 129), vous pourrez le renouveler. Dans ce cas, Kaspersky Mobile Security 9.0 renouvellera la durée de validité de la licence tous les 30 jours.

En cas de renouvellement de l'abonnement, le montant requis sera débité de votre compte personnel uniquement si la licence actuelle expire dans moins de trois jours.

Pour renouveler l'abonnement, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Licence**.

   L'écran **Licence** s'ouvre.

3. Choisissez l'option **Achat rapide**.

Si la licence actuelle est arrivée à échéance, alors, Kaspersky Mobile Security 9.0 propose d'activer à nouveau l'abonnement (cf. rubrique " Renouvellement de la licence " à la page 126).

Si la licence actuelle est toujours valide, alors Kaspersky Mobile Security 9.0 renouvelle l'abonnement et quand la licence actuelle arrive à échéance, il la renouvelle tous les 30 jours.

INTERFACE DE L'APPLICATION

L'interface de Kaspersky Mobile Security 9.0 est simple et conviviale. Cette section présente des informations sur les principaux composants de l'interface.

DANS CETTE SECTION

FENETRE D'ETAT DE LA PROTECTION

L'état des composants principaux de l'application s'affiche dans la fenêtre de l'état de la protection.

Il existe trois états possibles pour chaque composant. Chacun d'entre eux est associé à une couleur définie, comme les feux de circulation. Le vert signifie que la protection de l'appareil est assurée au niveau requis. Le jaune et le rouge indiquent qu'il y a différents types de menaces contre la sécurité. Les menaces sont non seulement les applications malveillantes, mais également les bases antivirus de l'application dépassée, certains composants désactivés, les paramètres minimes de fonctionnement de l'application, etc.

La fenêtre de l'état de la protection est accessible directement après le lancement de l'application et reprend les informations suivantes :

- **Protection** : état de la protection en temps réel (cf. la rubrique " Protection en temps réel " à la page 134).

  L'icône verte de l'état indique que la protection est activée et assurée au niveau requis. Les bases antivirus de l'application sont à jour.

  L'icône jaune signale que la mise à jour des bases antivirus n'a plus eu lieu depuis quelques jours.

  L'icône rouge signale des problèmes qui pourraient entraîner la perte d'informations ou l'infection de l'appareil. Par exemple, la protection est désactivée. Il se peut que les bases de l'application n'ait plus été actualisées plus de 15 jours.

- **Pare-feu** : le niveau de protection de l'appareil contre l'activité de réseau indésirable (cf. la rubrique " Filtrage de l'activité de réseau. Pare-feu " à la page 186).

  L'icône verte de l'état signifie que le composant est activé. Le niveau de protection du pare-feu a été sélectionné.

  Une icône rouge indique que le filtrage de l'activité de réseau n'a pas lieu.

- **Antivol** : état de la protection des données en cas de vol ou de perte de l'appareil (cf. la rubrique " Protection des données en cas de perte ou de vol de l'appareil " à la page 166).

  L'icône verte signifie que les fonctions de l'Antivol dont le nom apparaît sous l'état du composant sont activées.

  L'icône rouge indique que toutes les fonctions d'antivol sont désactivées.

- **Contacts personnels** : état de la protection des données confidentielles (cf. la rubrique " Dissimulation des données personnelles " à la page 177).

L'icône verte de l'état signifie que le composant est activé. Les données confidentielles sont masquées.

L'icône jaune prévient l'utilisateur que le composant est désactivé. Les données personnelles sont visibles et peuvent être consultées.

- **Licence** : durée de validité de la licence (cf. la rubrique " Administration des licences " à la page 124).

  L'icône verte d'état indique que la licence est valide pendant encore plus de 14 jours.

  L'icône jaune indique que la licence est valide pour moins de 14 jours.

  L'icône rouge indique que la validité de la licence est écoulée.

Figure 79 : La fenêtre d'état des composants du programme

Vous pouvez aussi passer à la fenêtre de l'état de la protection en choisissant l'option **Menu** → **Etat de la protection**.

MENU DE L'APPLICATION

Les composants de l'application sont regroupés logiquement et accessibles dans le menu de l'application. Chaque option du menu permet d'accéder aux paramètres du composant sélectionné ainsi qu'aux tâches de la protection (cf. ill. ci-après).

Figure 80: menu de l'application

Le menu de Kaspersky Mobile Security 9.0 propose les options suivantes :

- **Antivirus** : protection du système de fichiers contre les virus, analyse à la demande et actualisation des bases antivirus de l'application.
- **Antivol** : blocage de l'appareil et suppression des informations en cas de vol ou de perte.
- **Contacts personnels** : dissimulation des données confidentielles sur l'appareil.
- **Chiffrement** : protection des données sur l'appareil grâce au chiffrement.
- **Anti-Spam** : filtrage des SMS et des appels entrants non sollicités.
- **Contrôle Parental** : contrôle des SMS et des messages sortants.
- **Pare-feu** : protection de réseau de l'application.
- **Avancé** : paramètres généraux de l'application, informations sur l'application, sur les bases antivirus utilisées et sur la licence.
- **Etat de protection** : informations sur l'état de la protection de l'appareil.
- **Quitter** : fin de l'utilisation de l'application.

Pour ouvrir le menu de l'application,

sélectionnez **Menu**.

Pour naviguer dans le menu de l'application, utilisez le joystick de l'appareil ou le stylet.

- *Pour revenir à la fenêtre d'état des composants logiciels,*

  sélectionnez **Menu** → **Etat de protection**.

- *Pour quitter le programme,*

  choisissez **Menu** → **Quitter**.

PROTECTION DU SYSTÈME DE FICHIERS

La rubrique présente des informations sur le composant Protection qui permet d'éviter l'infection du système de fichiers de l'appareil. Elle explique comment activer / suspendre la Protection et la configurer.

DANS CETTE SECTION

PRESENTATION DE LA PROTECTION

La protection se charge en même temps que le système d'exploitation et s'exécute dans la mémoire de l'appareil, pour analyser tous les fichiers ouverts, enregistrés ou exécutés. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte toutes les tentatives d'accès aux fichiers de la part de l'utilisateur ou d'un autre programme.

2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés comparant aux bases antivirus utilisées par le logiciel. Les bases antivirus de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

3. Après l'analyse, Kaspersky Mobile Security 9.0 peut appliquer les actions suivantes :

   - quand du code malveillant est découvert dans le fichier, l'application le bloque et agit conformément aux paramètres définis ;

   - si aucun code malveillant n'est découvert, le fichier est immédiatement restitué.

Les informations sur les résultats de l'analyse sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

ACTIVATION ET DESACTIVATION DE LA PROTECTION

Lorsque la protection est activée, toutes les actions exécutées dans le système sont placées sous un contrôle permanent. La protection contre les objets malveillants usent les ressources de l'application. Pour diminuer la charge sur l'appareil lors de l'exécution de plusieurs tâches, vous pouvez suspendre temporairement la protection.

Les spécialistes de Kaspersky Lab recommandent vivement de ne pas désactiver la protection car cela pourrait entraîner l'infection de l'appareil et la perte de données.

L'état actuel de la protection est repris sur l'écran **Anti-Virus** à côté de l'option de menu **Protection**.

Vous pouvez activer/désactiver la protection d'une des méthodes suivantes :

- depuis le menu de configuration du composant ;
- depuis le menu **Anti-Virus**.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour désactiver la protection, procédez de la manière suivante :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Paramètres** s'ouvre.

3. Cochez la case **Activer la protection** (cf. ill. ci-après).

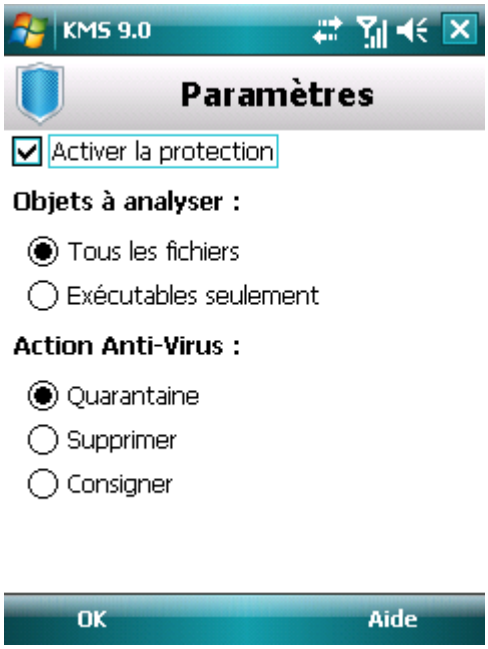


Figure 81 : activation de la protection

4. Appuyez sur **OK** pour enregistrer les modifications.

Pour désactiver la protection, procédez de la manière suivante :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Paramètres** s'ouvre.

3. Désélectionnez la case **Activer la protection**.

4. Appuyez sur **OK** pour enregistrer les modifications.

Pour activer/désactiver la protection, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.
2. L'écran **Anti-Virus** apparaît.
3. Appuyez sur **Activer** / **Désactiver**. Le texte du bouton prendra la valeur opposée en fonction de l'état actuel de la protection.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9.0 met les objets malveillants découverts en quarantaine. Vous pouvez modifier l'action qui sera exécutée par l'application en cas de découverte d'un objet malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour modifier la valeur des paramètres de la protection, assurez-vous qu'elle est activée.

Pour configurer la réponse du programme en présence d'un objet malveillant, procédez de la manière suivante (voir figure suivante) :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Protection**.

   L'écran **Paramètres** s'ouvre.

3. Définissez l'action que l'application exécutera en cas de découverte d'un objet malveillant. Pour ce faire, attribuez une valeur au paramètre Si un virus est découvert (cf. ill. ci-après) :

   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

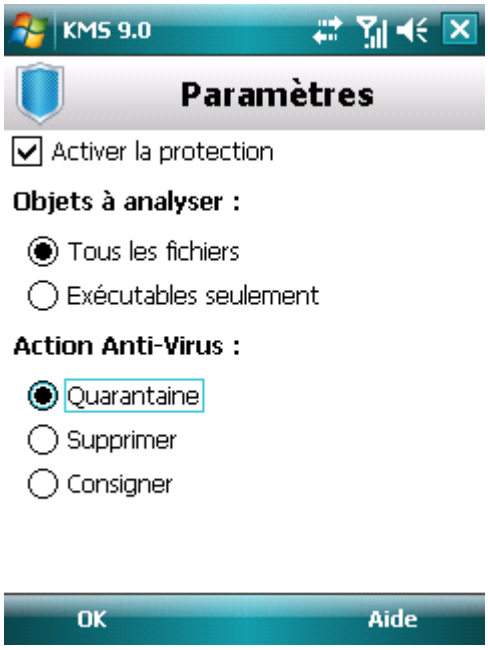


Figure 82 : Sélection de l'action appliquée à un objet

4. Appuyez sur **OK** pour enregistrer les modifications.

ANALYSE DE L'APPAREIL

La section reprend les informations sur la recherche des objets malveillants qui permet d'identifier et de neutraliser les menaces sur votre appareil. La section décrit également comment lancer la tâche d'analyse, comment programmer l'exécution de la tâche, comme sélectionner les objets à analyser et comment définir l'action que l'application exécutera sur la menace identifiée.

DANS CETTE SECTION

À PROPOS DE L'ANALYSE A LA DEMANDE

L'analyse de l'appareil permet d'identifier et de neutraliser les objets malveillants. Kaspersky Mobile Security 9.0 est capable de réaliser une analyse complète ou partielle de l'appareil. Autrement dit, il peut analyser uniquement le contenu de la mémoire intégrée de l'appareil ou un dossier en particulier (y compris les dossiers sur les cartes mémoire).

L'analyse de l'appareil s'opère selon l'algorithme suivant :

1. Kaspersky Mobile Security 9.0 analyse les fichiers d'un type défini (cf. la rubrique " Sélection des types de fichiers à analyser " à la page 140).

2. Le fichier est analysé à la recherche d'objets malveillants. Les objets malveillants sont détectés comparant aux bases de données utilisées par le logiciel. Les bases de données contiennent la description et les méthodes de réparation de tous les objets malveillants connus jusqu'à ce jour.

   Selon les résultats de l'analyse, Kaspersky Mobile Security 9.0 peut adopter les comportements suivants :

   - Quand un code malveillant est découvert dans un fichier, Kaspersky Mobile Security 9.0 bloque le fichier et exécute l'action sélectionnée conformément aux paramètres définis (cf. la rubrique " Sélection des actions à appliquer sur des objets " à la page 142).

   - Si aucun code malveillant n'est découvert, le fichier peut être directement manipulé.

La tâche d'analyse est lancée manuellement ou automatiquement selon un horaire défini (cf. rubrique " Exécution de l'analyse programmée " à la page 139).

Les informations sur les résultats de l'analyse à la demande sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

EXECUTION MANUELLE D'UNE ANALYSE

Vous pouvez lancer une analyse manuellement, par exemple lorsque le processeur de l'application n'est pas occupé par l'exécution d'autres tâches.

Pour lancer une analyse antivirus, procédez de la manière suivante :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez la zone d'analyse de l'appareil (cf. ill. ci-après) :

   - **Analyse complète** : analyse tout le système de fichiers de l'application. Les objets suivants sont analysés par défaut : mémoire de l'appareil et carte mémoire.

   - **Analyse de la mémoire** : analyse les processus lancés dans la mémoire système et les fichiers correspondants.

- **Analyser dossier** : analyse un objet distinct du système de fichiers de l'appareil ou sur une carte mémoire. La sélection de l'option **Analyser dossier** ouvre un écran qui présente le système de fichier de l'appareil. Utilisez le stylet ou les boutons du joystick pour vous déplacer dans le système de fichiers. Pour lancer l'analyse du dossier, sélectionnez le dossier requis, puis appuyez sur **Analyser**.

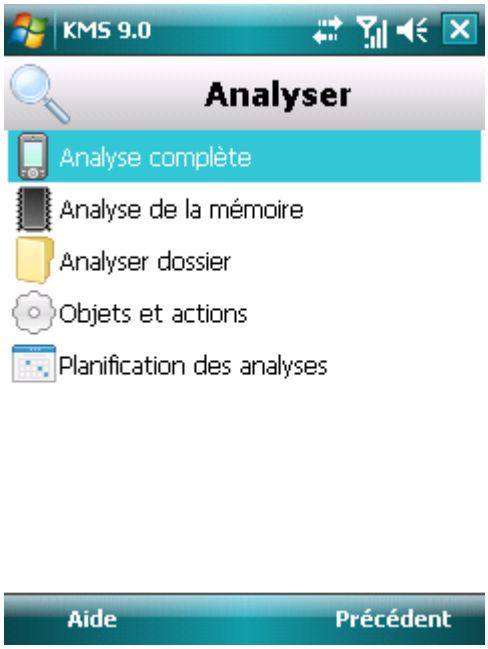


Figure 83: sélection de la zone d'analyse

Après le démarrage de l'analyse, une fenêtre affiche l'état actuel de la tâche : nombre d'objets analysés, chemin de l'objet en cours d'analyse.

Si Kaspersky Mobile Security 9.0 découvre un objet infecté, il exécute l'action conformément aux paramètres d'analyse définis (cf. la rubrique " Sélection des actions à appliquer sur les objets identifiés " à la page 142).

Par défaut, Kaspersky Mobile Security place en quarantaine toutes les menaces identifiées.

Une fois l'analyse terminée, des statistiques générales reprenant les informations suivantes s'affichent :

- Le nombre d'objets analysés ;
- Le nombre de virus découverts, placés en quarantaine et supprimés ;
- Le nombre d'objets ignorés (par exemple, lorsque le fichier est bloqué par le système d'exploitation ou lorsque le fichier n'est pas un fichier exécutable alors que l'analyse porte uniquement sur les fichiers exécutables) ;
- L'heure de l'analyse.

4. A la fin, cliquez sur **OK**.

EXÉCUTION DE L'ANALYSE PROGRAMMÉE

Kaspersky Mobile Security 9.0 permet de planifier des analyses de l'appareil qui s'exécuteront automatiquement à des heures programmées à l'avance. L'analyse est exécutée en en arrière plan. Quand un objet infecté est détecté, l'application exécute l'action sélectionnée dans la configuration de l'analyse (cf. la rubrique " Sélection des actions à appliquer sur les objets identifiés " à la page 142).

Par défaut, la planification est désactivée.

Pour configurer l'analyse programmée, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Planification des analyses**.

   L'écran **Planification** s'ouvre.

4. Cochez la case **Analyse programmée** (cf. ill. ci-après).

5. Sélectionnez une des valeurs proposées pour le paramètre **Fréquence** :

   - **Chaque jour** : l'analyse s'exécutera tous les jours. Spécifiez l'**Heure** dans le champ de saisie.
   - **Chaque semaine** : l'analyse s'exécutera une fois par semaine. Définissez les paramètres **Heure** et **Jour de la semaine**.

Figure 84 : Planification des analyses automatiques

6. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DU TYPE D'OBJET A ANALYSER

Vous pouvez sélectionner les types d'objet qui seront soumis à la recherche de code malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour sélectionner un objet à analyser, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Sélectionnez les objets à analyser dans le groupe **Objets à analyser** (cf. ill. ci-après) :

   - **Tous les fichiers :** l'analyse porte sur tous les types de fichiers. Les formats d'archive suivants sont pris en charge : *.zip, *.jar, *.jad et *.cab.
   - **Exécutables seuls** : analyse uniquement les fichiers exécutables des applications au format *.exe, *.dll, *.sis, *.mdl, *.app, * .rdl, *.prt, *.pxt, *.ldd, *.pdd ou *.class. Dans ce cas, les archives ne sont ni décompactées, ni analysées.

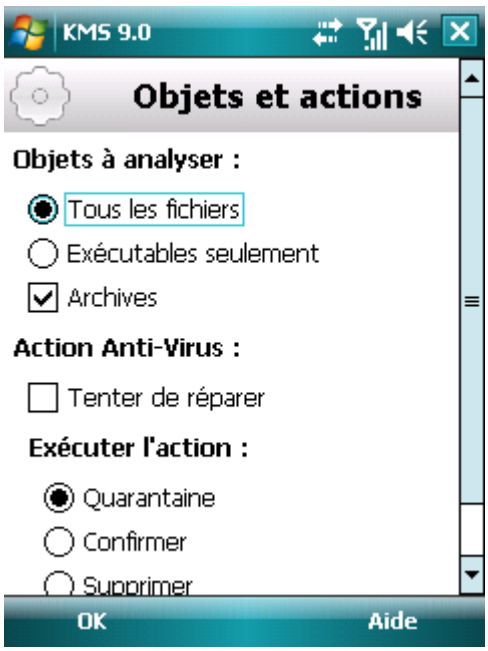


Figure 85: sélection des objets à analyser

5. Appuyez sur **OK** pour enregistrer les modifications.

CONFIGURATION DE L'ANALYSE DE FICHIERS COMPRESSES

Souvent, les virus se dissimulent dans des archives. Pour pouvoir analyser le contenu d'une archive, il faut absolument la décompacter. Ceci peut ralentir considérablement la vitesse de l'analyse de l'appareil.

Le décompactage des archives est désactivé par défaut. L'application analyse les archives des formats suivants : *.zip, *.jar, *.jad, *.cab. Pour accélérer l'analyse, vous pouvez désactiver le décompactage des archives.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

➧ *Pour désactiver le décompactage des archives, procédez comme suit :*

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Dans le groupe **Objets à analyser**, décochez la case **Archives**.

5. Appuyez sur **OK** pour enregistrer les modifications.

SELECTION DES ACTIONS A APPLIQUER SUR LES OBJETS IDENTIFIES

Par défaut Kaspersky Mobile Security 9.0 met les objets infectés découverts en quarantaine. Vous pouvez modifier les actions exécutées par l'application en cas de détection d'un objet malveillant.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour configurer la réponse du programme en présence d'un objet malveillant, procédez de la manière suivante (voir figure suivante) :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Choisissez l'option **Analyser**.

   L'écran **Analyser** s'ouvre.

3. Sélectionnez l'option **Objets et actions**.

   L'écran **Objets et actions** s'ouvre.

4. Pour que le programme tente de réparer les objets infectés, cochez la case **Tenter de réparer** pour le paramètre **Action Anti-Virus** (cf. ill. ci-après).

5. Définissez l'action à exécuter sur les objets malveillants découverts. Pour ce faire, attribuez une valeur au paramètre **Exécuter l'action** :

   Si la case **Tenter de réparer** avait été cochée, le paramètre s'appelle **Si la réparation échoue**. Ce paramètre détermine l'action de l'application en cas d'échec de la réparation.

   - **Quarantaine** : place en quarantaine les objets malveillants.
   - **Interroger** : demande une confirmation de l'action à l'utilisateur en cas de découverte d'objets malveillants.
   - **Supprimer** : supprime les objets malveillants sans le communiquer à l'utilisateur.

- **Consigner** : ignore les objets malveillants mais consigne les informations relatives à leur découverte dans le journal de l'application. Bloque l'objet en cas de tentative d'accès (par exemple, copie ou exécution).

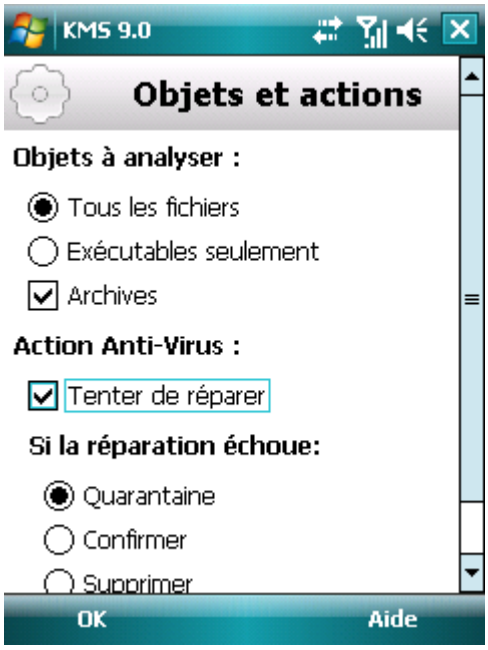


Figure 86 : sélection de l'action appliquée à un objet malveillant

6. Appuyez sur **OK** pour enregistrer les modifications.

QUARANTAINE DES OBJETS MALVEILLANTS

La rubrique présente les informations relatives à la *quarantaine*, un dossier spécial où sont placés les objets potentiellement dangereux. Elle décrit également comment manipuler les objets en quarantaine, à savoir comment consulter, restaurer ou supprimer les objets qui se trouvent dans ce dossier.

DANS CETTE SECTION

À PROPOS DE LA QUARANTAINE

La quarantaine est un dossier défini dans lequel Kaspersky Mobile Security 9.0 place les objets potentiellement malveillants.

Les objets malveillants peuvent être découverts et placés en quarantaine pendant l'analyse de l'appareil ou par la protection.

Les objets placés en quarantaine sont stockés sous forme d'archives et soumis à des règles empêchant leur activation, de telle sorte qu'ils ne représentent aucune menace pour l'appareil. Ensuite, ces objets pourront être supprimés ou restaurés.

AFFICHAGE DES OBJETS EN QUARANTAINE

Vous pouvez consulter la liste des objets que l'application a mis en quarantaine. Le nom complet de l'objet dans la liste et la date à laquelle il a été découvert sont repris.

Vous pouvez également consulter des informations complémentaires sur l'objet infecté sélectionné : chemin d'accès à l'objet sur l'appareil avant sa mise en quarantaine et nom de la menace.

Pour consulter la liste des objets en quarantaine, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre et présente la liste des objets placés en quarantaine (cf. ill. ci-après).

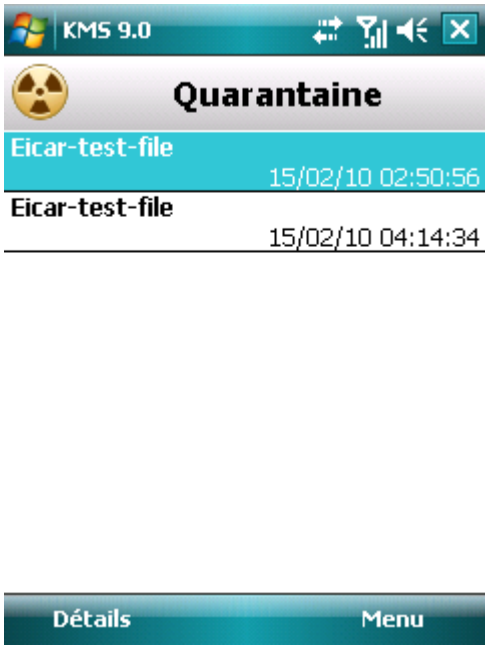


Figure 87 : liste des objets placés en quarantaine

Pour consulter les informations relatives à l'objet infecté,

appuyez sur **Détails**.

L'écran **Détails** présente les informations suivantes sur l'objet : chemin d'accès au fichier sur l'appareil avant sa détection et nom du virus.

L'écran **Info. objet** s'ouvre.

RESTAURATION D'OBJETS DE LA QUARANTAINE

Si vous êtes convaincu que l'objet découvert ne constitue pas une menace pour l'appareil, vous pouvez le restaurer depuis la quarantaine. L'objet restauré sera remis dans on répertoire d'origine.

Pour restaurer un objet depuis la quarantaine, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à restaurer, puis choisissez l'option **Menu** → **Restaurer**.

L'objet sélectionné dans la quarantaine est restauré dans son dossier d'origine.

SUPPRESSION D'OBJETS DE LA QUARANTAINE

Il est possible de supprimer un élément ou l'ensemble des éléments repris dans la quarantaine.

Pour supprimer un objet de la quarantaine, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Sélectionnez l'objet à supprimer, puis choisissez l'option **Menu** →·**Supprimer**.

L'objet sélectionné est supprimé de la quarantaine.

Pour supprimer tous les objets de la quarantaine, procédez comme suit :

1. Sélectionnez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Quarantaine**.

   L'écran **Quarantaine** s'ouvre.

3. Appuyez sur **Menu** → **Supprimer tout**.

Tous les objets en quarantaine seront éliminés.

FILTRAGE DES APPELS ET DES SMS ENTRANTS

La section présente le composant Anti-Spam qui filtre les SMS et les appels entrants sur la base des listes noire ou blanche. Elle décrit également comment composer les listes noire et blanche, comment sélectionner l'action réalisée par Anti-Spam sur les SMS et les appels entrants et comment configurer le fonctionnement du composant.

DANS CETTE SECTION

A PROPOS DU COMPOSANT ANTI-SPAM

Anti-Spam protège l'appareil contre la réception de SMS et d'appels non sollicités. Anti-Spam filtre les SMS et les appels entrants sur la base de listes noire ou blanche.

Les listes contiennent les enregistrements. Chacun de ces enregistrements peut contenir les paramètres suivants :

- Type de données (SMS, appels, SMS et appels) soumis au filtrage (paramètre obligatoire) ;
- Numéro d'où proviennent les données ;
- Texte que peut contenir le SMS.

L'Anti-Spam filtre les SMS et les appels sur la base de paramètres définis (cf. la rubrique " Présentation des modes de l'Anti-Spam " à la page 147). L'Anti-Spam analyse, sur la base du régime, chaque SMS ou appel entrant puis détermine si ce SMS ou cet appel est sollicité ou non. L'analyse se termine dès que l'Anti-Spam a attribué l'état de sollicité ou non au SMS ou à l'appel.

L'algorithme Anti-Spam se déroule de la manière suivante par défaut :

1. Analyse du SMS entrant pour voir si le texte ou le numéro de téléphone figurent dans :
   a. la liste noire. Si la liste contient un enregistrement dont le numéro ou le texte correspond aux données du SMS entrant, ce dernier est considéré comme indésirable et bloqué. L'application supprime le SMS bloqué.
   b. la liste blanche. Si la liste contient un enregistrement dont le numéro ou le texte correspond aux données du SMS entrant, ce dernier est considéré comme désirable et est autorisé.
2. Analyse des appels et des SMS uniquement sur la base du numéro :
   a. la liste noire. Si la liste contient un enregistrement dont le numéro correspond au numéro de l'appelant (pas de texte dans l'enregistrement), alors l'appel ou le SMS est considéré comme du spam et est bloqué. L'application supprime le SMS bloqué.
   b. la liste blanche. Si la liste contient un enregistrement dont le numéro correspond au numéro de l'appelant (pas de texte dans l'enregistrement), alors l'appel ou le SMS est considéré comme acceptable et est autorisé.
3. Analyse des SMS uniquement sur la base du texte :

a. la liste noire. Si la liste contient un enregistrement dont le texte correspond aux données du SMS entrant (le numéro ne figure pas dans l'enregistrement), alors ce SMS est considéré comme du spam et est bloqué. L'application supprime le SMS bloqué.

b. la liste blanche. Si la liste contient un enregistrement dont le texte correspond aux données du SMS entrant (le numéro ne figure pas dans l'enregistrement), alors ce SMS est considéré comme normal et est autorisé.

4. Sélection de l'action. Si aucune équivalence n'est trouvée dans la liste noire ou dans la liste blanche, l'Anti-Spam laisse passer par défaut les appels et les SMS et propose de choisir une action dans la fenêtre de notification. La notification présente en plus des informations complémentaires. S'agissant d'un appel reçu, la notification reprend le numéro de l'appelant. Dans le cas des SMS, la notification reprend le numéro de l'expéditeur et le contenu.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique " Journaux du logiciel " à la page 199).

PRESENTATION DES MODES DE L'ANTI-SPAM

Un mode de l'Anti-Spam est un ensemble de paramètres qui définissent la protection de votre appareil contre les SMS et les appels indésirables.

Les modes de fonctionnement Anti-Spam disponibles :

- **Désactivé**. Dans ce mode, l'Anti-Spam est désactivé. L'Anti-Spam ne filtre pas les SMS et les appels.
- **Liste blanche**. Dans ce mode, l'Anti-Spam accepte les SMS et les appels en provenance de numéros de la liste blanche. L'Anti-Spam bloque les SMS et les appels en provenance d'autres numéros. L'Anti-Spam supprime les numéros bloqués.
- **Liste noire**. Dans ce mode, l'Anti-Spam bloque les SMS et les appels en provenance de numéros de la liste noire. L'Anti-Spam accepte les SMS et les appels en provenance d'autres numéros. L'Anti-Spam supprime les numéros bloqués.
- **Les deux listes**. Dans ce mode, l'Anti-Spam remet les SMS et accepte les appels en provenance de numéros de la liste blanche et bloque ceux en provenance de numéros de la liste noire. Après la réception d'un appel ou d'un message en provenance d'un numéro qui ne figure dans aucune des deux listes, l'Anti-Spam propose une action à choisir : accepter le SMS/l'appel sans ajouter le numéro de téléphone de l'abonné à la liste ou ajouter le numéro de téléphone à la liste noire ou à la liste blanche.

  Ce mode est sélectionné par défaut.

Vous pouvez modifier le mode de l'Anti-Spam (cf. la rubrique " Modification du mode de l'Anti-Spam " à la page 147). Le mode actuel de l'Anti-Spam s'affiche à l'écran **Anti-Spam** à côté de l'option **Mode**.

MODIFICATION DU MODE DE L'ANTI-SPAM

Pour sélectionner le mode de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Menu** → **Antispam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Sélectionnez une valeur pour le paramètre **Mode de l'Anti-Spam** (cf. ill. ci-dessous).

Figure 88: modification du mode de l'Anti-Spam

4. Appuyez sur **OK** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à Anti-Spam pour bloquer les SMS et les appels entrants.

La liste reprend les numéros de téléphone et les expressions dont la présence dans un message indique son appartenance au spam.

Les informations relatives aux SMS et aux appels interdits sont consignées dans le journal (cf. la rubrique" Journaux du logiciel " à la page 199).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

➧ *Pour ajouter un enregistrement à la liste noire de l'Anti-Spam, procédez comme suit :*

1. Choisissez **Menu** → **Anti-Spam**.

L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

   L'écran **Nouvel enregistrement** s'ouvre.

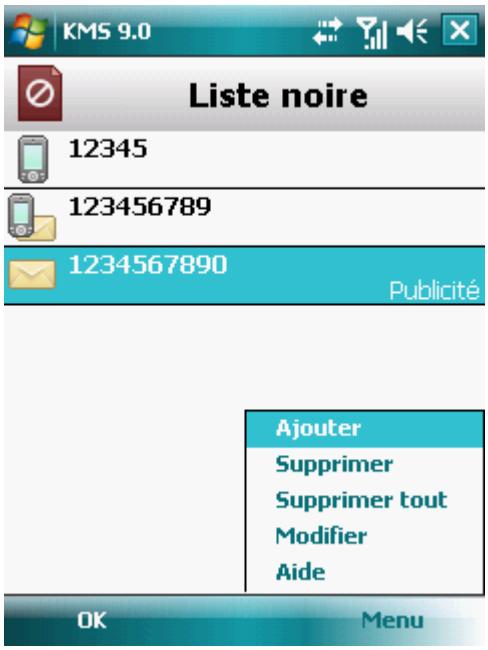


Figure 89: ajout d'un enregistrement à la liste noire.

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

   - **Bloquer tout** : type d'informations entrantes en provenance d'un numéro que l'Anti-Spam va bloquer :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seuls :** bloque uniquement les appels entrants.
     - **SMS seuls** : bloque uniquement les SMS entrants.
   - **Numéro de téléphone** : numéro de téléphone en provenance duquel les SMS et/ou les appels seront bloqués. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenants le texte** : mots/expressions clés qui indiquent que le SMS reçu est du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

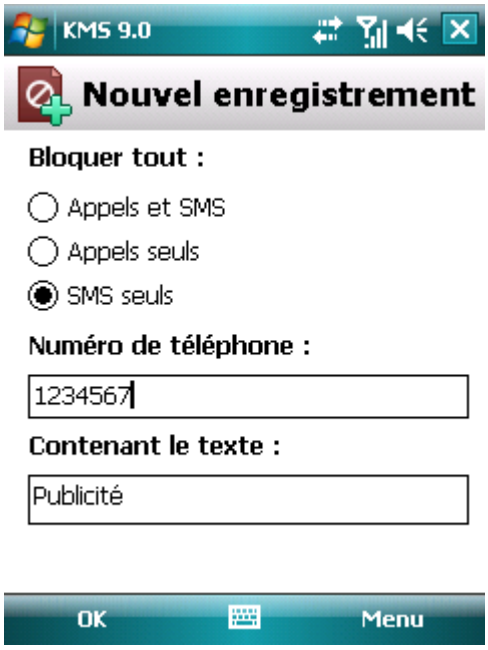


Figure 90: paramètres de l'enregistrement

5. Appuyez sur **Terminé** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Dans les enregistrements de la liste noire des numéros interdits, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste noire de l'Anti-Spam, exécutez les opérations suivantes :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

   L'écran **Modifier entrée** s'ouvre.

4. Modifiez les paramètres requis.

   - **Bloquer tout** : type d'informations entrantes en provenance d'un numéro que l'Anti-Spam va bloquer :
     - **Appels et SMS** : bloque les appels et les SMS entrants.
     - **Appels seuls :** bloque uniquement les appels entrants.
     - **SMS seuls** : bloque uniquement les SMS entrants.

- **Numéro de téléphone** : numéro de téléphone en provenance duquel les SMS et/ou les appels seront bloqués. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenants le texte** : mots/expressions clés qui indiquent que le SMS reçu est du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Bloquer tout**.

5. Appuyez sur **OK** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste. De plus, vous pouvez purger la liste noire de l'Anti-Spam en supprimant tous les enregistrements qu'elle contient.

Pour supprimer un enregistrement de la liste noire de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.

4. Confirmez la suppression de l'entrée. Pour ce faire, appuyez sur le bouton **Oui**.

Pour purger la liste noire de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.

3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer la liste blanche qui servira à Anti-Spam pour autoriser les SMS et les appels entrants.

La liste reprend les numéros de téléphone des expéditeurs et les expressions que vous ne considérez pas comme du spam

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer simultanément dans la liste noire et dans la liste blanche des numéros de l'Anti-Spam. Quand un numéro avec ces critères de filtrage est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour ajouter un enregistrement à la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Choisissez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

   L'écran **Nouvel enregistrement** s'ouvre.

Figure 91: ajout d'un enregistrement à la liste blanche

4. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :

   - **Autoriser tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va autoriser :
     - **Appels et SMS** : autorise les appels et les SMS entrants.

- **Appels seuls :** autorise uniquement les appels entrants.
- **SMS seuls** : autorise les messages SMS entrants uniquement.

- **Numéro de téléphone** – numéro de téléphone depuis lequel la réception des SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

- **Contenant le texte** : mots/expressions clés qui indiquent que le SMS reçu n'est pas du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

Figure 92: paramètres de l'enregistrement

5. Appuyez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste blanche de l'Anti-Spam, exécutez les opérations suivantes :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Choisissez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

   L'écran **Modifier entrée** s'ouvre.

4. Modifiez les paramètres requis.

- **Autoriser tout** : type de données entrantes en provenance d'un numéro que l'Anti-Spam va autoriser :
  - **Appels et SMS** : autorise les appels et les SMS entrants.
  - **Appels seuls :** autorise uniquement les appels entrants.
  - **SMS seuls** : autorise les messages SMS entrants uniquement.
- **Numéro de téléphone** – numéro de téléphone depuis lequel la réception des SMS ou d'appels est autorisée. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).
- **Contenant le texte** : mots/expressions clés qui indiquent que le SMS reçu n'est pas du spam. Le paramètre est accessible si la valeur **SMS seuls** a été attribuée au paramètre **Autoriser tout**.

5. Appuyez sur **Terminé** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer une seule entrée de la liste blanche ou toute la liste.

Pour supprimer un enregistrement de la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Anti-Spam** s'ouvre.

2. Choisissez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.

4. Confirmez la suppression de l'entrée. Pour ce faire, appuyez sur le bouton **Oui**.

Pour purger la liste blanche de l'Anti-Spam, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Choisissez l'option **Liste blanche**.

   L'écran **Liste blanche** s'ouvre.

3. Sélectionnez l'option **Menu** → **Supprimer tout**.

La liste est désormais vide.

REACTION AUX SMS ET APPELS DE CONTACTS QUI NE FIGURENT PAS DANS LE REPERTOIRE TELEPHONIQUE

Si le mode **Les deux listes** ou **Liste blanche** (cf. la rubrique " **Présentation des modes de l'Anti-Spam** " à la page 147) de l'Anti-Spam a été sélectionné, vous pouvez définir la réaction du composant face aux SMS ou aux appels de personnes dont le numéro ne figure pas dans le répertoire téléphonique. Anti-Spam permet d'élargir la liste blanche en y introduisant les numéros des contacts.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour définir la réaction de l'Anti-Spam face aux numéros ne figurant pas dans le répertoire téléphonique de l'appareil, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Mode**.

3. L'écran **Mode** s'ouvre.

4. Choisissez la valeur de paramètre **Autoriser contacts** (cf. ill. ci-après) :

   - Pour que l'Anti-Spam considère un numéro du répertoire téléphonique comme un ajout à la liste blanche et qu'il n'accepte pas les SMS et les appels en provenance de numéros qui ne figurent pas dans le répertoire, cochez la case **Autoriser contacts** ;

   - Pour que l'Anti-Spam filtre les SMS et les appels uniquement sur la base du régime défini de l'Anti-Spam, décochez la case **Autoriser contacts**.

Figure 93: réaction de l'Anti-Spam face à un numéro qui ne figure pas dans le répertoire téléphonique de l'appareil

5. Appuyez sur **OK** pour enregistrer les modifications.

REACTION AUX SMS EN PROVENANCE DE NUMEROS SANS CHIFFRES

Si le mode **Les deux listes** ou **Liste noire** (cf. la rubrique " **Présentation des modes de l'Anti-Spam** " à la page 147) de l'Anti-Spam a été sélectionné, vous pouvez enrichir la liste noire en incluant tous les numéros sans chiffres (composés de lettres). Alors Anti-Spam pourra bloquer les SMS en provenance de numéros sans chiffres.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour définir la réaction de l'Anti-Spam en cas de réception d'un SMS en provenance d'un numéro sans chiffres, procédez comme suit :

1. Choisissez **Menu** → **Anti-Spam**.

   L'écran **Antispam** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Choisissez une valeur pour le paramètre **Interdire non numériques** (cf. ill. ci-après) :

   - afin que l'Anti-Spam supprime automatiquement les SMS en provenance de numéros sans chiffres, cochez la case **Interdire non numériques** ;
   - afin que l'Anti-Spam filtre les SMS en provenance de numéros sans chiffres sur la base du mode sélectionné pour Anti-Spam, décochez la case **Interdire non numériques**.

Figure 94: configuration des actions exécutées par Anti-Spam en cas de réception de SMS depuis un numéro sans chiffres.

4. Appuyez sur **Terminé** pour enregistrer les modifications.

SELECTION DE L'ACTION A APPLIQUER SUR LES SMS ENTRANTS

Le mode par défaut activé pour Anti-Spam est **Les deux listes** (cf. la rubrique " **Modes du composant Anti-Spam** " à la page 147). Anti-Spam analyse les SMS entrants sur la base des listes blanche et noire.

Si le numéro de l'expéditeur ne figure ni dans la liste noire, ni dans la liste blanche, Anti-Spam vous prévient. Vous serez invité à choisir une des actions proposées par Anti-Spam pour traiter le SMS entrant (cf. ill. ci-après).

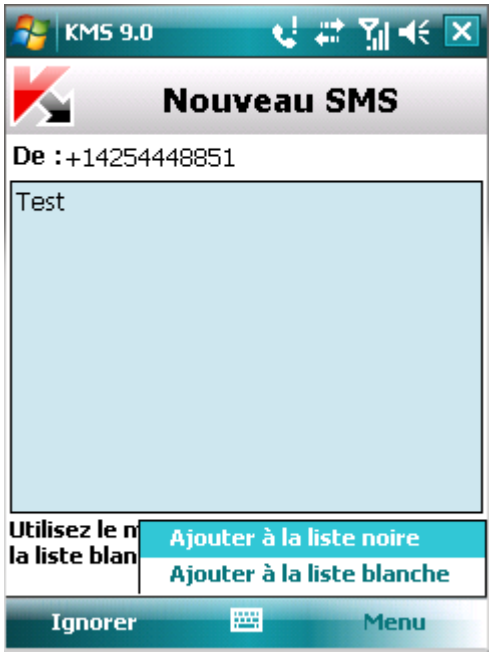


Figure 95: notification de l'Anti-Spam sur le SMS reçu

Vous pouvez choisir l'une des actions suivantes à appliquer sur le SMS :

- Pour bloquer le SMS et ajouter le numéro de l'appelant à la liste noire, choisissez **Menus** → **Ajouter à la liste noire**.
- Pour livrer le SMS et ajouter le numéro de l'appelant à la liste blanche, choisissez **Menu** → **Ajouter à la liste blanche**.
- Pour accepter le SMS sans consigner le numéro de téléphone de l'appelant dans aucune des listes, appuyez sur **Ignorer**.

Les informations sur les SMS bloqués sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

SELECTION DE L'ACTION A APPLIQUER SUR DES APPELS ENTRANTS

Le mode par défaut activé pour Anti-Spam est **Les deux listes** (cf. la rubrique " **Modes du composant Anti-Spam** " à la page 147). Anti-Spam analyse les appels entrants sur la base des listes blanche et noire.

Si le numéro de l'appelant ne figure ni dans la liste blanche, ni dans la liste noire, Anti-Spam vous le signalera après l'appel et proposera une action à exécuter sur les appels entrants (cf ill. ci-après).

Figure 96: notification de l'Anti-Spam sur l'appel reçu

Vous pouvez choisir une des actions suivantes pour le numéro de l'appelant (cf. ill. ci-après) :

- Pour ajouter le numéro de téléphone de l'appelant à la liste noire, choisissez **Menu** → **Ajouter à la liste noire**.
- Pour ajouter le numéro de téléphone de l'appelant à la liste blanche, choisissez **Menu** → **Ajouter à la liste blanche**.
- Choisissez **Ignorer** si vous ne souhaitez pas consigner le numéro de l'appelant dans aucune des listes.

Les informations sur les appels bloqués sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 106).

RESTRICTIONS SUR LES APPELS ET LES SMS SORTANTS. CONTROLE PARENTAL

Cette section présente le composant Contrôle Parental qui permet de restreindre les appels et les SMS sortants à numéros. Elle explique également comment composer des listes de numéros interdits ou autorisés et configurer les paramètres du contrôle parental.

DANS CETTE SECTION

À PROPOS DU CONTROLE PARENTAL

Contrôle Parental permet de contrôler les appels et les SMS sortants sur la base de listes noire et blanche de numéros de téléphone. Le fonctionnement du composant dépend du mode.

En mode **Liste noire**, le Contrôle Parental interdit l'envoi de SMS et la réalisation d'appels vers les numéros de la liste noire. L'envoi de SMS et la réalisation d'appels vers les autres numéros est autorisée. En mode **Liste blanche**, le Contrôle Parental autorise l'envoi de SMS et la réalisation d'appels uniquement vers les numéros de la liste blanche. L'envoi de SMS et la réalisation d'appels vers les autres numéros sont interdits par le Contrôle Parental. En mode **" Désactivé "**, le Contrôle Parental ne contrôle pas les SMS et les appels sortants.

Le Contrôle Parental interdit les SMS envoyés uniquement à l'aide des outils standards de l'appareil. Le Contrôle Parental autorise l'envoi de SMS via des logiciels tiers.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

MODES DU CONTROLE PARENTAL

Le mode du Contrôle Parental définit la règle selon laquelle le contrôle des SMS et des appels sortants est effectué.

Les modes de fonctionnement du contrôle parental suivants sont disponibles :

- **Désactivé** : désactive Contrôle Parental. Ne pas contrôler les SMS et les appels sortants.

  Ce mode est sélectionné par défaut.

- **Liste blanche** : autorise l'envoi de SMS et/ou la réalisation d'appels uniquement vers les numéros de la liste blanche (cf. la rubrique " Composition de la liste blanche " à la page 163). Tous les autres SMS ou numéros sont bloqués.

- **Liste noire** : interdit l'envoi de SMS et/ou la réalisation d'appels uniquement vers des numéros de la liste noire (cf. la rubrique " Composition de la liste noire " à la page 160). Tous les autres SMS ou numéros sont bloqués.

Vous pouvez changer le mode du Contrôle Parental (cf. la rubrique " Activation/désactivation du contrôle parental " à la page 159). Le mode sélectionné de Contrôle Parental apparaît à l'écran **Contrôle Parental** à côté de l'option de menu **Mode**.

ACTIVATION/DESACTIVATION DU CONTROLE PARENTAL

Pour modifier le mode de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.

2. L'écran **Contrôle Parental** s'ouvre.
3. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.
4. Sélectionnez un des modes proposés pour Contrôle Parental (cf. ill. ci-après).

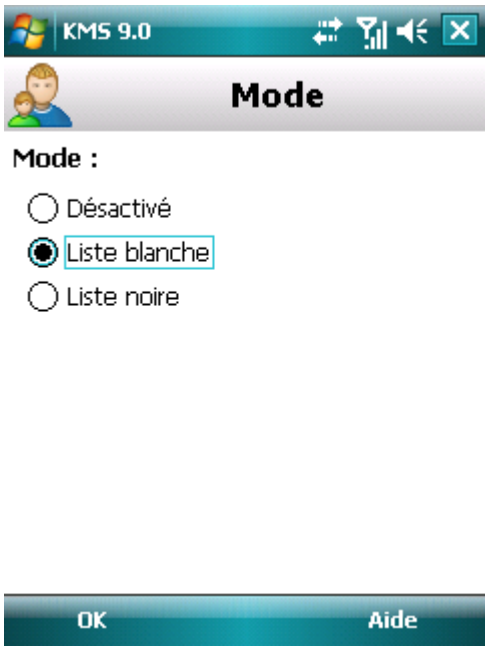


Figure 97 : modification du mode du Contrôle Parental

5. Appuyez sur **OK** pour enregistrer les modifications.

COMPOSITION DE LA LISTE NOIRE

Vous pouvez composer la liste noire qui servira à Contrôle Parental pour bloquer les SMS et les appels sortants. La liste reprend les numéros de téléphone vers lesquels l'envoi de SMS et la réalisation d'appels seront interdits.

Les informations sur les SMS et les appels interdits sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE NOIRE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Contrôle Parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour ajouter un enregistrement à la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.
4. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

Figure 98: ajout d'un enregistrement à la liste noire.

L'écran **Nouvel enregistrement** s'ouvre.

5. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :
   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
     - **Appels et SMS** : bloque les appels et les SMS sortants.
     - **Appels seuls :** bloque uniquement les appels sortants.
     - **SMS seuls** : interdit les SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

Figure 99: paramètres de l'enregistrement

6. Appuyez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Dans les enregistrements de la liste noire des numéros interdits, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.
4. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

   L'écran **Modifier entrée** s'ouvre.
5. Modifiez les paramètres requis.
   - **Bloquer tout** : type de données sortantes en provenance d'un numéro que Contrôle Parental va bloquer :
     - **Appels et SMS** : bloque les appels et les SMS sortants.
     - **Appels seuls :** bloque uniquement les appels sortants.
     - **SMS seuls** : interdit les SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone vers lequel l'envoi de messages SMS ou d'appels est interdit. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

6. Appuyez sur **OK** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE NOIRE

Il peut arriver qu'un numéro soit ajouté par erreur à la liste noire des numéros interdits. Vous pouvez supprimer ce numéro de la liste. De plus, vous pouvez purger la liste noire du Contrôle Parental en supprimant tous les enregistrements qu'elle contient.

Pour supprimer un enregistrement de la liste noire de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.
4. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
5. Confirmez la suppression. Pour ce faire, appuyez sur le bouton **Oui**.

Pour purger la liste noire de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Sélectionnez l'option **Liste noire**.

   L'écran **Liste noire** s'ouvre.
4. Choisissez **Menu** → **Supprimer tout**.

La liste est désormais vide.

COMPOSITION DE LA LISTE BLANCHE

Vous pouvez composer la liste blanche qui servira à Anti-Spam pour autoriser les SMS et les appels entrants.

La liste reprend les numéros de téléphone des expéditeurs et les expressions que vous ne considérez pas comme du spam

DANS CETTE SECTION

AJOUT D'UN ENREGISTREMENT A LA LISTE BLANCHE

N'oubliez pas qu'un même numéro possédant des critères de filtrage identique ne peut pas figurer à la foi dans la liste noire et dans la liste blanche des numéros du Contrôle Parental. Quand un numéro avec de tels critères est déjà enregistré dans une des deux listes, Kaspersky Mobile Security 9.0 vous prévient : le message de circonstance s'affiche.

Pour ajouter un enregistrement à la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Choisissez l'option **Liste blanche**.
4. L'écran **Liste blanche** s'ouvre.
5. Choisissez l'option **Menu** → **Ajouter** (cf. ill. ci-après).

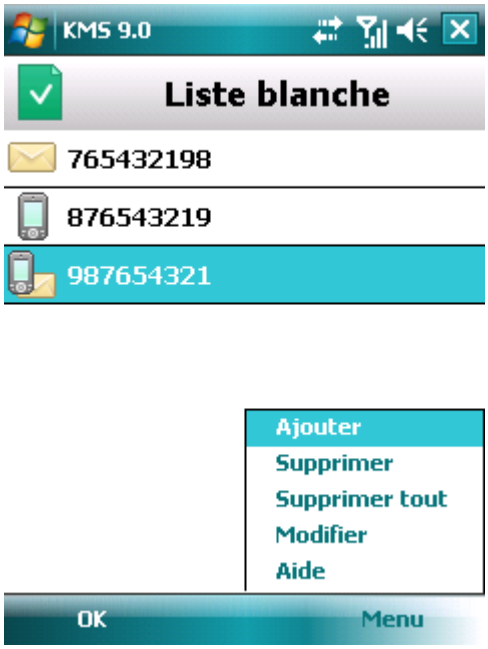


Figure 100: ajout d'un enregistrement à la liste blanche

L'écran **Nouvel enregistrement** s'ouvre.

6. Attribuez une valeur aux paramètres suivants (cf. ill. ci-après) :
   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :
     - **Appels et SMS** : autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.
     - **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle Parental pour l'envoi de SMS et/ou la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

Figure 101: paramètres de l'enregistrement

7. Appuyez sur **OK** pour enregistrer les modifications.

MODIFICATION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Dans les enregistrements de la liste blanche des numéros autorisés, vous pouvez modifier la valeur de tous les paramètres.

Pour modifier un enregistrement de la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Choisissez l'option **Liste blanche**.
4. L'écran **Liste blanche** s'ouvre.
5. Choisissez dans la liste l'élément que vous souhaitez modifier, puis choisissez l'option **Menu** → **Modifier**.

   L'écran **Modification d'entrée** s'ouvre.
6. Modifiez les paramètres requis.
   - **Autoriser tout** : type de données sortantes dont l'envoi est autorisé par Contrôle Parental vers le destinataire :
     - **Appels et SMS** : autorise les appels et les SMS sortants.
     - **Appels seuls :** autorise uniquement les appels sortants.

- **SMS seuls** : autorise les messages SMS sortants uniquement.

- **Numéro de téléphone** : numéro de téléphone accepté par Contrôle Parental pour l'envoi de SMS et/ou la réalisation d'appels. Le numéro peut commencer par un chiffre, par une lettre ou par le signe " + " et ne peut contenir que des caractères alphanumériques. Pour le numéro, vous pouvez également utiliser les masques " * " et " ? " (où " * " représente n'importe quel nombre de caractères et " ? ", n'importe quel caractère unique).

7. Appuyez sur **Terminé** pour enregistrer les modifications.

SUPPRESSION D'UN ENREGISTREMENT DE LA LISTE BLANCHE

Vous pouvez supprimer une seule entrée de la liste blanche ou toute la liste.

Pour supprimer un enregistrement de la liste blanche de Contrôle Parental, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Choisissez l'option **Liste blanche**.
4. L'écran **Liste blanche** s'ouvre.
5. Sélectionnez dans la liste l'entrée à supprimer, puis choisissez l'option **Menu** → **Supprimer**.
6. Confirmez la suppression. Pour ce faire, appuyez sur le bouton **Oui**.

Pour purger la liste blanche de l'Anti-Spam, procédez comme suit :

1. Sélectionnez **Menu** → **Contrôle Parental**.
2. L'écran **Contrôle Parental** s'ouvre.
3. Choisissez l'option **Liste blanche**.
4. L'écran **Liste blanche** s'ouvre.
5. Choisissez **Menu** → **Supprimer tout**.

La liste est désormais vide.

PROTECTION DES DONNEES EN CAS DE PERTE OU DE VOL DE L'APPAREIL

La section présente les informations sur le composant Antivol chargé de la protection sophistiquées de données personnelles en cas de vol ou de perte de l'appareil et qui facilite la recherche de celui-ci. Elle explique également comment activer/désactiver les fonctions de l'Antivol, configurer les paramètres de fonctionnement et comment lancer à distance la protection en cas de vol ou de perte de l'appareil.

DANS CETTE SECTION

À PROPOS DU COMPOSANT ANTIVOL

Antivol protège les données enregistrées sur l'appareil contre l'accès non autorisé. Cette fonction peut être utile en cas de perte ou de vol de l'appareil. Antivol permet de verrouiller à distance l'appareil et de supprimer les données qu'il renferme.

Ce composant dispose des fonctions suivantes :

- **Verrouillage** : permet de verrouiller l'appareil à la demande de l'utilisateur et de définir le texte qui apparaîtra à l'écran de l'appareil verrouillé.
- **Suppression** : permet de supprimer les données personnelles de l'utilisateur (tous les contacts, les messages, les photos, le calendrier, les journaux, les paramètres de connexion au réseau), les données de la carte mémoire et les fichiers des dossiers sélectionnés.
- **SIM-Surveillance** : permet, en cas de remplacement de la carte SIM, d'envoyer vers le numéro de téléphone et/ou l'adresse électronique défini le nouveau numéro ainsi que de bloquer l'appareil en cas de remplacement de la carte SIM ou de mise sous tension de l'appareil sans cette carte.
- **Localisation** : permet de récupérer les coordonnées géographiques de l'appareil volé par SMS sur un autre appareil ou dans une adresse de messagerie spécifiée.

  Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré.

Afin de pouvoir utiliser chaque fonction de l'Antivol, il faut se souvenir du code secret défini au premier lancement de Kaspersky Mobile Security 9.0.

Toutes les fonctions de l'Antivol sont désactivées après l'installation de Kaspersky Mobile Security 9.0.

De plus, Kaspersky Mobile Security 9.0 permet de lancer à distance la fonction Antivol via l'envoi d'instructions vers l'appareil volé/perdu (cf. la rubrique " Lancement à distance de la fonction Antivol " à la page 176).

L'état du fonctionnement actuel de chaque fonction apparaît dans l'écran **Antivol** à côté du nom de l'application.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

VERROUILLAGE DE L'APPAREIL

Après la réception d'une instruction SMS spéciale, la fonction Verrouillage permet de verrouiller à distance l'accès à l'appareil et aux données qu'il renferme. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

Cette fonction ne verrouille pas l'appareil mais active uniquement la possibilité de le verrouiller à distance.

Pour activer la fonction de verrouillage, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Verrouillage**.

   L'écran **Verrouillage** s'ouvre.

3. Cochez la case **Activer le verrouillage**.

4. Dans le champ **Texte en cas de verrouillage**, modifiez le message qui apparaîtra sur l'écran de l'appareil verrouillé (cf. ill. ci-après). Un texte standard est utilisé par défaut. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

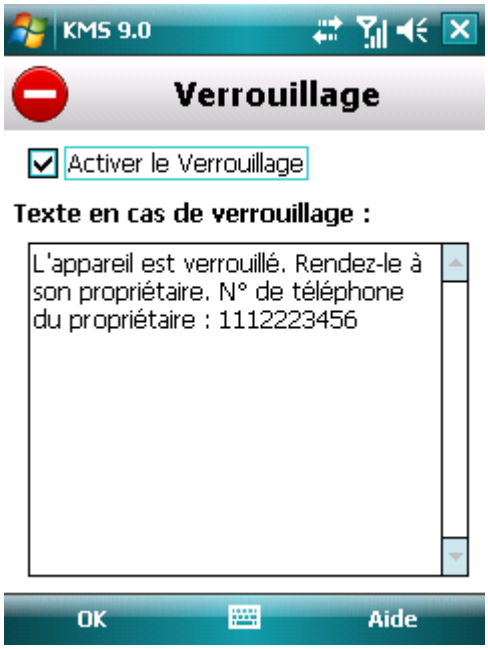


Figure 102: paramètres de la fonction Verrouillage

5. Appuyez sur **Terminé** pour enregistrer les modifications.

Pour verrouiller un autre appareil, si la fonction Verrouillage est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction **Envoi d'une instruction**. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. La réception du SMS passera inaperçu et déclenchera le blocage de votre appareil.

Pour verrouiller l'appareil à distance, il est conseillé d'utiliser la méthode sûre à l'aide de la fonction Envoi d'une instruction. Dans ce cas, l'instruction et le code secret sont envoyés en mode crypté.

- *Pour envoyer une instruction SMS à l'autre appareil à l'aide de la fonction Envoi d'une instruction, procédez comme suit :*

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Instruction SMS** la valeur **Verrouillage de l'appareil** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code distant**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

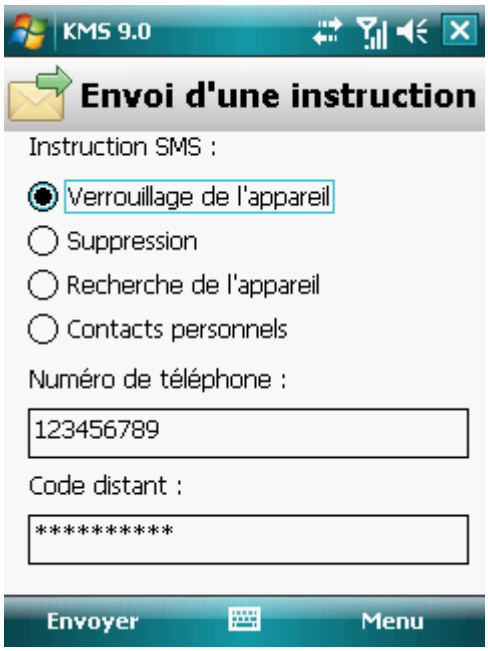


Figure 103: lancement à distance du verrouillage de l'appareil

6. Appuyez sur **Envoyer**.

- *Pour composer le SMS avec les fonctions standards de messagerie SMS de votre téléphone,*

  envoyez à l'appareil un message SMS avec le texte `block:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil à verrouiller). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

SUPPRESSION DE DONNEES PERSONNELLES

Après la réception de l'instruction SMS spéciale, la fonction Suppression permet de supprimer les informations suivantes sur l'appareil :

- Les données personnelles de l'utilisateur (tous les contacts, les messages, les photos, le calendrier et les paramètres de connexion au réseau). Qui plus est, Antivol supprime les contacts enregistrés dans le répertoire téléphonique de l'appareil et sur la carte SIM ;
- Les données de la carte mémoire ;
- Les fichiers du dossier **Mes documents** et d'autres dossiers de la liste **Dossiers à supprimer**.

Cette fonction ne supprime pas les données enregistrées sur l'appareil mais active la possibilité de le faire.

Pour activer la fonction de suppression des données, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Mode**.

   L'écran **Suppression** s'ouvre.

4. Cochez la case **Activer la Suppression de données**.

5. Sélectionnez les informations à supprimer. Pour ce faire, dans le groupe **Supprimer**, cochez les cases en regard des paramètres requis (cf. ill. ci-après) :

   - Pour supprimer les données personnelles, cochez la case **Données personnelles** ;
   - Pour supprimer les fichiers du dossier **Mes documents** et de la liste **Dossiers à supprimer**, cochez la case **Dossiers**.

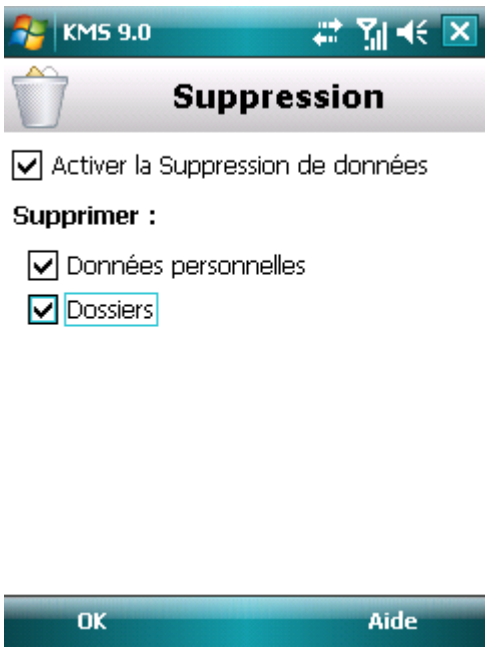


Figure 104: sélection du type de données à supprimer

6. Appuyez sur **OK** pour enregistrer les modifications.

7. Passez à la constitution de la liste **Dossiers à supprimer** (cf. rubrique " **Composition de la liste des objets à supprimer** " à la page 172).

La suppression des données personnelles de l'appareil peut être réalisée d'une des manières suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. Votre appareil recevra à l'insu de l'utilisateur un SMS et les données seront supprimées de l'appareil.

Pour supprimer à distance les informations de l'appareil, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, l'instruction et le code secret sont envoyés en mode crypté.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre.

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Instruction SMS** la valeur **Suppression** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code distant**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

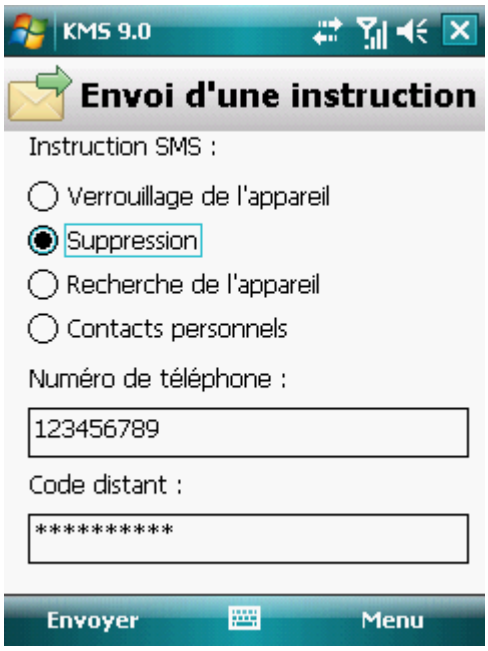


Figure 105: lancement à distance de la fonction Supprimer

6. Appuyez sur **Envoyer**.

Pour composer le SMS avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à l'appareil à verrouiller un SMS contenant le texte `wipe:<code>` (où `<code>` est le code secret défini sur l'appareil récepteur. Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES DOSSIERS A SUPPRIMER

La fonction Suppression permet de créer une liste de dossiers qui seront supprimés après la réception du SMS spécial.

Pour que l'Antivol supprime les dossiers de la liste après la réception de l'instruction spéciale par SMS, assurez-vous que la case **Dossiers** est cochée dans le menu **Mode**.

Pour ajouter un dossier à la liste des dossiers à supprimer, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

   L'écran **Dossiers à supprimer** s'ouvre.

4. Choisissez l'option **Menu** → **Ajouter un dossier** (cf. ill. ci-après).

Figure 106: sélection du dossier à supprimer

5. Sélectionnez le dossier requis dans l'arborescence, puis appuyez sur le bouton **Sélectionner**.

Le dossier sera ajouté à la liste.

Pour supprimer un dossier de la liste, procédez comme suit :

1. Choisissez **Menu** → **Antivol**.

L'écran **Antivol** s'ouvre.

2. Choisissez l'option **Suppression**.

   L'écran **Suppression** s'ouvre.

3. Sélectionnez l'option **Dossiers à supprimer**.

   L'écran **Dossiers à supprimer** s'ouvre.

4. Sélectionnez un dossier dans la liste, puis appuyez sur **Menu** → **Supprimer**.

CONTROLE DU REMPLACEMENT DE LA CARTE SIM SUR L'APPAREIL

SIM-Surveillance permet, en cas de remplacement de la carte SIM, d'envoyer le nouveau numéro de téléphone au numéro et/ou à l'adresse de messagerie spécifiés et de verrouiller l'appareil.

Pour activer la fonction SIM-Surveillance et contrôler le remplacement de la carte SIM sur l'appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Choisissez l'option **SIM-Surveillance**.

   L'écran **SIM-Surveillance** s'ouvre.

3. Cochez la case **Activer SIM-Surveillance**.

4. Pour contrôler le remplacement de la carte SIM sur l'appareil, configurez les paramètres suivants (cf. ill. ci-dessous) :

   - Pour envoyer automatiquement le SMS au sujet du nouveau numéro de votre téléphone, dans le champ **Numéro de téléphone** du groupe **Envoyer le nouveau numéro**, saisissez le numéro de téléphone vers lequel le message sera envoyé.

     Ces numéros peuvent commencer par un chiffre ou par le signe " + " et ne peuvent contenir que des chiffres.

   - Pour recevoir le message électronique sur le nouveau numéro de téléphone, saisissez l'adresse électronique requise dans le champ **Adresse courriel** du groupe **Envoyer le nouveau numéro**.

   - Pour verrouiller l'appareil en cas de remplacement de la carte SIM ou en cas de mise sous tension de l'appareil sans celle-ci, cochez la case **Verrouiller l'appareil** pour le paramètre **Au remplacement de la carte SIM**. L'appareil ne pourra être déverrouillé qu'après avoir entré le code secret.

- Pour qu'un message apparaisse à l'écran de l'appareil verrouillé, saisissez le texte dans le champ **Texte en cas de verrouillage**. Un texte standard est utilisé par défaut dans ce message. Vous pouvez y ajouter le numéro de téléphone du propriétaire.

Figure 107: paramètres de la fonction SIM-Surveillance

5. Appuyez sur **OK** pour enregistrer les modifications.

DETERMINATION DES COORDONNEES GEOGRAPHIQUES DE L'APPAREIL

Après avoir reçu l'instruction spéciale par SMS, la fonction Localisation détermine les coordonnées géographiques de l'appareil et les envoie par SMS ou courrier électronique à l'appareil à l'origine de la demande.

Cette fonction n'est disponible qu'avec des appareils équipés d'un récepteur GPS intégré. L'activation du récepteur a lieu automatiquement après la réception de l'instruction SMS.

La réception des coordonnées est possible uniquement si l'appareil se trouve dans une zone couverte par les satellites. Au cas où les satellites ne seraient pas disponibles au moment de la requête, des tentatives pour les trouver seront lancées à intervalles réguliers.

Pour activer la fonction Localisation, procédez comme suit :

1. Sélectionnez **Menu** → **Antivol**.

   L'écran **Antivol** s'ouvre.

2. Sélectionnez l'option **Localisation**.

   L'écran **Localisation** s'ouvre.

3. Cochez la case **Activer la localisation**.

   Kaspersky Mobile Security 9.0 renvoie par défaut les coordonnées de l'appareil dans un SMS.

4. Pour recevoir également les coordonnées par courrier électronique, saisissez l'adresse électronique dans le champ **Envoyer les coordonnées** (cf. ill. ci-après).

Figure 108: paramètres de la fonction Localisation

5. Appuyez sur **OK** pour enregistrer les modifications.

Pour récupérer les coordonnées de l'appareil, si la fonction Localisation est activée, vous disposez des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. Votre appareil recevra à l'insu de l'utilisateur un SMS et l'application enverra les coordonnées de l'appareil.

- Rédigez et envoyez un SMS avec un texte spécial depuis l'autre appareil nomade. Votre appareil recevra un SMS et l'application enverra les coordonnées de l'appareil.

Pour déterminer à distance les coordonnées, il est conseillé d'utiliser la méthode sûre qui implique la fonction Envoi d'une instruction. Dans ce cas, l'instruction et le code secret sont envoyés en mode crypté.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Instruction SMS** la valeur **Localisation** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code distant**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

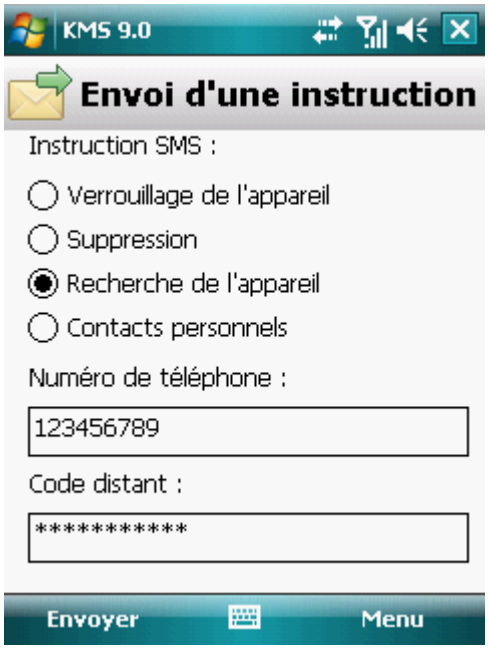


Figure 109 : Détermination des coordonnées de l'appareil

6. Appuyez sur **Envoyer**.

Pour composer le SMS avec les fonctions standards de messagerie SMS de votre téléphone,

envoyez à l'autre appareil un SMS contenant le texte `find:<code>` (où `<code>` est le code secret défini sur l'autre appareil). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

Le SMS contenant les coordonnées géographiques de l'appareil sera envoyé au numéro de téléphone à l'origine de l'envoi de l'instruction SMS et à une adresse électronique, si celle-ci a été définie dans les paramètres de la fonction Localisation.

LANCEMENT A DISTANCE DE LA FONCTION ANTIVOL

L'application permet d'envoyer une instruction spéciale par SMS afin de lancer à distance la fonction Antivol sur l'autre appareil doté de Kaspersky Mobile Security. L'instruction par SMS se présente sous la forme d'un SMS crypté qui contient le code secret de l'appareil auquel est envoyé le SMS. La réception de l'instruction passera inaperçue sur l'autre appareil.

Le coût du SMS envoyé est celui de votre opérateur de téléphonie mobile.

Pour envoyer une instruction vers un autre appareil, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

3. L'écran **Envoi d'une instruction** s'ouvre.

4. Sélectionnez une des valeurs proposées pour le paramètre **Instruction SMS** (cf. ill. ci-après) :

- **Verrouillage**.
- **Suppression**.
- **Localisation**.
- **Contacts personnels** (cf. la rubrique " **Dissimulation des informations confidentielles** " à la page 177).

5. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.
6. Dans le champ **Code distant**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

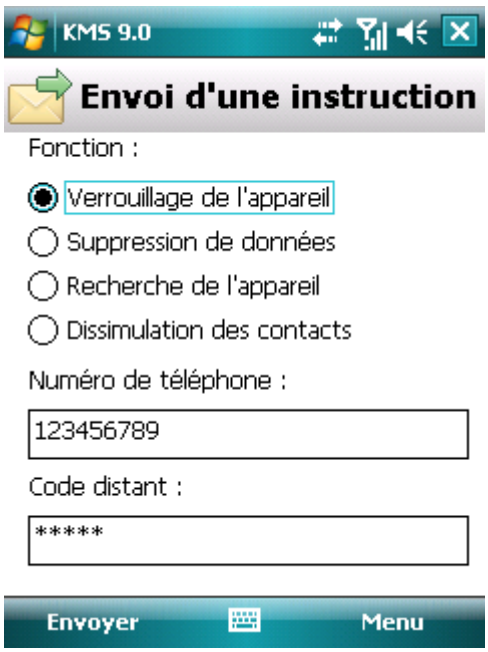


Figure 110: lancement à distance de la fonction Antivol

7. Appuyez sur **Envoyer**.

DISSIMULATION DES INFORMATIONS PERSONNELLES

La section présente le composant Contacts personnels. Le composant permet de dissimuler les données confidentielles de l'utilisateur pendant que l'appareil est utilisé temporairement par une autre personne.

DANS CETTE SECTION

PRESENTATION DU COMPOSANT CONTACTS PERSONNELS

Le composant Contacts personnels masque les informations confidentielles sur la base de la liste des contacts créée qui reprend les numéros confidentiels. Pour les numéros confidentiels, le composant masque les informations suivantes : contacts du répertoire, SMS entrants, sortants et transmis et entrées du journal des appels. Le composant masque également les informations entrantes : SMS et appels entrants. Le composant bloque le signal de réception d'un nouveau SMS et le masque dans la liste des SMS reçus. Le composant bloque l'appel d'un numéro confidentiel et n'affiche pas les informations relatives à sa réception. L'interlocuteur entendra la tonalité de ligne occupée. Pour voir les appels et SMS reçus pendant la période où le composant Contacts personnels était activé, désactivez-le. Quand vous activerez à nouveau le composant Contacts personnels, il masquera les informations consultées.

Vous pouvez configurer l'activation de la dissimulation des données confidentielles automatiquement ou à distance depuis un autre appareil mobile.

Contacts personnels peut être désactivé uniquement depuis l'application.

Les informations sur le fonctionnement de Contacts personnels sont conservées dans le journal (cf. la rubrique " Journaux de l'application " à la page 199).

PRESENTATION DES MODES DE CONTACTS PERSONNELS

Vous pouvez gérer le mode de fonctionnement de Contacts personnels. Le mode détermine si la fonction de dissimulation des données confidentielles est activée ou non.

La dissimulation est désactivée par défaut.

Les modes suivants sont prévus pour Contacts personnels :

- **Afficher** : les données confidentielles sont affichées. Les paramètres de Contacts personnels peuvent être modifiés.
- **Masquer** : les données confidentielles sont masquées. Les paramètres du composant Contacts personnels ne peuvent être modifiés.

Vous pouvez configurer l'activation automatique (cf. rubrique " Activation automatique de Contacts personnels " à la page 180) de la dissimulation des données personnelles ou son activation à distance depuis un autre appareil (cf. rubrique " Activation de la dissimulation des informations confidentielles à distance " à la page 181).

Le mode actuel de Contacts personnels s'affiche à l'écran **Contacts personnels** à côté de l'option **Mode**.

La modification du mode de fonctionnement du composant Contacts personnels peut prendre un certain temps.

ACTIVATION/DESACTIVATION DE CONTACTS PERSONNELS

Vous pouvez modifier le mode de Contacts personnels d'une des méthodes suivantes :

- depuis le menu de configuration du composant ;
- depuis le menu **Contacts personnels**.

Pour modifier le mode de Contacts personnels, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Sélectionnez une valeur pour le paramètre **Mode** (cf. ill. ci-dessous).

4. Appuyez sur **OK**.

Figure 111: modification du mode de Contacts personnels

5. Confirmez la modification du mode Contacts personnels. Pour ce faire, appuyez sur le bouton **Oui**.

Pour changer rapidement le mode Contacts personnels, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Appuyez sur **Masquer** / **Afficher**. Le texte du bouton changera en fonction de l'état actuel de Contacts personnels.

3. Confirmez la modification du mode Contacts personnels. Pour ce faire, appuyez sur le bouton **Oui**.

ACTIVATION AUTOMATIQUE DE CONTACTS PERSONNELS

Vous pouvez configurer l'activation automatique de la dissimulation des informations confidentielles après un certain temps. La fonction est activée quand l'appareil nomade est en mode d'économie d'énergie.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour activer automatiquement la dissimulation des informations confidentielles à l'issue d'une période déterminée, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Mode**.

3. L'écran **Mode** s'ouvre.

4. Cochez la case **Interdire l'accès** (cf. ill. ci-après).

5. Sélectionnez la période à l'issue de laquelle la dissimulation des données personnelles doit être activée automatiquement. Pour ce faire, choisissez une des valeurs prédéfinies pour le paramètre **Heure** :

   - **Sans délai**.
   - **1 minute**.
   - **5 minutes**.
   - **15 minutes**.
   - **1 heure**.

Figure 112: paramètres de lancement automatique de Contacts personnels

6. Appuyez sur **OK**.

ACTIVATION DE LA DISSIMULATION DES INFORMATIONS CONFIDENTIELLES A DISTANCE

Kaspersky Mobile Security 9.0 permet d'activer à distance depuis un autre appareil mobile la dissimulation des informations confidentielles. Pour ce faire, il faut avant tout activer la fonction qui autorise l'activation à distance de la dissimulation des informations.

Pour autoriser l'activation à distance de la dissimulation des informations confidentielles, procédez comme suit :

1. Choisissez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Mode**.

   L'écran **Mode** s'ouvre.

3. Cochez la case **Masquer sur instruction SMS** (cf. ill. ci-après).

Figure 113 : paramètres d'activation à distance du composant Contacts personnels

4. Appuyez sur **OK**.

Vous pouvez activer à distance la dissimulation des informations confidentielles d'une des méthodes suivantes :

- Sur un autre appareil nomade doté de l'application de Kaspersky Lab pour appareils nomades (par exemple, Kaspersky Mobile Security 9.0), composez une instruction SMS et envoyez-la à votre appareil. Pour rédiger l'instruction SMS spéciale, utilisez la fonction Envoi d'une instruction. La réception du SMS par votre appareil passera inaperçu et déclenchera la dissimulation des informations confidentielles.

- Sur un autre appareil mobile, rédigez le SMS avec le texte spécial et le code secret de l'application sur votre appareil et envoyez-le à votre appareil. Votre appareil recevra le SMS et les informations confidentielles seront masquées.

Pour activer à distance la dissimulation des informations confidentielles à l'aide d'une instruction spéciale envoyée par SMS, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Envoi d'une instruction**.

   L'écran **Envoi d'une instruction** s'ouvre.

3. Attribuez au paramètre **Instruction SMS** la valeur **Contacts personnels** (cf. ill. ci-après).

4. Dans le champ **Numéro de téléphone**, saisissez le numéro de téléphone de l'appareil qui va recevoir l'instruction SMS.

5. Dans le champ **Code distant**, saisissez le code secret de l'appareil qui va recevoir l'instruction SMS.

Figure 114 : lancement à distance de Contacts personnels

6. Appuyez sur **Envoyer**.

Quand l'appareil aura reçu l'instruction par SMS, la dissimulation des informations confidentielles sera activée automatiquement.

Pour activer à distance la dissimulation des informations confidentielles à l'aide de la fonction standard de rédaction de SMS, procédez comme suit :

envoyez à l'appareil un SMS contenant le texte `hide:<code>` (où `<code>` est le code secret de l'application défini sur l'appareil récepteur). Le message n'est pas sensible à la casse et les espaces avant ou après le signe deux-points sont ignorés.

COMPOSITION DE LA LISTE DES NUMEROS CONFIDENTIELS

La liste des contacts contient les numéros confidentiels dont les informations et les événements sont masqués par le composant Contacts personnels. La liste des numéros peut être enrichie manuellement, via importation depuis les contacts ou depuis la carte SIM

DANS CETTE SECTION

AJOUT D'UN NUMERO A LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez ajouter à la Liste de contacts des numéros de téléphone et des contacts enregistrés sur la carte SIM ou dans le répertoire téléphonique de l'appareil.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour ajouter un numéro de téléphone à la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

3. Exécutez une des opérations suivantes (cf. ill. ci-après) :

   - Pour ajouter un numéro du répertoire téléphonique, choisissez **Menu** → **Ajouter** → **Contact Outlook**. Dans l'écran **Contact Outlook** qui s'ouvre, choisissez l'entrée requise, puis appuyez sur **Sélectionner**.

   - Pour ajouter un numéro enregistré sur la carte SIM, sélectionnez **Menu** → **Ajouter** → **Contact de la carte SIM**. Dans l'écran **Contact de la carte SIM** qui apparaît, choisissez l'enregistrement requis, puis cliquez sur **OK**.

- Pour ajouter un numéro manuellement, choisissez l'option **Menu** → **Ajouter** → **Numéro**. Dans l'écran **Ajouter entrée** qui apparaît, remplissez le champ **Numéro de téléphone** puis cliquez sur **OK**.

Figure 115: ajout d'un enregistrement à la liste des contacts protégés

Le numéro est alors ajouté à la liste des contacts.

MODIFICATION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Seuls les numéros qui ont été saisis manuellement dans la liste des contacts peuvent être modifiés. Il est impossible de modifier les numéros sélectionnés dans le répertoire ou dans la liste des numéros de la carte SIM.

Pour modifier le numéro dans la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

3. Sélectionnez le numéro à modifier dans la Liste de contacts, puis choisissez **Options** → **Modifier**.

   L'écran **Modifier entrée** s'ouvre.

4. Modifiez les données dans le champ **Numéro de téléphone**.

5. Appuyez sur **OK** une fois les modifications terminées.

Le numéro sera modifié

SUPPRESSION D'UN NUMERO DE LA LISTE DES NUMEROS CONFIDENTIELS

Vous pouvez supprimer un numéro ou effacer tout le contenu de la Liste de contacts.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour supprimer un numéro de la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

3. Sélectionnez le numéro à supprimer, puis choisissez **Menu** → **Supprimer**.

4. Confirmez la suppression. Pour ce faire, appuyez sur le bouton **Oui**.

Pour purger la Liste de contacts, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Sélectionnez l'option **Liste des contacts**.

   L'écran **Liste de contacts** apparaît.

3. Sélectionnez l'option **Menu** → **Supprimer tout**.

4. Confirmez la suppression. Pour ce faire, appuyez sur le bouton **Oui**.

La Liste de contacts sera vide.

SELECTION DES INFORMATIONS A DISSIMULER : CONTACTS PERSONNELS

La fonction Contacts personnels masque par défaut les informations suivantes pour les numéros qui figurent dans la liste des contacts : contacts, SMS et entrées du journal des appels. Vous pouvez choisir les informations et les événements que la fonction Contacts personnels va dissimuler pour les numéros confidentiels.

Avant de modifier les paramètres des Contacts personnels, désactivez la fonction de dissimulation des informations confidentielles.

Pour choisir les informations et les événements à masquer pour les numéros confidentiels, procédez comme suit :

1. Sélectionnez **Menu** → **Contacts personnels**.

   L'écran **Contacts personnels** s'ouvre.

2. Choisissez l'option **Objets à masquer**.

   L'écran **Objets à masquer** (cf. ill. ci-après) apparaît.

3. Dans le groupe **Masquer les entrées**, choisissez les informations qui seront dissimulées pour les numéros confidentiels. Les paramètres suivants sont prévus:

   - **Contacts** : toutes les informations relatives aux numéros confidentiels sont masquées dans le répertoire téléphonique.
   - **SMS** : tous les SMS des numéros confidentiels sont masqués dans la liste des SMS entrants/sortants.
   - **Appels** : accepte les appels en provenance des numéros confidentiels mais masque le numéro de l'appelant et n'affiche pas les informations relatives aux numéros confidentiels dans la liste des appels (entrants, sortants ou en absence).

4. Dans le groupe **Masquer les événements**, sélectionnez les événements qui seront masqués pour les numéros confidentiels. Les paramètres suivants sont prévus:

   - **SMS entrants** : n'indique pas la réception de SMS entrants (rien n'indiquera à l'écran qu'un SMS en provenance d'un numéro confidentiel vient d'arriver). Tous les SMS envoyés depuis les numéros confidentiels pourront être consultés lorsque la dissimulation des informations confidentielles sera désactivée.
   - **Appels entrants** : bloque les appels en provenance des numéros confidentiels (dans ce cas, la personne qui appelle entendra la tonalité " occupé "). Les informations relatives à l'appel reçu sont affichées quand la dissimulation des informations confidentielles est désactivée.

Figure 116: Sélection des objets cachés

5. Appuyez sur **OK**.

FILTRAGE DE L'ACTIVITE DE RESEAU PARE-FEU

La section présente des informations sur le composant Pare-feu qui contrôle les connexions entrantes et sortantes sur votre périphérique. De plus, elle décrit comment activer/désactiver le composant et sélectionner le niveau de protection requis.

DANS CETTE SECTION

À PROPOS DU PARE-FEU

Le Pare-feu analyse toutes les connexions de réseau sur votre appareil. Il bloque ou autorise l'activité de réseau sur la base du niveau de protection sélectionné.

Le Pare-feu est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.0.

Les informations sur le fonctionnement du Pare-feu sont consignées dans le journal de l'application (voir section " Journaux de l'application " à la page 199).

ACTIVATION/DESACTIVATION DU PARE-FEU

Le fonctionnement du Pare-feu repose sur les niveaux de protection. Le niveau de sécurité permet de spécifier quels protocoles réseau sont autorisés, ou au contraire interdits, pour le transfert de données.

Les niveaux de sécurité suivants sont prévus :

- **Désact.** : autorisation de la moindre activité de réseau. Ce niveau de sécurité est choisi par défaut.
- **Protection minimum** : bloque uniquement les connexions entrantes. Les connexions sortantes sont autorisées.
- **Protection maximum** : bloque toutes les connexions entrantes. La réception du courrier, la consultation d'Internet et le téléchargement de fichiers sont autorisés. Les connexions sortantes peuvent être réalisées uniquement via les ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3.
- **Bloquer tout** : bloque la moindre activité de réseau, à l'exception de la mise à jour des bases antivirus et du renouvellement de la licence.

Vous pouvez modifier le niveau de sécurité offert par Pare-feu (cf. la rubrique " Sélection du niveau de sécurité du Pare-feu " à la page 187). Le mode actuel apparaît sur l'écran **Pare-feu** à côté de l'option du menu **Mode**.

SELECTION DU NIVEAU DE SECURITE DU PARE-FEU

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour sélectionner le niveau de protection du Pare-feu, procédez comme suit :

1. Sélectionnez **Menu** → **Pare-feu**.

   L'écran **Pare-feu** apparaît.

2. Sélectionnez l'option **Mode**.

   L'écran **Paramètres** s'ouvre.

3. Sélectionnez un des niveaux de sécurité proposé (cf. ill. ci-après).

Figure 117: sélection du niveau de sécurité du Pare-feu

4. Appuyez sur **OK**.

NOTIFICATIONS SUR LES BLOCAGES

Le Pare-feu permet d'obtenir des notifications sur le blocage des connexions. Vous pouvez administrer les notifications du Pare-feu.

Par défaut, la remise des notifications sur le blocage est désactivée.

➧ *Pour administrer les notifications sur le blocage, procédez comme suit :*

1. Sélectionnez **Menu** → **Pare-feu**.

   L'écran **Pare-feu** apparaît.

2. Choisissez l'option **Notifications**.

L'écran **Notifications** (cf. ill. ci-après) s'ouvre.

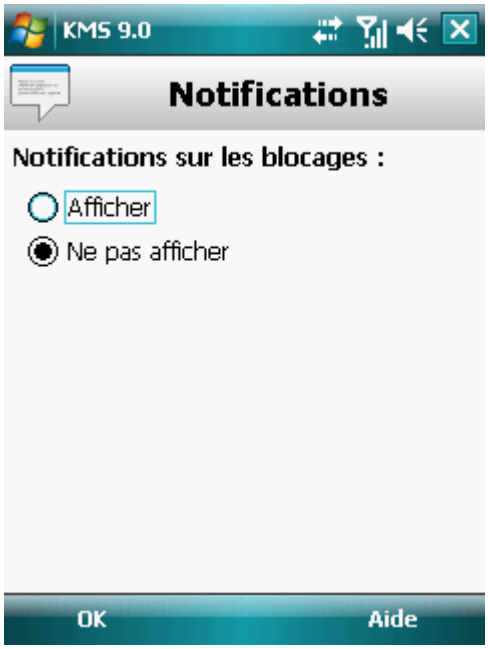


Figure 118 : configuration de la remise des notifications sur le blocage

3. Dans le groupe **Notifications sur les blocages**, sélectionnez une des options proposées :

   - **Afficher** : active la remise des notifications. Le Pare-feu signale le blocage de la connexion.
   - **Ne pas afficher** : désactive la remise des notifications. Le Pare-feu ne signale pas le blocage de la connexion.

4. Appuyez sur **OK**.

CHIFFREMENT DES DONNÉES PERSONNELLES

Cette section fournit des informations sur le composant Chiffrement qui protège les données confidentielles sur votre appareil. De plus, la rubrique décrit comment activer/désactiver le composant et chiffrer/déchiffrer les dossiers sélectionnés.

DANS CETTE SECTION

À PROPOS DU CHIFFREMENT

Le composant Chiffrement protège les données sur l'appareil contre la consultation par des tiers même s'ils ont pu accéder à l'appareil nomade. Le composant permet de chiffrer n'importe quel nombre de dossiers qui ne sont pas du système.

Pour chiffrer/déchiffrer les données, il suffit de saisir le code secret (cf. la rubrique " Saisie du code secret " à la page 121). Une fois que la période définie après le passage de l'appareil en mode d'économie de l'énergie est écoulée (cf. la rubrique " Interdiction d'accès aux données chiffrées " à la page 193), l'accès aux données est bloqué automatiquement.

Le contenu du dossier est chiffré dès l'exécution de la commande **Chiffrer** après quoi les données sont chiffrées ou déchiffrées " au vol " au fur et à mesure que des données sont ajoutées, extraites ou consultées dans le dossier.

Pour lancer les fichiers exécutables exe depuis le dossier chiffré, il faut d'abord déchiffrer le dossier.

Le composant Chiffrement est désactivé par défaut après l'installation de Kaspersky Mobile Security 9.0.

Les informations sur le fonctionnement du composant sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

CHIFFREMENT DES DONNEES

Le composant Chiffrement permet de chiffrer un nombre quelconque de dossiers non systèmes qui se trouvent dans la mémoire de l'appareil ou sur une carte mémoire.

La liste de tous les dossiers chiffrés ou déchiffrés antérieurement est accessible dans l'écran **Chiffrement** via l'option **Liste des dossiers**.

Vous pouvez également chiffrer directement tous les dossiers qui se trouvent dans la liste des dossiers.

Pour chiffrer les données, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Appuyez sur **Menu** → **Ajouter un dossier**.

   L'écran reprenant l'arborescence du système de fichiers de l'appareil apparaît.

4. Sélectionnez le dossier qu'il faut absolument chiffrer, puis appuyez sur **Chiffrer** (cf. ill. ci-après).

Pour parcourir le système de fichiers, utilisez le stylet ou les boutons du joystick de l'appareil.

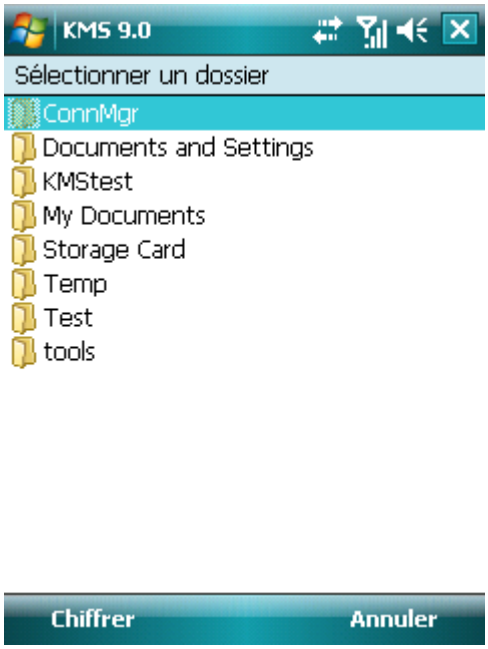


Figure 119: chiffrement des données

Kaspersky Mobile Security 9.0 vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

5. Appuyez sur **OK**.

   Pour le dossier sélectionné, l'option **Chiffrer** du **Menu** devient **Déchiffrer**.

Après le chiffrement, les donnée sont déchiffrées et chiffrées automatiquement lorsque vous manipulez des données depuis un dossier chiffré, lorsque vous les extrayez du dossier chiffré ou y placer de nouvelles données.

Pour chiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Sélectionnez **Menu** → **Actions compl.** → **Tout chiffrer**.

   Kaspersky Mobile Security 9.0 vous préviendra lorsque la procédure de chiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Appuyez sur **OK**.

DÉCHIFFREMENT DES DONNÉES

Il est possible de déchiffrer complètement les données préalablement chiffrées (cf. la rubrique " Chiffrement de données " à la page 190) Vous pouvez déchiffrer un seul dossier ou tous les dossiers chiffrés sur l'appareil.

Pour déchiffrer un dossier chiffré, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** apparaît. Il reprend la liste de tous les dossiers chiffrés et déchiffrés antérieurement.

3. Sélectionnez le dossier chiffré dans la liste, puis appuyez sur **Menu** → **Déchiffrer** (cf. ill. ci-après).

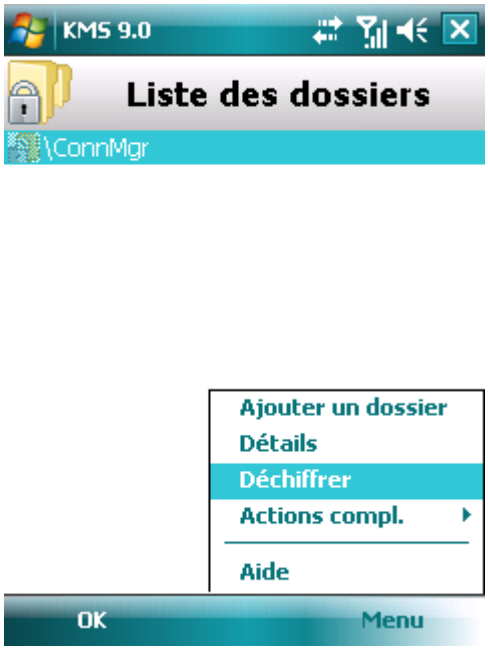


Figure 120: activation de la fonction

   Kaspersky Mobile Security 9.0 vous préviendra lorsque la procédure de déchiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Appuyez sur **OK**.

Pour le dossier déchiffré, l'option **Déchiffrer** du **Menu** devient **Chiffrer**. Vous pouvez à nouveau utiliser le chiffrement de données (cf. la rubrique " Chiffrement de données " à la page 190).

Pour déchiffrer directement tous les dossiers de la liste, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Liste des dossiers**.

   L'écran **Liste des dossiers** s'ouvre.

3. Sélectionnez **Menu** → **Actions compl.** → **Tout déchiffrer**.

   Kaspersky Mobile Security 9.0 vous préviendra lorsque la procédure de déchiffrement sera terminée. Une fenêtre contenant une notification s'affiche.

4. Appuyez sur **OK**.

INTERDICTION D'ACCES AUX DONNEES CHIFFREES

Le chiffrement permet de bloquer l'accès aux données chiffrées de manière instantanée ou à l'issue d'une période définie après le passage de l'appareil en mode d'économie d'énergie.

Par défaut, l'accès aux données chiffrées est bloqué directement après que le rétroéclairage de l'écran se coupe.

Vous pouvez définir la durée pendant laquelle les données chiffrées resteront accessibles après le passage de l'appareil en mode d'économie d'énergie. Ensuite, pour pouvoir utiliser les données chiffrées, il faudra saisir le code secret (cf. la rubrique " Saisie du code secret " à la page 121).

Vous pouvez également verrouiller momentanément l'accès aux données chiffrées et demander la saisie du code secret.

Pour bloquer l'accès au dossier après l'écoulement d'une durée définie, procédez comme suit :

1. Sélectionnez **Menu** → **Chiffrement**.

   L'écran **Chiffrement** s'ouvre.

2. Choisissez l'option **Interdiction de l'accès**.

   L'écran **Interdiction de l'accès** s'ouvre

3. Définissez la durée après le passage de l'appareil en mode de veille pendant laquelle les données seront accessibles. Pour ce faire, attribuez au paramètre **Interdire l'accès** une des valeurs proposées (cf. ill. ci-après) :

   - **Sans délai**.
   - **1 minute**.
   - **5 minutes**.
   - **15 minutes**.
   - **1 heure**.

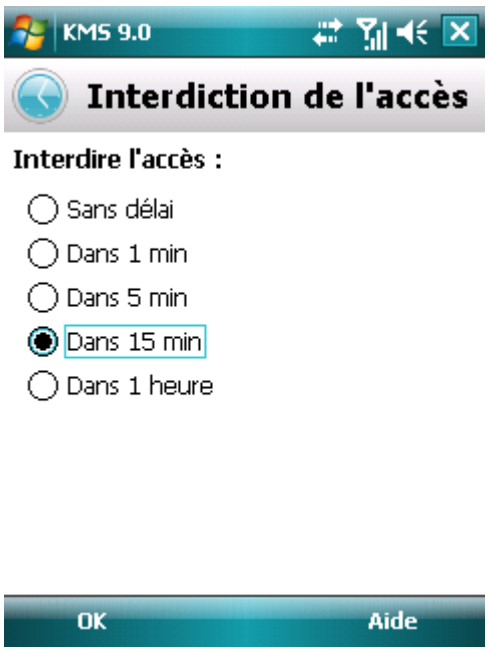


Figure 121: blocage de l'accès aux données chiffrées

4. Appuyez sur **Terminé** pour enregistrer les modifications.

Pour interdire momentanément l'accès aux dossiers,

cliquez sur l'icône de Kaspersky Mobile Security 9.0 dans la barre d'état système de l'appareil et choisissez l'option **Verrouiller les données** (cf. ill. ci-après).

Figure 122: menu contextuel de l'application dans la barre d'état système de l'appareil

MISE A JOUR DES BASES DU PROGRAMME

La section présente la mise à jour des bases antivirus de l'application qui garantit l'actualité de la protection de votre appareil. Elle explique également comment consulter les informations relatives aux bases antivirus installées, comment lancer la mise à jour manuelle ou comment programmer celle-ci.

DANS CETTE SECTION

À PROPOS DE LA MISE A JOUR DES BASES

La recherche d'application malveillante s'opère à l'aide de base de données qui contiennent les descriptions de toutes les applications malveillantes connues à ce jour et des moyens de les neutraliser ainsi que des descriptions d'autres objets indésirables. Il est extrêmement important d'assurer la mise à jour des bases antivirus.

Il est conseillé d'actualiser régulièrement les bases antivirus de l'application. Si plus de 15 jours se sont écoulés depuis la dernière mise à jour, les bases antivirus de l'application sont considérées comme étant fortement dépassées. Dans ces conditions, il est impossible de garantir la fiabilité de la protection.

Kaspersky Mobile Security 9.0 télécharge la mise à jour de l'application depuis les serveurs de mises à jour de Kaspersky Lab. Il s'agit de sites Internet spéciaux où sont hébergés les mises à jour des bases pour toutes les applications de Kaspersky Lab.

Pour pouvoir actualiser les bases antivirus de l'application, une connexion Internet doit être configurée sur l'appareil.

La mise à jour des bases antivirus de l'application s'opère selon l'algorithme suivant :

1. Les bases antivirus de l'application installées sur votre appareil sont comparées aux bases disponibles sur un serveur de mise à jour spécial de Kaspersky Lab.

2. Kaspersky Mobile Security 9.0 exécute une des actions suivantes :

   - Si les bases antivirus de l'application que vous utilisez sont à jour, un message d'informations apparaît à l'écran.

   - Si les bases antivirus installées diffèrent, alors le nouveau paquet de mise à jour sera téléchargé et installé.

     Une fois la mise à jour terminée, la connexion est automatiquement coupée. Si la connexion était déjà établie avant la mise à jour, elle reste alors disponible pour d'autres opérations.

Vous pouvez lancer la tâche de mise à jour manuellement à n'importe quel moment, si l'appareil n'est pas occupé par l'exécution d'autres tâches ou programmer l'exécution de la mise à jour.

Vous pouvez obtenir des informations détaillées sur les bases antivirus utilisées sur l'écran **Informations** via le point **Infos des bases**.

Les informations sur la mise à jour des bases antivirus sont consignées dans le journal de l'application (cf. la rubrique " Journaux de l'application " à la page 199).

AFFICHAGE D'INFORMATIONS SUR LES BASES

Vous pouvez consulter les informations sur les bases antivirus de l'application installées. Les données suivantes sont accessibles : date de la dernière mise à jour, date d'édition des bases et nombre d'enregistrements dans la base.

Pour consulter les informations relatives aux bases antivirus installées, procédez comme suit :

1. Choisissez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Infos des bases**.

L'écran **Infos des bases** s'ouvre. Il présente des informations sur les bases antivirus de l'application installées (cf. ill. ci-après).

Figure 123: informations relatives aux bases de l'application installées

MISE A JOUR MANUELLE

Vous pouvez lancer manuellement la mise à jour des bases antivirus de l'application.

Pour lancer la mise à jour des bases antivirus de l'application, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Mise à jour** (cf. ill. ci-après).

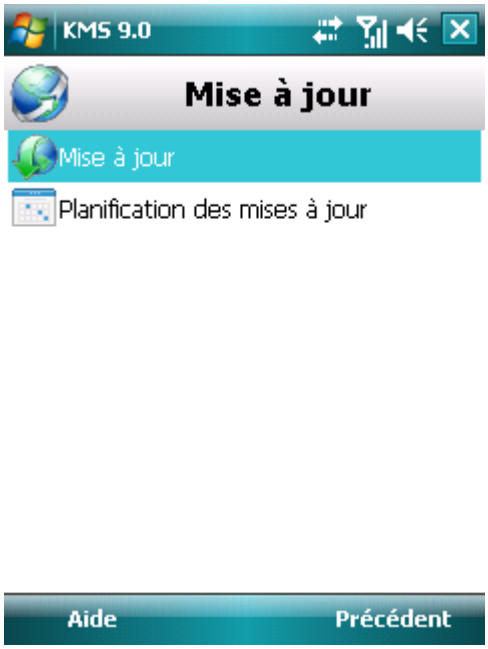


Figure 124: lancement manuel de la mise à jour

L'application lance la mise à jour des bases antivirus depuis le serveur de Kaspersky Lab. Les informations sur la mise à jour apparaissent à l'écran.

PLANIFICATION DES MISES A JOUR

Des mises à jour régulières sont nécessaires pour assurer une protection efficace de l'appareil protection contre les objets malveillants. Pour votre confort, vous pouvez configurer l'exécution automatique de la mise à jour des bases antivirus de l'application.

Pour configurer la mise à jour automatique des bases du logiciel, procédez de la manière suivante :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des mises à jour**.

   L'écran **Planification** s'ouvre.

4. Cochez la case **Mise à jour programmée** (cf. ill. ci-après).

5. Programmez l'exécution de la mise à jour. Pour ce faire, attribuez une valeur au paramètre **Fréquence** :

   - **Chaque jour** : actualise les bases antivirus chaque jour. Saisissez ensuite la valeur pour le paramètre **Heure**.

- **Chaque semaine** : actualise les bases antivirus de l'application une fois par semaine. Ensuite, sélectionnez une valeur pour les paramètres **Heure** et **Jour de la semaine**.

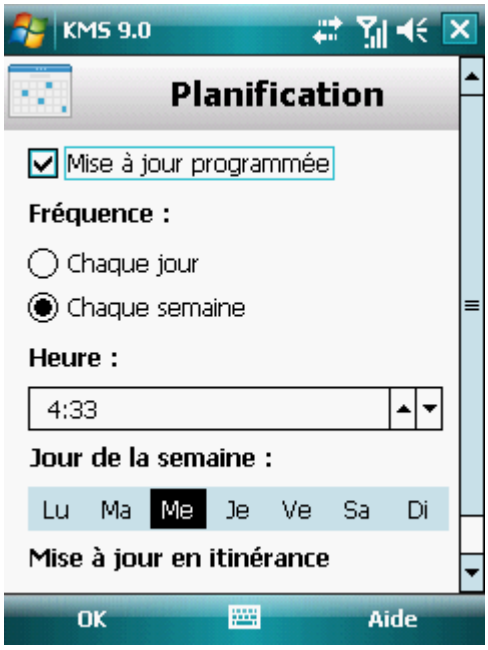


Figure 125: Paramètres de la mise à jour automatique

6. Appuyez sur **OK** pour enregistrer les modifications.

MISE A JOUR EN ITINERANCE

Si vous êtes en itinérance, vous pouvez activer/désactiver la mise à jour programmée des bases antivirus de l'application. Si la mise à jour programmée en itinérance est interdite, la mise à jour manuelle sera accessible en mode normal.

Pour autoriser la mise à jour des bases de l'application en cas d'itinérance, procédez comme suit :

1. Choisissez **Menu** → **Anti-Virus**.

   L'écran **Anti-Virus** apparaît.

2. Sélectionnez l'option **Mise à jour**.

   L'écran **Mise à jour** s'ouvre.

3. Sélectionnez **Planification des MAJ**.

   L'écran **Planification** s'ouvre.

4. Dans le groupe **Mise à jour en itinérance**, cochez la case **Mettre à jour en itinérance**.

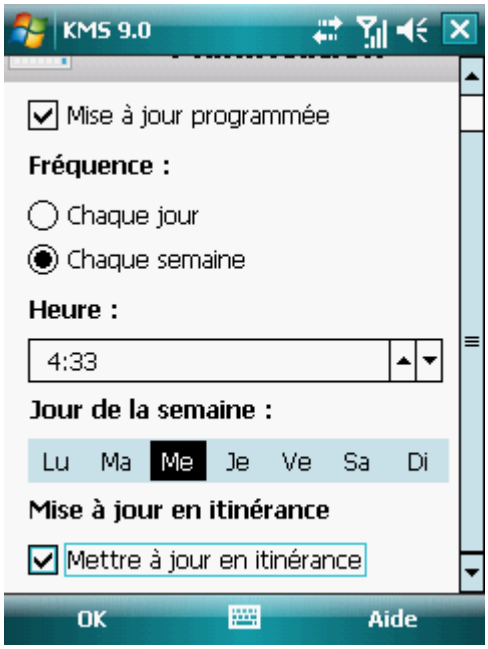


Figure 126 : configuration des mises en jour en itinérance

5. Appuyez sur **OK** pour enregistrer les modifications.

JOURNAUX DU LOGICIEL

La section présente des informations sur les journaux où sont consignées les informations sur le fonctionnement de chaque composant ainsi que les informations sur l'exécution de chaque tâche (par exemple, mise à jour des bases antivirus de l'application, analyse antivirus, etc.)

DANS CETTE SECTION

À PROPOS DES JOURNAUX

Les journaux reprennent les enregistrements sur les événements survenus pendant le fonctionnement de chaque composant de Kaspersky Mobile Security 9.0. Les enregistrements sont triés par l'heure de l'événement et classés dans l'ordre chronologique.

Il existe un journal des événements pour chaque composant.

AFFICHAGE DES EVENEMENTS DU JOURNAL

Pour afficher tous les enregistrements repris dans le journal, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

L'écran **Avancé** s'ouvre

2. Choisissez l'option **Journaux**.

   L'écran **Journaux** s'ouvre.

3. Choisissez le composant pour lequel vous souhaitez consulter le journal.

Le journal du composant sélectionné s'ouvre (cf. ill. ci-après).

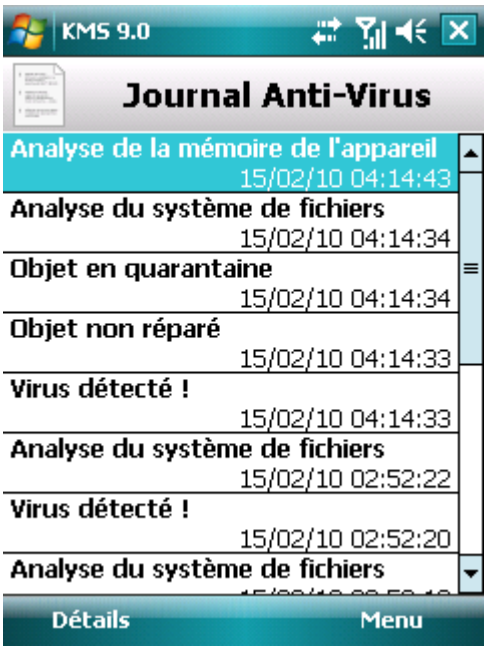


Figure 127 : Affichage d'événements dans les journaux

- *Pour afficher des informations détaillées sur les enregistrements du journal,*

  sélectionnez l'enregistrement requis puis cliquez sur **Détails**.

  L'écran **Détails** reprend des informations sur l'action exécutée par l'application et ses détails. Par exemple, pour l'action " Objet en quarantaine ", le chemin d'accès au fichier infecté sur l'appareil est également affiché.

- *Pour revenir à la liste des journaux,*

  appuyez sur **Menu** → **Précédent**.

SUPPRESSION DES ENREGISTREMENTS DU JOURNAL

Vous pouvez purger tous les journaux. Les informations relatives au fonctionnement des composants de Kaspersky Mobile Security 9.0 seront supprimées.

- *Pour purger tous les journaux, procédez comme suit :*

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Choisissez l'option **Journaux**.

   L'écran **Journal** s'ouvre

3. Ouvrez le journal de n'importe quel composant.

4. Choisissez **Menu** → **Supprimer tout** (cf. ill. ci-dessous).

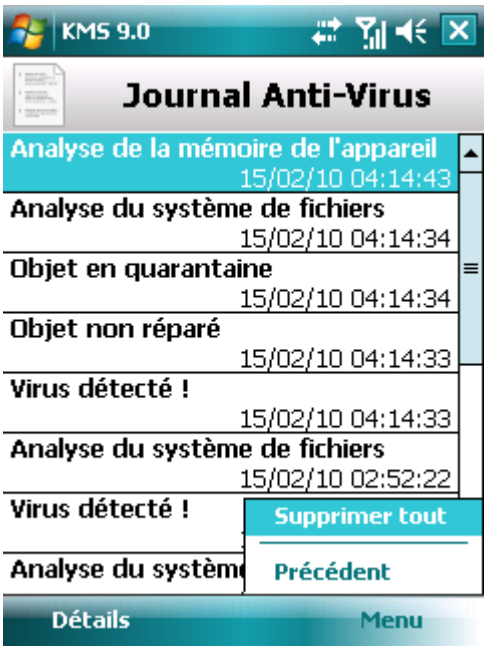


Figure 128: suppression des enregistrements

5. Pour confirmer la suppression, appuyez sur le bouton **Oui**.

Tous les événements du journal de chaque composant seront supprimés.

CONFIGURATION DES PARAMETRES COMPLEMENTAIRES

La section offre des informations sur les possibilités complémentaires de Kaspersky Mobile Security 9.0 : comment modifier le code secret, administrer les notifications sonores de l'application et comment activer/désactiver l'affichage des astuces.

DANS CETTE SECTION

MODIFICATION DU CODE SECRET

Vous pouvez modifier le code secret défini après l'activation de l'application.

Pour changer le code secret, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

3. Choisissez l'option **Modification du code**.

4. Tapez le code actuel dans la zone **Saisissez le code**.

5. Saisissez le nouveau code dans le champ **Saisissez le nouveau code** et **Confirmation du code**, puis cliquez sur **OK** pour conserver les modifications.

AFFICHAGE DES ASTUCES

Lorsque vous configurez les paramètres des composants, Kaspersky Mobile Security 9.0 affiche par défaut des astuces reprenant une brève description de la fonction sélectionnée. Vous pouvez configurer l'affichage des astuces de Kaspersky Mobile Security 9.0.

Pour configurer l'affichage des astuces, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

3. Sélectionnez l'option **Astuces**.

   L'écran **Astuces** s'ouvre.

4. Sélectionnez une des valeurs proposées pour le paramètre **Astuces** :

   - **Afficher** : affiche l'astuce avant de configurer les paramètres de la fonction sélectionnée.
   - **Masquer** : aucune astuce n'est affichée.

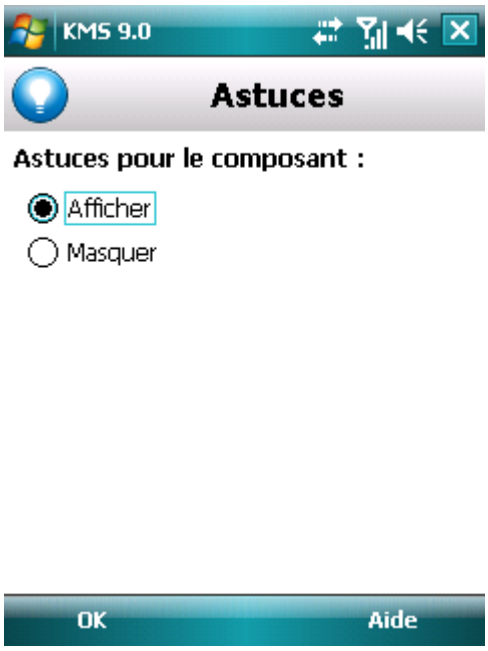


Figure 129: configuration de l'affichage des astuces.

5. Appuyez sur **OK**.

NOTIFICATIONS SONORES

Divers événements définis peuvent survenir durant l'utilisation de l'application : découverte d'un objet infecté ou d'un virus, expiration de la licence, etc. Pour que l'application vous signale chacun de ces événements, vous pouvez activer la notification sonore pour les événements survenus.

Par défaut, Kaspersky Mobile Security 9.0 active la notification sonore uniquement selon le mode défini de l'appareil.

Pour modifier les valeurs des paramètres, utilisez le stylo ou le joystick de votre appareil.

Pour administrer les notifications sonores de l'application, procédez comme suit :

1. Sélectionnez **Menu** → **Avancé**.

   L'écran **Avancé** s'ouvre

2. Sélectionnez l'option **Paramètres**.

   L'écran **Paramètres** s'ouvre.

3. Choisissez l'option **Son**.

   L'écran **Son** s'ouvre.

4. Sélectionnez une des valeurs proposées pour le paramètre **Notifications sonores** (cf. ill. ci-après) :

   - **Activer** : utilise les notifications sonores quel que soit le profil sélectionné pour l'appareil.
   - **Désactiver** : n'utilise pas les notifications sonores.

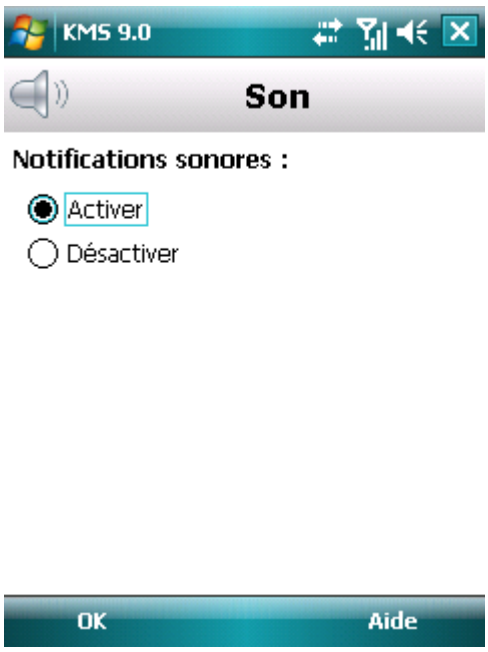


Figure 130 : contrôle des notifications sonores

5. Appuyez sur **OK** pour enregistrer les modifications.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez déjà acheté Kaspersky Mobile Security, des informations peuvent être obtenues auprès du Service d'assistance technique par téléphone ou par Internet.

Les experts du Service d'assistance technique répondront à vos questions sur l'installation et l'utilisation du logiciel et, si votre appareil mobile est infecté par une activité malveillante, ils vous aideront à en éliminer les conséquences.

Avant de prendre contact avec le Service d'assistance technique, prenez connaissance des Règles de support (http://support.kaspersky.com/fr/support/rules).

Écrire sa question au Service d'assistance technique

Vous pouvez transmettre votre demande aux spécialistes du Service d'assistance technique en remplissant le formulaire du Helpdesk à l'adresse: https://my.kaspersky.com/fr.

Vous pouvez rédiger votre demande en allemand, anglais, espagnol, français ou en russe.

Pour traiter votre demande par messagerie, vous devez indiquer le reçu en même **numéro de client**temps que votre mot **de passe** lors de votre enregistrement sur le site du Service d'assistance technique.

Si vous n'êtes pas encore inscrit en tant qu'utilisateur d'applications Kaspersky Lab, vous disposez d'un formulaire pour ce faire sur le site du Helpdesk (https://my.kaspersky.com/fr/registration). Pendant votre inscription, saisissez le *code d'activation* du logiciel ou le fichier *clé de licence*.

Vous recevrez la réponse d'in spécialiste du Service d'assistance technique dans votre Espace personnel (https://my.kaspersky.com/fr) et à l'adresse de messagerie précisée dans votre demande.

Décrivez votre problème avec tous les détails possibles dans le formulaire de saisie de votre demande. Spécifiez dans les champs obligatoires :

- **Le type de demande**. Sélectionnez le sujet qui correspond le mieux au problème rencontré, par exemple, " Problème d'installation/de suppression du logiciel " ou " Problème de recherche/de neutralisation de virus ". Si vous ne trouvez pas un sujet qui se rapproche le plus de votre situation, choisissez " Question générale ".
- **Nom et version de l'application**.
- **Zone de texte**. Décrivez le problème rencontré avec le plus de détails possible.
- **Numéro client et mot de passe**. Saisissez l'Identifiant client et le mot de passe reçus lors de votre inscription sur le site du Service d'assistance technique.
- **Adresse de messagerie**. Les experts du Service d'assistance technique enverront leur réponse à cette adresse.

Assistance technique téléphonique

Si le problème est urgent, appelez le Service d'assistance technique de votre région. Avant de connecter localement (http://support.kaspersky.com/fr/desktop (Rubrique Contacter le Support Technique)) ou à l'international (http://support.kaspersky.com/fr/support/international) le Service d'assistance technique, préparez des informations (http://support.kaspersky.com/fr/support/details) sur votre appareil et sur l'application antivirus dont il est équipé. Ces informations réduiront le temps de réponse de nos spécialistes.

GLOSSAIRE

A

ACTIVATION DU LOGICIEL

Passage de l'application en mode pleinement opérationnel. L'utilisateur doit avoir une licence pour activer l'application.

ANALYSE A LA DEMANDE

Mode de fonctionnement du programme Kaspersky Lab exécuté à la demande de l'utilisateur et conçu pour analyser et vérifier tous les fichiers résidents.

ARCHIVE

Fichier " conteneur " d'un ou plusieurs autres objets pouvant être eux-mêmes des archives.

B

BASES

Bases de données maintenues par les experts de Kaspersky Lab contenant des descriptions détaillées de toutes les menaces de sécurité informatique existantes, ainsi que les méthodes permettant de les détecter et de les neutraliser. La base de données est constamment mise à jour par Kaspersky Lab chaque fois qu'une nouvelle menace apparaît.

BLOCAGE D'UN OBJET

Interdire l'accès à un objet par des programmes externes. Un objet interdit ne peut pas être lu, exécuté, modifié ni supprimé.

D

DUREE DE LICENCE

Période de temps pendant laquelle il est possible d'exploiter toutes les caractéristiques d'une application Kaspersky Lab. Normalement, la durée de validité d'une licence est d'une année calendaire, à compter de son installation. Après l'expiration de la licence, le fonctionnement du programme est limité : vous ne pouvez plus mettre à jour la base de données.

DESINFECTION OU REPARATION D'OBJETS

Méthode de traitement d'objets infectés permettant la récupération complète ou partielle des données, ou la prise d'une décision si l'objet ne peut être réparé. La réparation d'objets fait appel au contenu des bases de données. La réparation peut entraîner la perte d'une partie des données.

L

LISTE BLANCHE

Les entrées de cette liste contiennent :

- les numéros de téléphone, depuis lesquels les appels et les SMS entrants sont autorisés par l'Anti-Spam, et les numéros de téléphone sur lesquels les appels et les SMS sortants sont autorisés par le Contrôle Parental.
- le texte, dont la détection permet d'autoriser un SMS entrant.

LISTE NOIRE

Les entrées de cette liste contiennent :

- les numéros de téléphone, depuis lesquels les appels et les SMS entrants sont refusé par l'Anti-Spam, et les numéros de téléphone sur lesquels les appels et les SMS sortants sont refusé par le Contrôle Parental.

- le texte, dont la détection permet d'autoriser un SMS entrant

M

MASQUE DE FICHIERS

Représentation du nom et de l'extension d'un fichier moyennant des caractères génériques. Les deux caractères génériques de base utilisés dans les masques de fichier sont * et ? (où * représente une suite de caractères quelconques et ? un seul caractère). Grâce à ces caractères génériques, il est possible de désigner n'importe quel fichier. Notez que le nom et l'extension du fichier sont toujours séparés par un point.

MISES A JOUR

Procédé de remplacement ou d'ajout de nouveaux fichiers (bases de données ou composants logiciels), téléchargés depuis les serveurs de mise à jour de Kaspersky Lab.

N

NON-NUMERIQUES

Numéro de téléphone contenant des lettres ou composé intégralement de lettres.

O

OBJET INFECTE

Objet contenant du code malveillant : sa détection au cours de l'analyse est possible car une section du code de l'objet est identique à la section de code d'une menace déjà connue. Les experts de Kaspersky Lab ne recommandent pas d'utiliser des objets de ce type, qui peuvent causer l'infection de l' appareil.

P

PLACER DES OBJETS EN QUARANTAINE

Méthode permettant de traiter des objets probablement infectés, en interdisant leur accès et en les déplaçant de leur position d'origine vers le dossier de quarantaine, où l'objet est enregistré sous une forme chiffrée qui annule toute menace d'infection.

Q

QUARANTAINE

Dossier spécial dans lequel sont placés tous les objets probablement infectés, détectés pendant l'analyse de l' appareil ou par la protection en temps réel.

R

RESTAURATION

Restitution de l'objet en quarantaine ou sauvegardé dans le dossier d'origine où il se trouvait avant d'être placé en quarantaine ou réparé, ou bien encore, dans un autre dossier choisi par l'utilisateur.

S

SUPPRESSION SMS

Méthode de traitement d'un SMS contenant des caractéristiques indésirables (SPAM) impliquant sa suppression physique. Nous recommandons cette méthode pour des SMS clairement indésirables.

SUPPRESSION D'UN OBJET

Procédé de traitement d'un objet, impliquant sa suppression physique de l'emplacement où il a été détecté par le programme (disque fixe, dossier, ressource réseau). Nous recommandons d'appliquer ce traitement aux objets dangereux qui ne peuvent être, pour une raison quelconque, réparés.

KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, dans les pays du Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Un nouveau service de la compagnie, le centre européen de recherches antivirus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les analystes senior de Kaspersky Lab sont membres permanents de la CARO (Organisation pour la recherche antivirus en informatique).

Kaspersky Lab offre les meilleures solutions de sécurité, soutenues par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de lutte contre les virus informatiques. Une analyse approfondie de l'activité virale informatique permet aux spécialistes de la société de détecter les tendances dans l'évolution du code malveillant et d'offrir à nos utilisateurs une protection permanente contre les nouveaux types d'attaques. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour assurer la plus grande des protections antivirus aussi bien aux particuliers, qu'aux clients corporatifs.

Des années de dur travail ont fait de notre société l'un des premiers fabricants de logiciels antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Anti-Virus : il assure une protection complète de tous les systèmes informatiques contre les attaques de virus, comprenant les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab profitent d'un large éventail de services complémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. Nous assurons l'étude, l'installation et la maintenance de suites antivirus de grandes organisations. La base antivirus de Kaspersky Lab est mise à jour toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site Web de Kaspersky Lab:	http://www.kaspersky.com/fr
L'Encyclopédie des virus:	http://www.securelist.com/en
Laboratoire antivirus :	newvirus@kaspersky.com (envoi uniquement d'objets suspects sous forme d'archive) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=fr (pour les questions aux experts antivirus)
Forum de Kaspersky Lab :	http://forum.kaspersky.com

AUTRES INFORMATIONS

La bibliothèque logicielle de protection des informations (BLPI) Crypto C, développée par CryptoEx intervient dans la formation et la vérification de la signature numérique dans Kaspersky Mobile Security.

Le site de CryptoEx : http://www.cryptoex.ru

INDEX

A

C

D

E

I

J

L

M

N

O

P

Q

R

S