Kaspersky Internet Security for Android

Manual Do Utilizador

Estimado utilizador,

Obrigado por escolher o nosso produto. Esperamos que esta documentação lhe seja útil e lhe forneça respostas à maioria das suas questões que possam surgir.

Nota: Este documento é propriedade do Kaspersky Lab ZAO (doravante referido como Kaspersky Lab): todos os direitos a este documento são reservados pelas leis de copyright da Federação Russa, e por tratados internacionais. A reprodução e distribuição ilegais deste documento ou de partes do mesmo resultará em responsabilidade civil, administrativa ou criminal, de acordo com as leis aplicáveis.

Apenas é permitido qualquer tipo de reprodução ou distribuição de quaisquer materiais, incluindo traduções, com a permissão por escrito da Kaspersky Lab.

Este documento, bem como as imagens gráficas relacionadas com o mesmo, podem ser utilizadas para fins exclusivamente informativos, não comerciais e pessoais.

A Kaspersky Lab reserva-se o direito de alterar este documento sem aviso prévio. Pode obter a versão mais recente deste documento no site da Kaspersky Lab, no endereço <u>http://www.kaspersky.com/pt/docs</u>.

A Kaspersky Lab não será responsável pelo conteúdo nem pela qualidade, relevância ou exactidão de quaisquer materiais utilizados neste documento cujos direitos sejam detidos por terceiros, bem como por quaisquer perdas potenciais associadas à utilização destes documentos.

Data de revisão do documento: 30.01.2014

© 2014 Kaspersky Lab ZAO. Todos os direitos reservados.

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

ÍNDICE

SOBRE ESTE MANUAL	5
Neste documento	5
Convenções de documentos	6
FONTES DE INFORMAÇÃO SOBRE A APLICAÇÃO	8
Fontes de informação para pesquisa independente	8
Discutir as aplicações da Kaspersky Lab no Fórum	9
Contactar o Departamento de Vendas	9
Contactar o Departamento de Documentação Técnica e Localização por e-mail	9
KASPERSKY INTERNET SECURITY	
O que há de novo	
Requisitos de hardware e software	11
Kit de distribuição	
Serviços de utilizador	12
INSTALAR E DESINSTALAR A APLICAÇÃO	13
Instalar a anlicação	13
Desinstalar a aplicação	
	45
Janeia principal do Kaspersky internet Security	
Painel de início rápide	
fairlei de Inicio rapido	
Widget do ecrá inicial do dispositivo	
Notificações	
	22
Acorea da Acorda da Licanza da Utilizadar Einal	
Sobre a licenca	
Sobre o código de activação	23
Acerca do fornecimento de dados	23
INICIAR E PARAR A APLICAÇAO	25
GUIA RÁPIDO DE INSTALAÇÃO	
Como proceder em caso de detecção de um objecto malicioso	
Como proteger dados contra acessos não autorizados	
Finalidade do código secreto	27
O que é uma Conta Kaspersky	
Efectuar a configuração inicial do Anti-Roubo	
O que fazer em caso de perda ou roubo do dispositivo	
PROCESSAR TAREFAS PADRÃO	
Scanner (Antivírus)	
Verificação completa do dispositivo	
Verificação rápida	
Verificação de ficheiros e pastas	
Verificação agendada automática	

Actualizar as bases de dados de antivírus e a versão da aplicação	32
Actualizações agendadas automáticas	32
Protecção de Privacidade	33
Ocultar informações relacionadas com contactos	33
Iniciar remotamente a Protecção de Privacidade a partir de outro dispositivo	34
Anti-Roubo	34
Adicionar um dispositivo à conta de Web Management	35
Enviar comandos de SMS do Kaspersky Internet Security	35
Controlar o cartão SIM remotamente	36
Bloquear e localizar o dispositivo remotamente	36
Activar o alarme do dispositivo remotamente	37
Limpar dados do dispositivo remotamente	
Tirar uma fotografia de identificação	39
Filtro de Texto e Chamadas	40
Filtro de contactos padrão	40
Bloquear todos os contactos excepto os permitidos	40
Bloquear apenas contactos não solicitados	41
Protecção de Internet e Anti-Phishing de Texto	41
Verificação constante de sites	42
Verificação constante de ligações de mensagens SMS	42
Outras tarefas	42
Activar a versão Premium da aplicação	43
Adquirir a licença	43
Renovar licença	44
Ver informações sobre a licença e respectivo período de validade	44
Visualizar os relatórios de funcionamento da aplicação	44
Alterar o código secreto	45
Recuperação do código secreto	45
CONTACTAR O SERVIÇO DE SUPORTE TÉCNICO	46
Obter suporte técnico	46
Suporte Técnico por telefone	46
Obter suporte técnico através da Conta Kaspersky	46
GLOSSÁRIO	48
KASPERSKY LAB	50
INFORMAÇÃO SOBRE CÓDIGO DE TERCEIROS	51
AVISOS DE MARCAS COMERCIAIS	52
ÍNDICE	53

SOBRE ESTE MANUAL

Este documento é o Manual de Utilizador do Kaspersky Internet Security for Android (doravante designado "Kaspersky Internet Security").

O Manual do Utilizador destina-se aos utilizadores do Kaspersky Internet Security que estão familiarizados com a interface do sistema operativo, têm conhecimentos básicos da utilização do sistema e sabem como utilizar a Internet.

Este Manual destina-se a:

- Ajudar na instalação, activação e utilização do Kaspersky Internet Security.
- Permitir uma procura rápida de informações sobre questões relacionadas com a aplicação.
- Descrever fontes adicionais de informações acerca da aplicação e formas de receber Suporte Técnico.

NESTA SECÇÃO

Neste documento	<u>5</u>
Convenções de documentos	<u>6</u>

NESTE DOCUMENTO

Este manual inclui as seguintes secções.

Fontes de informação sobre a aplicação

Esta secção descreve fontes de informação acerca da aplicação e apresenta uma lista de sites que pode utilizar para discutir o funcionamento da aplicação.

Kaspersky Internet Security

Esta secção descreve as funcionalidades da aplicação e fornece informação resumida sobre as funções e componentes da mesma. Ficará a saber quais os itens incluídos no kit de distribuição e quais os serviços que estão disponíveis para os utilizadores registados da aplicação. Esta secção fornece informação acerca dos requisitos de software e hardware que o computador deve cumprir para permitir que o utilizador instale a aplicação no mesmo.

Instalar e desinstalar a aplicação

Esta secção contém instruções detalhadas para instalar e remover o Kaspersky Internet Security.

Interface da aplicação

Esta secção contém indicações sobre os principais elementos da interface gráfica da aplicação: janela principal, indicador do estado de protecção em forma de escudo, painel de início rápido, ícone da aplicação, widget e janelas de notificações.

Licenciar a aplicação

Esta secção fornece informação acerca dos termos gerais relacionados com a activação da aplicação. Leia esta secção para saber mais sobre o objectivo do contrato de licença, as formas de activação da aplicação e a renovação da licença.

Iniciar e parar a aplicação

Esta secção contém informações sobre como iniciar a aplicação e parar a utilização da mesma.

Guia Rápido de Instalação

Esta secção descreve como começar a utilizar a aplicação rapidamente após a instalação:

- Instruções para neutralizar um objecto malicioso;
- Informações sobre como proteger os seus dados contra acesso não autorizado;
- Instruções a seguir em caso de furto ou extravio do dispositivo.

Processar tarefas padrão

Esta secção contém instruções passo a passo sobre como executar as tarefas de utilizador básicas associadas à aplicação.

Contactar o Serviço de Suporte Técnico

Esta secção contém informações acerca de como contactar o Serviço de Suporte Técnico da Kaspersky Lab.

Glossário

Esta secção contém uma lista de termos referidos no documento e as suas respectivas configurações.

Kaspersky Lab ZAO

Esta secção fornece informação sobre a Kaspersky Lab.

Informação sobre código de terceiros

Esta secção fornece informação acerca da utilização de código de terceiros na aplicação.

Avisos de marcas comerciais

Esta secção indica as marcas comerciais propriedade de terceiros utilizadas no presente documento.

Índice

Esta secção permite-lhe encontrar rapidamente a informação necessária no documento.

CONVENÇÕES DE DOCUMENTOS

O presente texto é acompanhado por elementos semânticos aos quais deve prestar especial atenção – avisos, sugestões, exemplos.

As convenções de documentos são utilizadas para destacar os elementos semânticos. As convenções de documentos e os exemplos da sua utilização são apresentados na tabela seguinte.

Tabela 1.Convenções de documentos

TEXTO DE AMOSTRA	DESCRIÇÃO DAS CONVENÇÕES DO DOCUMENTO
	Os avisos são destacados a vermelho e são apresentados dentro de caixas.
Note que	Os avisos fornecem informações sobre possíveis acções não pretendidas que podem originar perda de dados, falhas na utilização do equipamento ou problemas no sistema operativo.
É	As notas aparecem dentro de caixas.
E recomendado utilizar	As notas podem conter sugestões úteis, recomendações, valores específicos para as configurações ou casos especiais importantes na utilização da aplicação.
Exemplo:	Os exemplos são apresentados num fundo amarelo e com o título "Exemplo".
Actualização significa	Os seguintes elementos semânticos aparecem em itálico no texto:
A ocorrência do evento Bases de	Novos termos
	 Nomes dos estados das aplicações e eventos
Clique no botão Activar .	Os nomes dos elementos da interface da aplicação, como os campos de registo, os itens de menu e os botões, aparecem a negrito.
 Para configurar um agendamento de tarefas: 	As frases introdutórias das instruções estão em itálico e assinaladas com uma seta.
<nome de="" utilizador=""></nome>	As variáveis são apresentadas entre parênteses angulares. É necessário substituir cada variável pelo valor correspondente, omitindo os parênteses angulares.
Envie uma mensagem SMS para o seu dispositivo com o texto seguinte: find: <código>.</código>	O tipo de letra diferente indica o texto do comando de SMS.

FONTES DE INFORMAÇÃO SOBRE A APLICAÇÃO

Esta secção descreve fontes de informação acerca da aplicação e apresenta uma lista de sites que pode utilizar para discutir o funcionamento da aplicação.

Pode seleccionar a fonte de informação mais adequada, dependendo do nível de importância e urgência da questão.

NESTA SECÇÃO

Fontes de informação para pesquisa independente	. <u>8</u>
Discutir as aplicações da Kaspersky Lab no Fórum	. <u>9</u>
Contactar o Departamento de Vendas	. <u>9</u>
Contactar o Departamento de Documentação Técnica e Localização por e-mail	. <u>9</u>

FONTES DE INFORMAÇÃO PARA PESQUISA INDEPENDENTE

Pode utilizar as seguintes fontes para encontrar informações acerca da aplicação:

- A página da aplicação no site da Kaspersky Lab
- A página da aplicação no site de Suporte Técnico (Base de Conhecimento)
- Ajuda online
- Documentação

Se não encontrar uma solução para o seu problema, recomendamos contactar o Suporte Técnico da Kaspersky Lab (consulte a secção "Suporte técnico por telefone" na página <u>46</u>).

É necessária uma ligação à Internet para utilizar as fontes de informação no site da Kaspersky Lab.

A página da aplicação no site da Kaspersky Lab

O site da Kaspersky Lab dispõe de uma página individual para cada aplicação.

Numa página desse tipo (<u>http://www.kaspersky.com/pt/android-security</u>), pode visualizar informações gerais acerca de uma aplicação, as suas funções e funcionalidades.

A página http://www.kaspersky.com/pt/ inclui um URL para a eLoja. Aqui pode adquirir ou renovar a aplicação.

A página da aplicação no Web site do Serviço de Apoio Técnico (Base de Dados de Conhecimento).

A Base de Conhecimento é uma secção do site do Suporte Técnico que fornece aconselhamento sobre a utilização das aplicações da Kaspersky Lab. A Base de Conhecimento inclui artigos de referência agrupados por tópicos.

Na página da aplicação na Base de Conhecimento (<u>http://support.kaspersky.com/mobile/kisandroid</u>), pode obter artigos que fornecem informações e recomendações úteis, assim como respostas para perguntas frequentes acerca de como adquirir, instalar e utilizar a aplicação.

Os artigos respondem a questões relacionadas não só com o Kaspersky Internet Security, mas também com outras aplicações da Kaspersky Lab. Podem também conter notícias do Serviço de Suporte Técnico.

Ajuda online

A ajuda online da aplicação é constituída por ficheiros de ajuda.

A ajuda de contexto contém dados sobre todas as janelas na aplicação: uma lista de configurações e respectivas descrições, bem como uma lista das tarefas a executar.

A ajuda completa contém informações detalhadas sobre como gerir a protecção, como configurar as definições da aplicação e como executar as tarefas básicas.

A Documentação instalada

O Manual do Utilizador descreve a interface da aplicação bem como as formas de executar tarefas comuns ao utilizar a aplicação.

DISCUTIR AS APLICAÇÕES DA KASPERSKY LAB NO Fórum

Se a sua questão não requer uma resposta imediata, pode discuti-la com os especialistas da Kaspersky Lab e com outros utilizadores no nosso fórum (<u>http://forum.kaspersky.com/index.php?showforum=86</u>).

Neste fórum, pode visualizar os tópicos existentes, deixar os seus comentários, criar novos tópicos.

CONTACTAR O DEPARTAMENTO DE VENDAS

Se tiver alguma questão sobre como seleccionar, adquirir ou renovar a aplicação, pode contactar os especialistas do nosso Departamento de Vendas através de uma das seguintes formas:

- Contactando os nossos escritórios (<u>http://www.kaspersky.com/pt/about/contactinfo</u>).
- Enviando as suas questões por e-mail para sales@kaspersky.com.

O serviço é fornecido em russo e em inglês.

Contactar o Departamento de Documentação Técnica e Localização por e-mail

Para contactar o Grupo de Desenvolvimento de Documentação, envie a sua mensagem para o endereço <u>docfeedback@kaspersky.com</u>. Utilize "Kaspersky Help Feedback: Kaspersky Internet Security for Android" como assunto da sua mensagem.

KASPERSKY INTERNET SECURITY

O Kaspersky Internet Security inclui as principais funcionalidades seguintes:

Protecção contra vírus e outro software malicioso

O dispositivo é protegido contra vírus e outro software malicioso pelo componente Scanner (Anti-Vírus).

O componente é denominado Scanner na versão gratuita e Anti-Virus na versão Premium.

O Scanner permite apenas verificar o dispositivo na totalidade, as aplicações instaladas, ou uma pasta específica, quando à presença de ameaças, configurar verificações agendadas do dispositivo, bem como actualizar as bases de dados de antivírus para manter actualizada a protecção dos seus dados.

O antivírus combina todas as funcionalidades do Scanner com as funcionalidades adicionais seguintes:

- Protecção do seu dispositivo em tempo real;
- Verifica as aplicações instaladas recentemente, antes de estas serem iniciadas pela primeira vez, utilizando as bases de dados de antivírus e o serviço cloud online da Kaspersky Security Network;
- Suporte de actualizações automáticas das bases de dados de antivírus.

Ocultar contactos confidenciais e histórico de chamadas relacionado e correspondência de SMS

O componente Protecção de Privacidade permite ocultar contactos confidenciais e informações relacionadas.

A Protecção de Privacidade está disponível apenas com a versão Premium do Kaspersky Internet Security em dispositivos com um cartão SIM inserido.

A Protecção de Privacidade permite ocultar temporariamente contactos confidenciais e todo o histórico de chamadas e mensagens SMS relacionadas. Pode ocultar contactos e informações relacionadas utilizando as configurações da aplicação ou remotamente com um comando de SMS especial.

Protecção de dados em caso de perda ou roubo do dispositivo

O componente Anti-Roubo protege os seus dados contra acessos não autorizados e ajuda a localizar o dispositivo em caso de furto ou extravio.

O componente Anti-Roubo permite activar remotamente o alarme do dispositivo, bloquear o dispositivo, determinar a sua localização, eliminar os dados do dispositivos e tirar uma fotografia de identificação da pessoa que actualmente utiliza o seu dispositivo. O Anti-Roubo permite-lhe iniciar remotamente as funções no dispositivo com comandos de SMS especiais ou a partir de Web Management em https://anti-theft.kaspersky.com. Para dispositivos com uma ranhura para cartão SIM, quando o cartão SIM é substituído ou o dispositivo é ligado sem um cartão SIM, o componente Anti-Roubo pode enviar o novo número de telefone do dispositivo numa mensagem SMS ou de e-mail, ou bloquear o dispositivo.

Bloquear a recepção de chamadas e mensagens de texto não solicitadas

O Filtro de Texto e Chamadas é utilizado para bloquear a recepção de chamada e mensagens de texto não solicitadas.

O componente Filtro de Texto e Chamadas está disponível apenas em dispositivos com um cartão SIM inserido.

Protecção contra as ameaças online

Os componentes Protecção de Internet e Anti-Phishing de Texto fornecem protecção contra ameaças online.

Os componentes Protecção de Internet e Anti-Phishing de Texto estão disponíveis apenas na versão Premium do Kaspersky Internet Security.

O componente Anti-Phishing de Texto está disponível apenas em dispositivos com um cartão SIM inserido.

A Protecção de Internet bloqueia sites maliciosos, que procuram distribuir código malicioso, e sites falsos (phishing), que procuram roubar os dados confidenciais do utilizador, e obter acesso às contas bancárias do utilizador.

O Anti-Phishing de Texto bloqueia as ligações em mensagens SMS para sites maliciosos ou falsos.

NESTA SECÇÃO

O que há de novo	<u>11</u>
Requisitos de hardware e software	<u>11</u>
Kit de distribuição	<u>12</u>
Serviços de utilizador	<u>12</u>

O QUE HÁ DE NOVO

O Kaspersky Internet Security fornece as seguintes funcionalidades novas:

- Possibilidade de excluir os programas do sistema da verificação.
- Interface de licenciamento melhorada.
- Suporte da plataforma Android x86.
- A funcionalidade de Protecção foi melhorada: a tecnologia de detecção de ameaças foi optimizada (análise heurística).
- A estabilidade da quarentena optimizada.

REQUISITOS DE HARDWARE E SOFTWARE

O dispositivo deve cumprir os requisitos seguintes para suportar o Kaspersky Internet Security:

- Smartphone ou tablet com uma resolução de ecrã de 320x480 píxeis ou superior.
- 65 MB de espaço de disco livre na memória principal do dispositivo.
- Versões 2.3.x a 4.4.x do sistema operativo Android™.
- Plataformas Intel Atom x86, ARM5, ARM6 ou ARM7.

A aplicação apenas pode ser instalada na memória principal do dispositivo.

O cartão SIM tem de estar inserido no dispositivo para utilizar o Filtro de Texto e Chamadas, Protecção de Privacidade, Prot. Cartão SIM e Anti-Phishing de Texto.

KIT DE DISTRIBUIÇÃO

Pode adquirir a aplicação através de uma das seguintes formas:

- Caixa. Vendida nas lojas dos nossos parceiros.
- Loja online. Distribuído nas lojas online da Kaspersky Lab (por exemplo, <u>http://www.kaspersky.com/pt/</u>, secção eLoja) ou empresas parceiras.
- através da Google Play Store . Carregado para o dispositivo através do serviço Google Play Store.

Se adquirir a aplicação numa caixa, o kit de distribuição inclui os seguintes componentes:

- envelope selado com um código QR para instalação da aplicação;
- guia rápido de instalação, que contém o código de activação da aplicação;
- contrato de licença que especifica os termos mediante os quais pode utilizar a aplicação.

O conteúdo do kit de distribuição pode variar consoante a região onde a aplicação foi adquirida.

Se adquirir o Kaspersky Internet Security numa loja online, estará a copiar a aplicação a partir do site da loja. As informações necessárias para activar a aplicação, incluindo o código de activação, ser-lhe-ão enviadas por e-mail após o pagamento.

Para obter mais detalhes sobre as formas de aquisição e o kit de distribuição, contacte o Departamento de Vendas sales@kaspersky.com.

SERVIÇOS DE UTILIZADOR

Ao adquirir uma licença de utilização da aplicação, poderá aceder aos seguinte serviços durante o prazo de validade da licença:

- actualização das bases de dados e disponibilização de novas versões da aplicação;
- aconselhamento por telefone e por e-mail acerca de questões relacionadas com a instalação, configuração e utilização da aplicação;
- As notificações acerca da existência de novas aplicações da Kaspersky Lab e de novos vírus e surtos de vírus.
 Para utilizar este serviço, subscreva o boletim de notícias da Kaspersky Lab no site do Serviço de Suporte Técnico.

Não são prestados serviços de aconselhamento acerca de questões relacionadas com o funcionamento de sistemas operativos, software e tecnologias de terceiros.

INSTALAR E DESINSTALAR A APLICAÇÃO

Esta secção contém instruções detalhadas para instalar e remover o Kaspersky Internet Security.

NESTA SECÇÃO

Instalar a aplicação	. <u>13</u>
Desinstalar a aplicação	.14

INSTALAR A APLICAÇÃO

O Kaspersky Internet Security for Android pode ser instalado a partir da Google Play Store ou a partir do pacote de distribuição da aplicação guardado no dispositivo.

Pode utilizar a Google Play Store para instalar o Kaspersky Internet Security a partir da aplicação da Google Play Store no seu dispositivo ou a partir do site <u>https://play.google.com</u> no seu computador.

É necessário que se verifiquem as condições seguintes para instalar a aplicação utilizando a Google Play Store:

- É necessário ter uma conta Google.
- O seu dispositivo tem de estar associado à sua conta Google.
- O seu dispositivo tem de estar ligado à Internet.

Para obter mais informações sobre como criar uma conta Google, associar o seu dispositivo à sua conta ou utilizar a Google Play Store, consulte o suporte o site de técnico da Google <u>http://support.google.com/googleplay/</u>.

Para instalar o Kaspersky Internet Security no seu dispositivo a partir da Google Play Store:

- 1. Inicie a aplicação do Google Play no seu dispositivo.
- 2. Localize o Kaspersky Internet Security. Para o fazer, introduza o nome da aplicação no campo de pesquisa do Google Play e toque em Introduzir.
- 3. Seleccione Kaspersky Internet Security nos resultados de pesquisa.

Abre a página com os detalhes do Kaspersky Internet Security.

- 4. Toque em Instalar na página com os detalhes da aplicação.
- 5. Consulte a lista de direitos de acesso requeridos pelo Kaspersky Internet Security. Se concorda em conceder estes direitos à aplicação, toque em Aceitar e transferir.

A transferência e instalação do Kaspersky Internet Security serão iniciadas.

6. Se recusar conceder estes direitos ao Kaspersky Password Manager, toque em Anterior.

Isto cancela a instalação da aplicação.

Para instalar o Kaspersky Internet Security a partir de <u>https://play.google.com</u> utilizando um computador, proceda do seguinte modo:

- 1. Abra o site <u>https://play.google.com</u> no computador.
- Localize o Kaspersky Internet Security. Para o fazer, introduza o nome da aplicação no campo de pesquisa do Google Play e toque em Introduzir.

3. Seleccione Kaspersky Internet Security nos resultados de pesquisa.

Abre a página com os detalhes do Kaspersky Internet Security.

4. Toque em Instalar na página com os detalhes da aplicação.

Se não tiver sessão iniciada no serviço Google Play, é apresentada uma janela para iniciar sessão na sua conta Google.

Se já tiver sessão iniciada no serviço Google Play, é apresentada uma janela com um formulário de pedido.

- 5. No menu pendente **Enviar para outro dispositivo** no formulário de pedido, seleccione o dispositivo onde pretende instalar a aplicação. A lista contém os dispositivos associados à sua conta Google.
- 6. Na janela do formulário de pedido, reveja a lista dos direitos requeridos pela aplicação. Se aceitar conceder estes direitos à aplicação, toque em **Instalar**.

Se o seus dispositivo estiver ligado a uma rede Wi-Fi ou 3G/4G, a transferência da aplicação é iniciada imediatamente. Se o seu dispositivo não estiver ligado à Internet, a transferência da aplicação é iniciada quando estabelecer ligação à Internet.

7. Se não pretender conceder estes direitos à aplicação, toque em Cancelar.

Isto cancela a instalação da aplicação.

- Para instalar o Kaspersky Internet Security for Android a partir do pacote de distribuição:
 - 1. Copie o pacote de distribuição da aplicação para o dispositivo. Efectue uma das seguintes acções:
 - Se o pacote de distribuição da aplicação foi transferido e guardado anteriormente num computador, ligue o dispositivo ao computador e copie o pacote de distribuição da aplicação para o dispositivo.
 - Transfira o pacote de distribuição da aplicação para o dispositivo a partir da eLoja da Kaspersky Lab (<u>http://www.kaspersky.com/pt/globalstore</u>) ou nas lojas online de empresas parceiras.
 - 2. Inicie a instalação da aplicação. Para tal, abra o arquivo APK no dispositivo.

O assistente de instalação da aplicação é iniciado. Quando o assistente estiver concluído, a aplicação é instalada com as definições recomendadas pelos especialistas da Kaspersky Lab.

DESINSTALAR A APLICAÇÃO

- Para desinstalar o Kaspersky Internet Security:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações >Definições adicionais > Desinstalar a aplicação**.
 - Se definiu um código secreto da aplicação, introduza-o (consulte a secção "Porque é necessário um código secreto" na página <u>27</u>).

Caso se esqueça do código secreto da aplicação, pode recuperá-lo (consulte a secção "Recuperar o código secreto da aplicação" na página <u>45</u>).

Se não definiu um código secreto, avance para o passo seguinte.

3. Confirme que a aplicação deve ser desinstalada.

A aplicação começa a ser desinstalada. Caso a ocultação de dados tenha sido activada, a mesma será automaticamente desactivada (consulte a secção "Protecção de Privacidade" na página <u>33</u>).

A Kaspersky Lab não recomenda desinstalar o Kaspersky Internet Security. Tal irá comprometer a segurança do seu dispositivo e dados pessoais.

INTERFACE DA APLICAÇÃO

Esta secção contém indicações sobre os principais elementos da interface gráfica da aplicação: janela principal, indicador do estado de protecção em forma de escudo, painel de início rápido, ícone da aplicação, widget e janelas de notificações.

NESTA SECÇÃO

Janela principal do Kaspersky Internet Security	<u>16</u>
Indicador do estado de protecção em forma de escudo	<u>17</u>
Painel de início rápido	<u>19</u>
cone na área de notificação	<u>20</u>
Widget do ecrã inicial do dispositivo	<u>20</u>
Notificações	<u>21</u>

JANELA PRINCIPAL DO KASPERSKY INTERNET SECURITY

A janela principal da aplicação (consulte a figura abaixo) contém os elementos da interface para aceder às funções principais da aplicação.



Figura 1. Janela principal

O aspecto da janela principal varia ligeiramente em resoluções de ecrã diferentes.

O número de botões no painel de início rápido pode variar conforme as funções disponíveis.

INDICADOR DO ESTADO DE PROTECÇÃO EM FORMA DE ESCUDO

O indicador do estado de protecção tem a forma de um escudo e encontra-se no centro da janela principal (consulte a imagem abaixo).



Figura 2. Escudo no centro da janela principal

A cor do escudo muda conforme o estado de protecção do dispositivo:

- Verde o dispositivo tem a protecção adequada. Todos os componentes de protecção funcionam de acordo com as configurações recomendadas pelos especialistas da Kaspersky Lab. As bases de dados do Kaspersky Internet Security estão actualizadas. Não foram detectados objectos maliciosos durante a verificação do dispositivo, ou todos os objectos detectados foram neutralizados pela aplicação.
- Amarelo o nível de protecção é inferior ao normal e existem alguns problemas no funcionamento do Kaspersky Internet Security. Por exemplo, o dispositivo não é verificado há mais de 14 dias ou foi instalada uma nova aplicação que ainda não foi verificada.
- Vermelho existem problemas que podem levar à infecção do dispositivo e à perda de dados. Por exemplo, determinados componentes de protecção foram colocados em pausa ou as bases de dados de antivírus não são actualizadas há mais de 14 dias.

Tocando no escudo na janela principal da aplicação, pode abrir a secção **Estado** (consulte a figura abaixo). A secção **Estado** apresenta o estado de segurança do dispositivo, uma lista de problemas e as soluções propostas.



Figura 3. Secção Estado

Os problemas relacionados com a protecção são agrupados por categorias. Para cada problema, estão listadas as acções que pode utilizar para resolver o problema.

Existem dois tipos de problemas de protecção:

- Notificações de problemas. Realçadas a amarelo. As notificações de problemas notificam o utilizador sobre eventos que podem potencialmente afectar a segurança do dispositivo (por exemplo, se a última verificação foi realizada há mais de 14 dias ou se uma aplicação nova ainda não foi verificada). Pode ocultar uma notificação de problema arrastando a mesma para a esquerda. Nesse caso, a informação sobre o problema pode ser consultada no menu Problemas ocultos.
- Problemas críticos. Realçadas a vermelho. As notificações críticas notificam o utilizador sobre eventos de importância crítica para a segurança do dispositivo (tais como a existência de uma nova versão da aplicação ou se as bases de dados de antivírus não forem actualizadas há bastante tempo). Um problema crítico não pode ser ocultado.

Funções dos botões do painel de início rápido

PAINEL DE INÍCIO RÁPIDO

O painel de início rápido fornece acesso rápido às funções principais da aplicação (consulte a figura abaixo).



Figura 4. Painel de início rápido

Tabela 2.

O painel de início rápido está minimizado por predefinição. Pode maximizar o painel de início rápido puxando-o ou tocando no botão .

O número de botões no painel de início rápido pode variar conforme as funções disponíveis.

O significado de cada botão do painel de início rápido é indicado na tabela abaixo.

Вотãо	Função
(Verificação)	Permite verificar todo o dispositivo, apenas as aplicações instaladas, uma pasta ou ficheiro seleccionado.
(Actualização)	Inicia a actualização das bases de dados de antivírus e da aplicação para garantir a protecção actualizada do dispositivo.
(Navegador)	Abre o navegador do Android padrão com a verificação de sites activada quanto a vírus e phishing.
(Protecção de Privacidade)	Oculta ou apresenta temporariamente os contactos confidenciais pré-seleccionados e as respectivas informações relacionadas.
(Filtro de Texto e Chamadas)	Abre a janela de selecção do modo Filtro de Texto e Chamadas.
(Anti-Theft Web Management)	Abre a Web Management para a gestão remota das funções de anti-roubo no dispositivo.

19

Вотãо	Função
(Configurações)	Abre a janela de configurações da aplicação.
(Ajuda)	Abre a ajuda da aplicação.

ÍCONE NA ÁREA DE NOTIFICAÇÃO

Após o assistente da primeira inicialização terminar, o ícone do Kaspersky Internet Security é apresentado na barra de estado.

O ícone reflecte o funcionamento da aplicação e fornece acesso à janela principal da aplicação.

Indicação de que a aplicação está em execução

O ícone indica que a aplicação está em execução. Na versão Premium, indica o estado de protecção do dispositivo:

- Karactivada;
- Mainto Marcella (icone preto e branco): a protecção está desactivada;
- Mais (ícone de cor com um ponto de exclamação): existem problemas de protecção. Por exemplo, as bases de dados de antivírus estão desactualizadas ou uma nova aplicação instalada não foi verificada.

Na versão gratuita da aplicação, o ícone não indica o estado de protecção do dispositivo.

Acesso à janela principal da aplicação

Pode abrir a janela principal da aplicação através do ícone da aplicação na área de notificação.

WIDGET DO ECRÃ INICIAL DO DISPOSITIVO

O Kaspersky Internet Security inclui o widget de ecrã inicial do dispositivo (consulte a figura abaixo).



Figura 5. Widget do ecrã inicial

O widget é utilizado para mudar para a janela principal da aplicação.

Na versão Premium da aplicação, a cor do widget do ecrã inicial indica o estado de protecção do seu dispositivo. Na versão Premium da aplicação, a cor do widget também pode indicar a existência de contactos confidenciais ocultos e de informações relacionadas, caso a função esteja activada nas opções do widget.

O widget utiliza os códigos de cor seguintes:

- um escudo verde indica que a Protecção está activada;
- um escudo cinzento indica que a Protecção está desactivada;
- um fundo de cor verde indica que a aplicação está a ocultar contactos confidenciais e informações relacionadas;
- um fundo de cor cinza indica que a aplicação está a apresentar os contactos confidenciais e as informações relacionadas.

Na versão gratuita da aplicação, a cor do widget não indica o estado de protecção do dispositivo.

NOTIFICAÇÕES

O Kaspersky Internet Security for Android notifica o utilizador acerca de eventos significativos que ocorram durante o processamento das operações, através de *janelas de notificação* e *notificações de pop-up*, apresentadas na barra de estado.

O Kaspersky Internet Security for Android apresenta *janelas de notificação* quando tem opções diferentes em resposta a um evento. Por exemplo, quando a aplicação detectar um objecto malicioso que não pode desinfectar, o utilizador pode eliminar o objecto, ignorá-lo ou consultar a Ajuda para obter informações sobre como processar o objecto (consulte a figura abaixo). A aplicação solicita ao utilizador que escolha uma acção. A janela de notificação apenas desaparece do ecrã depois de seleccionar uma das acções propostas.

K Ameaça detectada!		
Ameaça detectada: EICAR-Test- File		
Ficheiro: /mnt/sdcard/EICAR- STANDARD-ANTIVIRUS-TEST- FILE.txt		
Aplicar a todos		
Eliminar	Quarentena	
Ignorar		

Figura 6. Janelas de notificação

O Kaspersky Internet Security for Android apresenta *notificações de pop-up* na barra de estado para informar o utilizador sobre eventos que não necessitam da selecção de uma acção (consulte a fig. abaixo). É possível visualizar as notificações mais tarde, através da barra de notificações do dispositivo.



Figura 7. Notificações de pop-up

Conforme o nível de importância de um evento, as notificações são divididas em três tipos em termos de segurança do dispositivo:

- As notificações críticas informam o utilizador sobre eventos de importância prioritária para a segurança do dispositivo (por exemplo, a detecção de um ficheiro malicioso). As notificações críticas são realçadas a vermelho.
- As notificações importantes informam o utilizador sobre eventos potencialmente importantes para a segurança do dispositivo (por exemplo, o início de uma verificação ou actualização). As notificações importantes são realçadas a verde.
- As notificações informativas informam o utilizador sobre eventos de menor importância para a segurança do dispositivo. As notificações informativas não são realçadas.

LICENCIAR A APLICAÇÃO

Esta secção fornece informação acerca dos termos gerais relacionados com a activação da aplicação. Leia esta secção para saber mais sobre o objectivo do contrato de licença, as formas de activação da aplicação e a renovação da licença.

Nesta secção	
Acerca do Acordo de Licença de Utilizador Final	
Sobre a licença	
Sobre o código de activação	
Acerca do fornecimento de dados	

ACERCA DO ACORDO DE LICENÇA DE UTILIZADOR FINAL

O Acordo de Licença de Utilizador Final é um acordo vinculativo entre o utilizador e a Kaspersky Lab ZAO, que define os termos de utilização da aplicação.

Leia atentamente os termos do Contrato de Licença antes de começar a utilizar a aplicação.

Considera-se que aceitou os termos do Contrato de Licença quando confirmar que concorda com o texto do Contrato de Licença, ao instalar a aplicação. Se não aceitar os termos do Acordo de Licença de Utilizador Final, terá de interromper a instalação da aplicação e não utilizar a mesma.

SOBRE A LICENÇA

Licença- o direito de utilizar a aplicação, fornecido no âmbito do Contrato de Licença.

A licença concede-lhe o direito de beneficiar dos seguintes serviços:

• Utilizar a aplicação em um ou em vários dispositivos.

O número de dispositivos nos quais pode utilizar a aplicação é especificado nos termos do Acordo de Licença de Utilizador Final.

- Contactar o Serviço de Suporte Técnico da Kaspersky Lab.
- Outros serviços disponíveis junto da Kaspersky Lab ou dos seus parceiros durante o período de vigência da licença. (consulte a secção «Serviços para utilizadores registados» na página <u>12</u>).

O âmbito de serviços disponíveis e os termos de utilização da aplicação dependem da versão da aplicação.

Estão disponíveis as versões seguintes da aplicação:

- Versão gratuita. A versão gratuita oferece funcionalidades limitadas do Kaspersky Internet Security durante um período ilimitado. As limitações da versão gratuita estão descritas no Acordo de Licença. A versão gratuita fica disponível imediatamente após instalar a aplicação. Pode mudar para a versão gratuita ou para a versão Premium da aplicação a partir da versão de avaliação.
- Versão de avaliação. A versão de avaliação permite utilizar todas as funcionalidades da aplicação, gratuitamente, durante um período de avaliação.

Pode mudar para a versão Premium ou para a versão gratuita da aplicação a partir da versão de avaliação. Quando o período de avaliação termina, a aplicação muda automaticamente para a versão gratuita.

 Versão Premium. A versão Premium permite utilizar todas as funcionalidades da aplicação. A versão Premium está disponível para quem adquirir a licença da aplicação. A licença Premium é válida durante um período limitado.

Pode continuar a utilizar a aplicação após a licença expirar. Para tal, renove a licença Premium ou mude para a versão gratuita. Para renovar a licença, introduza um código de activação novo fornecido com o produto licenciado, ou adquira uma nova licença online.

Quando a licença expira, a aplicação muda automaticamente para a versão gratuita.

SOBRE O CÓDIGO DE ACTIVAÇÃO

O código de activação é o código recebido ao adquirir a licença Premium do Kaspersky Internet Security. O código é necessário para a activação da aplicação.

O código de activação é uma sequência exclusiva de 20 caracteres e números, no formato xxxxx-xxxxx-xxxxx.

Dependendo do método de aquisição da aplicação, estão disponíveis as seguintes opções para receber um código de activação:

- Se adquiriu a versão embalada do Kaspersky Internet Security, o código de activação é especificado na documentação incluída na caixa que contém o CD de instalação.
- Se adquiriu o Kaspersky Internet Security numa loja online, o código de activação é enviado para o endereço de e-mail que especificou ao encomendar o produto.

O prazo de validade da licença é calculado a partir da data em que a aplicação foi activada. Se adquiriu uma licença destinada à utilização do Kaspersky Internet Security em vários dispositivos, o período da licença tem início no momento em que aplica pela primeira vez o código de activação.

Se perdeu ou eliminou acidentalmente o seu código de activação após a activação, contacte o Serviço de Suporte Técnico da Kaspersky Lab.

ACERCA DO FORNECIMENTO DE DADOS

Para aumentar o nível de protecção, o Kaspersky Internet Security utiliza o serviço cloud da Kaspersky Security Network (consulte a secção "Kaspersky Security Network (KSN)" na página <u>48</u>) nas seguintes funcionalidades:

- Verificação. A aplicação verifica adicionalmente as aplicações instaladas antes do primeiro início. Esta verificação permite detectar novas ameaças que não foram adicionadas ou descritas nas bases de dados de antivírus.
- Protecção de Internet. A aplicação verifica adicionalmente os sites antes de os abrir.
- Anti-Phishing. de Texto. A aplicação bloqueia as ligações em mensagens SMS para sites maliciosos ou de phishing.

Para obter informações mais detalhadas acerca dos dados transferidos pela Kaspersky Lab quando utiliza o serviço cloud é utilizado nos dispositivos dos utilizadores, consulte o Contrato de Licença. Ao aceitar os termos e condições do Contrato de Licença, está a concordar em transferir as seguintes informações:

- informações acerca da soma de verificação dos ficheiros processados (MD5);
- informações necessárias para avaliar a reputação dos URLs;
- dados durante a activação do Kaspersky Internet Security e a versão actualmente em utilização;
- informações acerca dos resultados da actividade do verificador heurístico;
- informações acerca dos tipos de ameaças detectadas.

Todas as informações transferidas não incluem dados pessoais nem outras informações confidenciais do utilizador.

A Kaspersky Lab protege todas as informações recebidas do modo legalmente descrito. A Kaspersky Lab utiliza as informações recolhidas apenas para estatísticas gerais. As estatísticas gerais são automaticamente geradas utilizando as informações obtidas e não contêm dados pessoais ou outras informações confidenciais. As informações originais recolhidas são guardadas num formato encriptado; estas informações são eliminadas à medida que se recolhem (duas vezes por ano). As estatísticas gerais são guardadas indefinidamente.

INICIAR E PARAR A APLICAÇÃO

O Kaspersky Internet Security for Android é iniciado com o arranque do sistema operativo e protege o dispositivo ao longo de toda a sessão.

Pode parar a utilização da aplicação eliminando o Kaspersky Internet Security ou desactivando todos os componentes da aplicação.

A Kaspersky Lab não recomenda desactivar todos os componentes do Kaspersky Internet Security. Tal irá comprometer a segurança do seu dispositivo e dados pessoais.

GUIA RÁPIDO DE INSTALAÇÃO

Esta secção descreve como começar a utilizar a aplicação rapidamente após a instalação:

- Instruções para neutralizar um objecto malicioso
- Informações sobre como proteger os seus dados contra acesso não autorizado
- Instruções a seguir em caso de furto ou extravio do dispositivo.

NESTA SECÇÃO

Como proceder em caso de detecção de um objecto malicioso	<u>26</u>
Como proteger dados contra acessos não autorizados	<u>26</u>
O que fazer em caso de perda ou roubo do dispositivo	<u>28</u>

Como proceder em caso de detecção de um objecto malicioso

Se uma ameaça de segurança for detectada no arranque de uma aplicação (por exemplo, num jogo), o Kaspersky Internet Security solicita ao utilizador que seleccione uma acção a aplicar a essa aplicação. Pode seleccionar uma das seguintes acções:

- Quarentena: a aplicação é movida para a Quarentena.
- **Desinstalar**: a aplicação é eliminada.
- Ignorar: não é aplicada qualquer acção à aplicação.

A Kaspersky Lab recomenda neutralizar as ameaças à medida que são detectadas.

Se um objecto malicioso for detectado durante uma verificação de ficheiros, o Kaspersky Internet Security for Android move o mesmo para a Quarentena, por predefinição, e notifica o utilizador de que uma ameaça foi neutralizada.

Pode ver informações sobre os objectos maliciosos detectados nas secções Estado e Relatórios.

Como proteger dados contra acessos não autorizados

O Kaspersky Internet Security for Android protege os seus dados privados contra acesso não autorizado utilizando os métodos de protecção seguintes:

- Especificar um código secreto que impede o acesso não autorizado às definições da Protecção de Privacidade e Anti-Roubo
- Configurar Definições de Anti-Roubo

O componente Anti-Roubo é controlado por comandos de SMS e comandos enviados a partir da Web Management em https://anti-theft.kaspersky.com. Para controlar as funções de Anti-Roubo a partir da Web Management é necessário criar uma conta em Web Management.

Para proteger os seus dados contra acessos não autorizados, pode criar uma conta em Web Management para controlar o componente Anti-Roubo, especificar um código secreto para restringir o acesso às configurações da aplicação e configurar o dispositivo correctamente.

NESTA SECÇÃO

Finalidade do código secreto	<u>27</u>
O que é uma Conta Kaspersky	<u>27</u>
Efectuar a configuração inicial do Anti-Roubo	27

FINALIDADE DO CÓDIGO SECRETO

O código secreto é pedido nas seguintes situações:

- Para aceder às configurações de Anti-Roubo e Protecção de Privacidade
- Ao enviar um comando de SMS de outro dispositivo móvel para remotamente activar o alarme do dispositivo, bloquear o dispositivo, localizá-lo no mapa, eliminar dados ou ocultar contactos confidenciais e as informações relacionadas

Será solicitado que especifique o código secreto durante a configuração inicial do Anti-Roubo (consulte a secção "Efectuar a configuração inicial do Anti-Roubo" na página <u>27</u>) ou quando iniciar a Protecção de Privacidade pela primeira vez. Pode alterar o código secreto instalado mais tarde.

O código secreto é constituído por números. O número mínimo de caracteres do código secreto é quatro.

Caso se esqueça do código secreto da aplicação, pode restaurá-lo (consulte a secção "Recuperar o código secreto da aplicação" na página <u>45</u>).

O QUE É UMA CONTA KASPERSKY

Uma conta permite-lhe utilizar a Web Management em <u>https://anti-theft.kaspersky.com</u> para activar remotamente o alarme no dispositivo, bloquear o dispositivo, localizá-lo num mapa, eliminar dados ou secretamente tirar uma fotografia de identificação da pessoa que está actualmente a utilizar o dispositivo. Também pode utilizar a Web Management para recuperar um código secreto esquecido do Kaspersky Internet Security.

A Conta Kaspersky é uma conta única para aceder a todos os serviços da Kaspersky Lab. Se efectuou o registo com A Minha Conta ou se possui uma conta Web Management <u>https://center.kaspersky.com</u>, significa que tem uma Conta Kaspersky.

É necessário especificar a conta durante a configuração inicial do Anti-Roubo (consulte a secção"Efectuar a configuração inicial do Anti-Roubo" na página <u>27</u>). O endereço de e-mail funciona como nome de utilizador. Se não se lembrar da password da conta ao iniciar sessão em Web Management, pode restaurar a password.

EFECTUAR A CONFIGURAÇÃO INICIAL DO ANTI-ROUBO

As funções do componente Anti-Roubo estão desactivadas por predefinição quando a aplicação é instalada: não é possível iniciar as funções remotamente através de Web Management ou comandos de SMS. Para activar as funções de Anti-Roubo, é necessário efectuar a configuração inicial do Anti-Roubo.

Após a configuração inicial, todas as funções de Anti-Roubo serão activadas com as configurações recomendadas pelos especialistas da Kaspersky Lab.

O assistente de configuração inicial do Anti-Roubo pode ser iniciado apenas uma vez. Pode configurar o Anti-Roubo mais tarde nas definições da aplicação.

Para efectuar a configuração inicial do Anti-Roubo:

1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Anti-Roubo.

O assistente de configuração do Anti-Roubo é iniciado.

- 2. Siga as instruções do assistente.
- Para editar as definições de Anti-Roubo após a configuração inicial:

No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações > Anti-Roubo**.

O QUE FAZER EM CASO DE PERDA OU ROUBO DO DISPOSITIVO

Em caso de furto ou extravio do dispositivo, pode remotamente ocultar os contactos e informações relacionadas, bem como iniciar as funcionalidades de Anti-Roubo: activar o alarme, bloquear o dispositivo, remover dados armazenados no mesmo, obter a respectiva localização no mapa, ou secretamente obter a fotografia de identificação da pessoa que está a utilizar o seu dispositivo.

Pode activar o Anti-Roubo remotamente através de Web Management em <u>https://anti-theft.kaspersky.com</u> ou utilizando comandos de SMS especiais, enviados a partir de qualquer dispositivo.

Apenas pode ocultar remotamente os contactos e informações relacionadas utilizando um comando de SMS especial.

Pode ocultar os contactos e as informações relacionadas apenas se a versão Premium do Kaspersky Internet Security for Android estiver activada no seu dispositivo.

O comando para obter a fotografia de identificação da pessoa que está a utilizar o seu dispositivo só pode ser enviado através de Web Management em https://anti-theft.kaspersky.com. Este comando não pode ser enviado através de SMS.

A mensagem SMS enviada é cobrada de acordo com o tarifário do operador da rede móvel do dispositivo utilizado para enviar o comando de SMS.

O início remoto das funções Anti-Roubo no dispositivo é possível quando se verificam as condições seguintes:

- O Kaspersky Internet Security tiver sido definido como o Administrador do Dispositivo;
- O dispositivo detecta um sinal de rede móvel;
- As funções de Anti-Roubo e Protecção de Privacidade são permitidas no dispositivo.
- Para iniciar remotamente o Anti-Roubo através de Web Management:
 - 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
 - Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
 - 3. Seleccione o dispositivo para o qual pretende poder iniciar remotamente a função Anti-Roubo.

- 4. Nas secções na área superior da janela de Web Management, seleccione as acções a executar no dispositivo.
- Para ocultar informações de contactos remotamente e iniciar as funções de Anti-Roubo utilizando comandos de SMS, execute uma das acções seguintes:
 - Se o Kaspersky Internet Security estiver instalado noutro dispositivo, utilize o mesmo para criar e enviar um comando de SMS para o seu dispositivo (consulte a secção "Enviar comandos de SMS do Kaspersky Internet Security" na página <u>35</u>).

Ao criar um comando de SMS, utilize o código secreto do Kaspersky Internet Security instalado no seu dispositivo.

- Envie uma mensagem SMS para o seu dispositivo com o texto especial seguinte:
 - hide: <código> para ocultar contactos confidenciais e informações relacionadas;
 - alarm: <código> código para activar o alarme e bloquear o dispositivo (em que <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo);
 - find: <código> para bloquear o dispositivo e obter as suas coordenadas;
 - wipe: <código> para eliminar dados pessoais e dados do cartão de memória;
 - fullreset: <código> para eliminar todos os dados do dispositivo e reverter o dispositivo para as predefinições.

Depois de todos os dados terem sido removidos e o dispositivo reposto com as predefinições, não será possível receber e executar comandos remotos.

PROCESSAR TAREFAS PADRÃO

Esta secção contém instruções passo a passo sobre como executar as tarefas de utilizador básicas associadas à aplicação.

NESTA SECÇÃO

Scanner (Antivírus)	<u>30</u>
Protecção de Privacidade	<u>33</u>
Anti-Roubo	<u>34</u>
Filtro de Texto e Chamadas	<u>40</u>
Protecção de Internet e Anti-Phishing de Texto	<u>41</u>
Outras tarefas	<u>42</u>

SCANNER (ANTIVÍRUS)

O componente é denominado Scanner na versão gratuita e Anti-Virus na versão Premium.

O Scanner (Antivírus) foi concebido para verificar o dispositivo, detectar e neutralizar ameaças. O Kaspersky Internet Security for Android permite uma verificação total ou parcial do dispositivo incluído, isto é, verifica o conteúdo da memória incorporada do dispositivo ou de uma pasta específica (incluindo uma pasta localizada no cartão de memória).

A aplicação verifica o dispositivo quanto a objectos maliciosos utilizando a base de dados de antivírus da aplicação com descrições de todas as aplicações maliciosas identificadas e outros objectos maliciosos e formas de os neutralizar. É recomendado actualizar regularmente as bases de dados da aplicação.

O Kaspersky Internet Security actualiza as bases de dados antivírus da aplicação a partir dos servidores de actualização da Kaspersky Lab. Tratam-se de sites da Internet especiais que contêm actualizações para bases de dados de todos os produtos da Kaspersky Lab.

Para actualizar as bases de dados de antivírus da aplicação, é necessário ter uma ligação à Internet configurada no seu dispositivo. O tráfego da actualização das bases de dados de antivírus é facturado de acordo com o seu tarifário

NESTA SECÇÃO

Verificação completa do dispositivo	<u>31</u>
Verificação rápida	<u>31</u>
Verificação de ficheiros e pastas	<u>31</u>
Verificação agendada automática	<u>31</u>
Actualizações da base de dados de antivírus e da versão	<u>32</u>
Actualizações agendadas automáticas	<u>32</u>

VERIFICAÇÃO COMPLETA DO DISPOSITIVO

Uma verificação completa da presença de vírus e outro software malicioso em todo o dispositivo ajuda a proteger os seus dados pessoais e o seu dinheiro, bem como a detectar e a eliminar ameaças no dispositivo (nas aplicações instaladas e não instaladas).

A maior parte do software malicioso ameaça os dados pessoais do utilizador existentes no dispositivo: recolhe os dados pessoais do proprietário do dispositivo e todas as informações existentes no mesmo (por exemplo, coordenadas de GPS e mensagens) e envia estes dados para um utilizador mal intencionado.

É recomendado verificar a existência de vírus em todo o sistema de ficheiros do dispositivo pelo menos uma vez depois de instalar a aplicação, para assegurar a protecção dos dados pessoais.

Para verificar a existência de vírus e outro software malicioso em todo o sistema de ficheiros:

No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Verificação > Verificação completa.

VERIFICAÇÃO RÁPIDA

Pode ser efectuada uma verificação rápida para verificar apenas as aplicações instaladas.

Se estiver a utilizar a versão gratuita, a Kaspersky Lab recomenda efectuar uma verificação rápida assim que instalar novas aplicações.

Para executar uma verificação rápida,

no painel de início rápido na janela principal do Kaspersky Internet Security, toque em Verificação > Verificação rápida.

VERIFICAÇÃO DE FICHEIROS E PASTAS

Para verificar um ficheiro ou pasta na memória interna do dispositivo ou no cartão de memória.

- Para verificar uma pasta ou ficheiro:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Verificação > Verificação de pasta.
 - 2. Seleccione uma pasta ou ficheiro para verificar.

Verificação agendada automática

É possível configurar a inicialização automática de uma verificação completa do dispositivo e criar um agendamento para a respectiva execução, seleccionar a frequência da verificação, bem como o dia e a hora da execução, se necessário. A aplicação verifica automaticamente a totalidade do sistema de ficheiros do dispositivo, de acordo com o agendamento.

Para que uma verificação completa seja executada automaticamente, o dispositivo tem de estar ligado.

Para configurar o início automático de uma verificação agendada:

- No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Antivírus > Definições de verificação.
- 2. Configure a frequência da verificação. Para tal, seleccione um valor para a configuração Agendamento.

3. Defina o dia e a hora para o início da verificação. Para o fazer, seleccione os valores para as definições **Dia de** início e Hora de início.

As verificações serão iniciadas conforme o agendamento.

ACTUALIZAR AS BASES DE DADOS DE ANTIVÍRUS E A VERSÃO DA APLICAÇÃO

O Kaspersky Internet Security utiliza as bases de dados de antivírus para pesquisar software malicioso. As bases de dados de antivírus da aplicação contêm descrições de todos os softwares maliciosos actualmente conhecidos pela Kaspersky Lab e métodos para neutralizar os mesmos, bem como descrições de outros objectos maliciosos. É recomendado actualizar regularmente as bases de dados.

Para além das bases de dados de antivírus, o Kaspersky Internet Security permite actualizar a versão da aplicação. As actualizações da versão da aplicação removem vulnerabilidades do Kaspersky Internet Security e adicionam novas funções ou melhoram as funções existentes.

Para actualizar as bases de dados de antivírus da aplicação, é necessário ter uma ligação à Internet configurada no seu dispositivo.

Se fizer o download do Kaspersky Internet Security através do Google Play, a aplicação apenas actualizará as bases de dados de antivírus. A versão da aplicação é actualizada através do Google Play.

Actualizar as bases de dados de antivírus e a versão

No painel de início rápido na janela principal do Kaspersky Internet Security toque em Actualização.

ACTUALIZAÇÕES AGENDADAS AUTOMÁTICAS

Pode configurar as actualizações automáticas da versão da aplicação e das bases de dados de antivírus (doravante "actualização"). Para tal, crie um agendamento para a inicialização: seleccione a frequência, bem como o dia e a hora, se necessário. A aplicação irá actualizar automaticamente as bases de dados de antivírus e a versão, de acordo com o agendamento.

As actualizações automáticas estão disponíveis apenas na versão Premium do Kaspersky Internet Security.

É necessária uma ligação à Internet para efectuar as actualizações.

Para actualizar automaticamente à hora seleccionada, é necessário que o dispositivo esteja ligado a essa hora.

Para configurar uma actualização automática agendada:

- No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Antivírus > Actualização.
- 2. Configure a frequência das actualizações. Para tal, seleccione um valor para a configuração Agendamento.
- 3. Seleccione um dia e uma hora para iniciar as actualizações. Para o fazer, seleccione os valores para as definições **Dia de início** e **Hora de início**.

As actualizações serão iniciadas conforme o agendamento.

PROTECÇÃO DE PRIVACIDADE

Pode ocultar os seus contactos confidenciais e todo o histórico de chamadas relacionadas e correspondência de mensagens SMS utilizando o componente Protecção de Privacidade.

A Protecção de Privacidade está disponível apenas com a versão Premium do Kaspersky Internet Security em dispositivos com um cartão SIM inserido.

A Protecção de Privacidade suporta as funções seguintes:

- Mantém uma lista dos contactos confidenciais, incluindo os contactos a ocultar;
- Oculta entradas da lista de contactos, as mensagens de texto recebidas lidas, as mensagens de texto enviadas e os rascunhos de mensagens de texto, bem como as informações de contactos em registos telefónicos;
- Bloqueia os sinais de notificação de SMS e chamadas recebidas de números privados (neste caso, o número chamador ouve o sinal de "ocupado")

Para ver as chamadas e as mensagens de texto recebidas correspondentes a um período em que a Protecção de Privacidade estive activada, a Protecção de Privacidade deve ser desactivada. Se voltar a activar a Protecção de Privacidade, as informações confidenciais são novamente ocultadas.

Pode activar a Protecção de Privacidade a partir da aplicação ou remotamente, enviando um comando de SMS a partir de outro dispositivo móvel.

Pode enviar uma mensagem SMS padrão com um código especial ou enviar uma mensagem SMS a partir do Kaspersky Internet Security, se a aplicação estiver instalada no outro dispositivo.

Pode activar ou bloquear o início remoto da Protecção de Privacidade no seu dispositivo. Se o início remoto da Protecção de Privacidade estiver bloqueado, não é possível iniciar a função remotamente utilizando um comando de SMS.

Pode desactivar a Protecção de Privacidade apenas na aplicação instalada no dispositivo.

O acesso às definições da Protecção de Privacidade está protegido com um código secreto (consulte a secção "Finalidade do código secreto" na página <u>27</u>). O código secreto é especificado durante a configuração inicial do componente Anti-Roubo (consulte a secção "Efectuar a configuração inicial do Anti-Roubo" na página <u>27</u>) ou quando a Protecção de Privacidade é iniciada pela primeira vez.

NESTA SECÇÃO

Ocultar informações relacionadas com contactos
Iniciar remotamente a Protecção de Privacidade a partir de outro dispositivo

OCULTAR INFORMAÇÕES RELACIONADAS COM CONTACTOS

- Para ocultar contactos e informações relacionadas:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Protecção de Privacidade**.
 - 2. Toque em Contactos a ocultar.
 - 3. Introduza o código secreto.

Caso se esqueça do código secreto da aplicação, pode recuperá-lo (consulte a secção "Recuperar o código secreto da aplicação" na página <u>45</u>).

4. Para criar uma lista de contactos a ocultar, toque em Adicionar.

A lista contém os contactos cujos detalhes pretende ocultar. Ignore este passo se já criou uma lista de contactos.

5. Mude o botão Protecção de Privacidade para ligado.

INICIAR REMOTAMENTE A PROTECÇÃO DE PRIVACIDADE A PARTIR DE OUTRO DISPOSITIVO

Se necessário, pode ocultar contactos e informações relacionadas no dispositivo remotamente. Para tal, pode enviar um comando de SMS especial a partir de outro dispositivo.

O início remoto das funções de Protecção de Privacidade é possível caso se verifiquem as condições seguintes:

- A versão Premium da aplicação é activada no dispositivo que recebe o comando de SMS;
- O dispositivo detecta um sinal de rede móvel;
- O início remoto da Protecção de Privacidade é permitido no dispositivo.
- Para iniciar a Protecção de Privacidade no seu dispositivo remotamente, execute uma das operações seguintes:
 - Crie um comando noutro dispositivo e envie-o para o seu dispositivo a partir do Kaspersky Internet Security utilizando a função de comando de SMS (se a aplicação estiver instalada noutro dispositivo).
 - Noutro dispositivo, crie e envie uma mensagem SMS com o texto hide:<código>, em que
 <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo.

Irá receber um relatório de execução de comandos na mensagem SMS recebida.

Os comandos de SMS enviados são cobrados de acordo com o tarifário do operador móvel.

ANTI-ROUBO

O Anti-Roubo protege os seus dados contra acessos não autorizados e ajuda a localizar o dispositivo em caso de furto ou extravio.

Pode utilizar o Web Management ou comandos de SMS especiais para efectuar as seguintes operações remotamente:

- Bloquear o dispositivo e determinar a sua localização
- Activar um alarme sonoro no dispositivo
- Eliminar dados do dispositivo
- Tirar uma fotografia de identificação da pessoa que está actualmente a utilizar o dispositivo

Se o cartão SIM for substituído ou se o dispositivo for ligado sem um cartão SIM, pode bloquear o dispositivo remotamente e obter o novo número de telefone. Desta forma, é possível iniciar outras funções de Anti-Roubo no dispositivo extraviado.

NESTA SECÇÃO

Adicionar um dispositivo à conta de Web Management	. <u>35</u>
Enviar comandos de SMS do Kaspersky Internet Security	. <u>35</u>
Controlar o cartão SIM remotamente	. <u>36</u>
Bloquear e Localizar o dispositivo remotamente	. <u>36</u>
Activar o alarme do dispositivo remotamente	. <u>37</u>
Limpar dados do dispositivo remotamente	. <u>38</u>
Tirar uma fotografia de identificação com o dispositivo remotamente	. 39

Adicionar um dispositivo à conta de Web Management

Pode gerir vários dispositivos ao mesmo tempo, através da Conta Kaspersky na Web Management em <u>https://anti-theft.kaspersky.com</u>.

Para adicionar um dispositivo à sua conta de utilizador, introduza os detalhes da mesma, durante a configuração inicial do Kaspersky Internet Security no novo dispositivo.

O novo dispositivo é automaticamente associado à sua conta e está disponível através do Web Management.

ENVIAR COMANDOS DE SMS DO KASPERSKY INTERNET SECURITY

Em caso de furto ou extravio do dispositivo, pode iniciar remotamente as funções de Anti-Roubo ou Protecção de Privacidade no dispositivo. Para tal, envie comandos especiais para o seu dispositivo através da Web Management em https://anti-theft.kaspersky.com ou por SMS.

Pode enviar um comando de SMS padrão com um código especial a partir de outro dispositivo para o seu dispositivo (consulte a secção "O que fazer em caso de perda ou roubo do dispositivo" na página <u>28</u>). Se o Kaspersky Internet Security estiver instalado no outro dispositivo, pode enviar um comando de SMS a partir da aplicação. Para enviar um comando de SMS, é necessário o código secreto do Kaspersky Internet Security no seu dispositivo.

Os comandos de SMS enviados são cobrados de acordo com o tarifário do operador móvel.

- Para iniciar remotamente as funções de Anti-Roubo e Protecção de Privacidade a partir de um dispositivo com o Kaspersky Internet Security instalado:
 - 1. Abra o Kaspersky Internet Security no outro dispositivo.
 - No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Anti-Roubo.
 - 3. Introduza o código secreto.

Caso se esqueça do código secreto da aplicação, pode recuperá-lo (consulte a secção "Recuperar o código secreto da aplicação" na página <u>45</u>).

- 4. Toque em Enviar comandos de SMS.
- 5. Toque em **Enviar comando de SMS agora**, crie o comando e envie o mesmo para o seu dispositivo. Ao criar um comando de SMS, utilize o código secreto do Kaspersky Internet Security instalado no seu dispositivo.

Irá receber um relatório de execução de comandos na mensagem SMS recebida.

CONTROLAR O CARTÃO SIM REMOTAMENTE

Se o cartão SIM for substituído ou se o dispositivo for ligado sem um cartão SIM, pode bloquear o dispositivo remotamente e obter o novo número de telefone. Desta forma, é possível iniciar outras funções de Anti-Roubo no dispositivo extraviado.

Pode obter o novo número de telefone por SMS ou e-mail. Se esta função estiver activada, a aplicação bloqueia automaticamente o dispositivo extraviado quando este é ligado sem um cartão SIM. Quando o cartão SIM é substituído, a aplicação envia automaticamente uma mensagem por SMS e e-mail com o novo número de telefone para o número de telefone e endereço de e-mail especificados.

Para enviar uma mensagem de e-mail, a aplicação envia uma mensagem SMS para o número dedicado do operador MTS (Rússia). O operador MTS (Rússia) envia o número de telefone novo para o seu endereço de e-mail. A conta de telemóvel associada ao novo cartão de SMS instalado é utilizada para cobrar a mensagem SMS enviada para o número dedicado.

- Para activar Prot. Cartão SIM, execute previamente as operações seguintes:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações > Anti-Roubo**.
 - 2. Introduza o código secreto.
 - Caso se esqueça do código secreto da aplicação, pode recuperá-lo (consulte a secção "Recuperar o código secreto da aplicação" na página <u>45</u>).
 - 4. Seleccione Prot. Cartão SIM.
 - 5. Seleccione a caixa de verificação Prot. Cartão SIM.
 - Na secção Formas de receber o novo número de telefone e a localização do dispositivo, preencha o campo N.º de telefone e Endereço de e-mail para receber o novo número de telefone por mensagem SMS ou por e-mail se o seu cartão SIM for substituído.
 - Na secção Bloqueio do Dispositivo seleccione a caixa de verificação Bloquear quando o cartão SIM é substituído para que a aplicação bloqueie o dispositivo quando seu cartão SIM é substituído ou se o dispositivo for ligado sem o cartão.
 - 8. Se necessário, na secção **Texto quando bloqueado** introduza a mensagem que pretende apresentar no ecrã do dispositivo bloqueado.

BLOQUEAR E LOCALIZAR O DISPOSITIVO REMOTAMENTE

Se o seu dispositivo se extraviar ou for furtado, pode bloquear o dispositivo e obter as coordenadas da sua localização através de Web Management em https://anti-theft.kaspersky.com ou do comando de SMS "find: <código> (em que <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo).

Os comandos de SMS enviados são cobrados de acordo com o tarifário do operador móvel.

Um dispositivo pode ser bloqueado e localizado remotamente quando se verificam as condições seguintes:

- O Kaspersky Internet Security for Android tiver sido instalado como o Administrador do Dispositivo;
- O dispositivo detecta um sinal de rede móvel;
- o início desta função é permitido no dispositivo.

A Kaspersky Lab também recomenda a activação do GPS nas definições do dispositivo, para que a aplicação possa determinar a localização do dispositivo através de GPS.

- Para bloquear o dispositivo e obter as suas coordenadas através de Web Management:
 - 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
 - 2. Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
 - 3. Seleccione o dispositivo que pretende bloquear e localizar.
 - 4. Toque no botão Bloquear e Localizar.
 - 5. Se necessário, em **Bloquear e Localizar** introduza o texto que pretende apresentar no ecrã do dispositivo bloqueado. Introduza também o endereço de e-mail onde pretende receber as coordenadas do dispositivo no mapa.
 - 6. Toque no botão Bloquear e Localizar.

Quando o Kaspersky Internet Security for Android localizar o dispositivo, poderá visualizar as suas coordenadas em Web Management e recebê-las na caixa de correio.

Em Web Management, apenas é possível visualizar a localização do dispositivo no mapa detectada mais recentemente. As coordenas de GPS anteriores do dispositivo permanecem na caixa de correio e são removidas de Web Management.

- Para bloquear o dispositivo e obter as suas coordenadas utilizando um comando de SMS, execute um dos procedimentos seguintes:
 - Se o Kaspersky Internet Security estiver instalado noutro dispositivo, utilize o mesmo para criar e enviar um comando de SMS para o seu dispositivo (consulte a secção "Enviar comandos de SMS do Kaspersky Internet Security" na página <u>35</u>). Ao criar um comando de SMS, utilize o código secreto do Kaspersky Internet Security instalado no seu dispositivo.
 - Envie uma mensagem SMS para o seu dispositivo com o texto seguinte: find: <código>, em que
 <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo.

Quando o Kaspersky Internet Security for Android localiza o seu dispositivo, irá obter as suas coordenadas na mensagem SMS de resposta e na mensagem de e-mail enviada para o endereço especificado.

ACTIVAR O ALARME DO DISPOSITIVO REMOTAMENTE

Em caso de furto ou extravio do seu dispositivo, pode activar o alarme do dispositivo remotamente (mesmo que o dispositivo esteja sem som) e bloquear o dispositivo através de Web Management em https://anti-theft.kaspersky.com ou do comando de SMS "alarm: <código> (em que <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo).

Os comandos de SMS enviados são cobrados de acordo com o tarifário do operador móvel.

O início remoto do Alarme é possível se o dispositivo captar um sinal de rede móvel e o início remoto desta função estiver activado no dispositivo.

- Para activar o alarme no dispositivo e bloquear o dispositivo através de Web Management:
 - 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
 - Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
 - 3. Seleccione o dispositivo onde pretende activar o alarme e que pretende bloquear.

- 4. Toque no botão Alarme.
- 5. Se necessário, na secção Alarme introduza o texto que pretende apresentar no ecrã do dispositivo bloqueado.
- 6. Toque no botão Activar Alarme.
- Para activar o alarme do dispositivo e bloquear o dispositivo utilizando um comando de SMS, execute um dos procedimentos seguintes:
 - Se o Kaspersky Internet Security estiver instalado noutro dispositivo, utilize o mesmo para criar e enviar um comando de SMS para o seu dispositivo (consulte a secção "Enviar comandos de SMS do Kaspersky Internet Security" na página <u>35</u>). Ao criar um comando de SMS, utilize o código secreto do Kaspersky Internet Security instalado no seu dispositivo.
 - Envie uma mensagem SMS para o seu dispositivo com o texto seguinte: alarm: <código>, em que
 <código> corresponde ao código secreto do Kaspersky Internet Security no seu dispositivo.

Irá receber um relatório de execução de comandos na mensagem SMS recebida.

LIMPAR DADOS DO DISPOSITIVO REMOTAMENTE

Em caso de furto ou extravio do seu dispositivo, pode eliminar os dados do mesmo remotamente através da Web Management no endereço <u>https://anti-theft.kaspersky.com</u> ou através de comandos de SMS.

Pode eliminar as seguintes informações:

- dados pessoais (por exemplo, contactos, mensagens e dados da conta Google™) e dados do cartão de memória;
- todos os dados, incluindo dados do cartão de memória (repondo as predefinições do dispositivo).

Os comandos de SMS enviados são cobrados de acordo com o tarifário do operador móvel.

É possível eliminar os dados remotamente caso se verifiquem as condições seguintes:

- O Kaspersky Internet Security for Android tiver sido instalado como o Administrador do Dispositivo;
- O dispositivo detecta um sinal de rede móvel;
- o início desta função é permitido no dispositivo.

Para eliminar remotamente dados do dispositivo através de Web Management:

- 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
- 2. Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
- 3. Seleccione o dispositivo de onde pretende eliminar dados.
- 4. Toque no botão Limpeza de Dados.
- 5. Na secção Limpeza de Dados, seleccione os dados que pretende eliminar do dispositivo.
 - Para eliminar dados pessoais (por exemplo, dados da conta Google, contactos e mensagens) e formatar o cartão de memória, seleccione Apenas dados pessoais.
 - Para eliminar todos os dados, incluindo dados no cartão de memória, e reverter o dispositivo para as predefinições, seleccione **Todos os dados do seu dispositivo**.

Depois de todos os dados terem sido eliminados do dispositivo, o Kaspersky Internet Security for Android também é removido. O dispositivo já não poderá executar comandos remotos.

- 6. Prima o botão Limpar.
- Para eliminar dados do dispositivo remotamente utilizando um comando de SMS, execute um dos seguintes procedimentos:
 - Se o Kaspersky Internet Security estiver instalado noutro dispositivo, utilize o mesmo para criar e enviar um comando de SMS para o seu dispositivo (consulte a secção "Enviar comandos de SMS do Kaspersky Internet Security" na página <u>35</u>). Pode optar por eliminar dados pessoais ou todos os dados. Ao criar um comando de SMS, utilize o código secreto do Kaspersky Internet Security instalado no seu dispositivo.
 - Envie uma mensagem SMS para o seu dispositivo com o texto especial seguinte:
 - wipe: <código> –para eliminar dados pessoais e dados armazenados no cartão de memória;
 - fullreset: <código> para eliminar todos os dados do dispositivo e repor o dispositivo com as predefinições.

<código> – o código secreto do Kaspersky Internet Security no dispositivo.

Irá receber um relatório de execução de comandos na mensagem SMS recebida.

TIRAR UMA FOTOGRAFIA DE IDENTIFICAÇÃO

Em caso de furto ou extravio do seu dispositivo, pode tirar uma fotografia de identificação da pessoa que está actualmente a utilizar o seu dispositivo e bloquear o dispositivo através de Web Management em <u>https://anti-theft.kaspersky.com</u>.

A função de fotografia de identificação é suportada se o seu dispositivo incluir uma câmara anterior. Esta função só pode ser iniciada a partir de Web Management. Não pode ser iniciada por comando de SMS.

O início remoto das funções de Anti-Roubo é possível caso se verifiquem as condições seguintes:

- O Kaspersky Internet Security tiver sido definido como o Administrador do Dispositivo;
- O dispositivo detecta um sinal de rede móvel;
- o início remoto desta função é permitido no dispositivo.

Para obter uma fotografia da pessoa que está a utilizar o seu dispositivo:

- 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
- Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
- 3. Seleccione o dispositivo onde pretende iniciar a função Fotografia de identificação e que pretende bloquear.
- 4. Prima o botão Fotografia de identificação.
- 5. Se necessário, na secção **Fotografia de identificação** introduza o texto que pretende apresentar no ecrã do dispositivo bloqueado.
- 6. Toque no botão Fotografar.

Quando o Kaspersky Internet Security for Android executar o comando, a fotografia de identificação é carregada para a Web Management. Pode reenviar o comando após obter a fotografia de identificação.

FILTRO DE TEXTO E CHAMADAS

O Filtro de Texto e Chamadas está disponível apenas em dispositivos com um cartão SIM inserido.

O Filtro de Texto e Chamadas permite bloquear a recepção de chamada e mensagens de texto não solicitadas. A aplicação filtra as chamadas e as mensagens de texto com base nas listas de contactos permitidos e bloqueados e em conformidade com o modo de filtro seleccionado.

NESTA SECÇÃO

Filtro de contactos padrão	<u>40</u>
Bloquear todos os contactos excepto os permitidos	<u>40</u>
Bloquear apenas contactos não solicitados	<u>41</u>

FILTRO DE CONTACTOS PADRÃO

Utiliza o modo de filtro padrão para receber chamadas e mensagens de texto dos contactos permitidos e bloqueia as chamadas e as mensagens de texto dos contactos bloqueados.

Se receber uma chamada ou uma mensagem de texto de um contacto que não está na lista de contactos permitidos e bloqueados, a aplicação solicita que seleccione uma acção a aplicar à chamada ou mensagem de texto deste contacto. Posteriormente, a aplicação irá processar automaticamente as chamadas e as mensagens de texto deste contacto de acordo com a acção seleccionada.

Para activar o modo de filtro padrão:

- 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Filtro de Texto e Chamadas > Padrão.
- 2. Crie uma lista de contactos bloqueados. Para isso, no painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Contactos bloqueados.
- 3. Crie uma lista de contactos permitidos. Para isso, no painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Contactos permitidos.
- 4. Se necessário, pode activar definições de filtro adicionais. Para tal, no painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Filtro de Texto e Chamadas**.

Para permitir chamadas e mensagens de texto de todos os contactos no livro de endereços do dispositivo, seleccione a caixa de selecção **Permitir contactos**.

Para bloquear as mensagens de texto de números de telefone que incluem letras, seleccione a caixa de selecção **Bloquear Números Não Numéricos**.

BLOQUEAR TODOS OS CONTACTOS EXCEPTO OS PERMITIDOS

Para bloquear as chamadas e as mensagens de texto de todos os contactos, excepto dos contactos permitidos, utilize o filtro no modo de contactos permitidos.

Para activar o filtro no modo de contactos permitidos:

1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Filtro de Texto e Chamadas > Contactos permitidos.

- 2. Crie uma lista de contactos permitidos. Para isso, no painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Filtro de Texto e Chamadas > Contactos permitidos**.
- 3. Se necessário, pode permitir as chamadas e as mensagens de texto dos contactos no livro de endereços do dispositivo:
 - a. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações > Filtro de Texto e Chamadas**.
 - b. Seleccione a caixa de selecção Permitir contactos.

BLOQUEAR APENAS CONTACTOS NÃO SOLICITADOS

Para bloquear as chamadas e as mensagens de texto apenas dos contactos bloqueados, utilize o filtro no modo de contactos bloqueados.

- Para activar o filtro no modo de contactos bloqueados:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Filtro de Texto e Chamadas > Contactos bloqueados.
 - 2. Crie uma lista de contactos bloqueados. Para isso, no painel de início rápido na janela principal do Kaspersky Internet Security, toque em Filtro de Texto e Chamadas > Contactos bloqueados.
 - 3. Se necessário, pode activar o bloqueio automático das mensagens de texto de números que incluem letras:
 - a. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações > Filtro de Texto e Chamadas**.
 - b. Seleccione a caixa de selecção Bloquear Números Não Numéricos.

PROTECÇÃO DE INTERNET E ANTI-PHISHING DE TEXTO

Com a Protecção de Internet e Anti-Phishing de Texto pode visitar sites confiáveis e utilizar dados pessoais na rede, em segurança.

A Protecção de Internet e o Anti-Phishing de Texto estão disponíveis apenas na versão Premium do Kaspersky Internet Security.

O componente Anti-Phishing de Texto está disponível apenas em dispositivos com um cartão SIM inserido.

A Protecção de Internet bloqueia sites maliciosos, que procuram distribuir código malicioso, e sites falsos (phishing), que procuram roubar os dados confidenciais do utilizador, e obter acesso às contas bancárias do utilizador.

O Anti-Phishing de Texto bloqueia ligações em mensagens SMS para sites de phishing ou maliciosos.

A Protecção de Internet verifica os sites antes de estes serem abertos. O Anti-Phishing de Texto também verifica as ligações em mensagens SMS antes de estas serem abertas. A Protecção de Internet e o Anti-Phishing de Texto efectuam verificações utilizando o serviço cloud da Kaspersky Security Network (um serviço online dedicado da Kaspersky Lab que contém informações sobre a fiabilidade de ficheiros, aplicações e recursos da Web).

NESTA SECÇÃO

Verificação constante de sites	<u>42</u>
Verificação constante de ligações de mensagens SMS	. <u>42</u>

VERIFICAÇÃO CONSTANTE DE SITES

A Protecção de Internet verifica os sites da Internet apenas no navegador do Android padrão e não os verifica noutros navegadores. Para utilizar a Protecção de Internet sempre que navegar na Web, definida o navegador do Android padrão como o navegador predefinido.

- Para activar a verificação em tempo real de sites:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações > Protecção de Internet**.
 - 1. Seleccione a caixa de verificação Protecção de Internet.
 - Toque em Alterar navegador (este botão é apresentado se a Protecção de Internet estiver activada e o navegador do Android padrão não estiver definido como o navegador predefinido).

É iniciado o assistente de selecção do navegador predefinido

3. Siga as instruções do assistente.

Pode activar a verificação de sites em tempo real na aplicação ou remotamente através do Web Management.

VERIFICAÇÃO CONSTANTE DE LIGAÇÕES DE MENSAGENS SMS

O componente Anti-Phishing de Texto está disponível apenas em dispositivos com um cartão SIM inserido.

- Para activar a verificação de ligações em SMS:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Protecção de Internet.
 - 2. Seleccione a caixa de verificação Anti-Phishing de SMS.

OUTRAS TAREFAS

Também pode executar as acções seguintes:

- activar a versão Premium da aplicação;
- comprar uma licença ou renovar uma licença existente;
- ver informações sobre a licença;
- ver relatórios sobre o funcionamento da aplicação (por exemplo, relatórios sobre verificações efectuadas, ameaças detectadas, mensagens SMS, chamadas ou websites bloqueados);
- alterar o código secreto da aplicação;
- restaurar o código secreto da aplicação.

NESTA SECÇÃO

Activar a versão Premium da aplicação	<u>43</u>
Adquirir uma licença	<u>43</u>
Renovar licença	<u>44</u>
Ver informações sobre a licença e respectivo período de validade	. <u>44</u>
Visualizar os relatórios de funcionamento da aplicação	. <u>44</u>
Alterar o código secreto da aplicação	. <u>45</u>
Recuperação do código secreto	<u>45</u>

ACTIVAR A VERSÃO PREMIUM DA APLICAÇÃO

Para utilizar todas as funções da aplicação, é necessário activar a versão Premium do Kaspersky Internet Security.

Activação – muda a aplicação para o modo com todas as funcionalidades. Para activar a aplicação, é necessário introduzir o código de activação recebido ao adquirir a aplicação, ou comprar uma licença numa loja online (consulte a secção "Adquirir uma licença" na página <u>43</u>).

Pode activar a versão Premium da aplicação quando iniciar a aplicação pela primeira ou mais tarde.

É necessária uma ligação à Internet em funcionamento para activar a aplicação.

Para activar a versão Premium da aplicação com o código de activação:

- No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Definições adicionais > Licenciamento > Activar a versão Premium.
- 2. Seleccione Inserir código de activação.
- 3. Introduza o código de activação na janela apresentada e toque em Activar.

A aplicação envia um pedido de activação para o servidor de activação da Kaspersky Lab. Quando a confirmação do pedido tiver sido recebida com êxito, a aplicação notifica o utilizador e apresenta as informações sobre a licença.

ADQUIRIR A LICENÇA

Se optar por utilizar a versão Premium do Kaspersky Internet Security, pode comprar uma licença para a aplicação na loja online da Kaspersky Lab ou junto de empresas parceiras.

Se adquirir uma licença na loja online, irá receber um código de activação para activar a versão Premium da aplicação (consulte a secção "Activar a versão Premium" na página <u>43</u>).

Quando compra a licença através da Google Play Store, a aplicação é activada automaticamente.

- Para comprar uma licença numa loja online:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Definições adicionais** > **Licenciamento** > **Activar a versão Premium**.

Quando renovar a licença o botão indicada Renovar.

2. Seleccione Adquirir uma licença.

É apresentada a página de Internet da loja online, onde poderá adquirir uma nova licença.

RENOVAR LICENÇA

Sempre que a aplicação é iniciada, o Kaspersky Internet Security verifica a existência de uma licença Premium para o Kaspersky Internet Security.

Se estiver a utilizar a versão Premium da aplicação, verifique o número de dias restantes até a licença expirar, consultando as informações sobre a licença (consulte a secção "Ver informações sobre licença" na página 44).

Quando restarem menos de 14 dias para a licença expirar, pode proceder à renovação. Para tal, pode comprar uma licença numa loja online (consulte a secção "Adquirir uma licença" na página <u>43</u>), ou utilizar um código de activação (consulte a secção "Código de activação" na página <u>23</u>) recebido ao comprar a licença.

Quando a licença expira, a aplicação muda automaticamente para a versão gratuita.

- Para renovar a licença com o código de activação:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Definições adicionais** > **Licenciamento** > **Renovar**.
 - 2. Seleccione Inserir código de activação.
 - 3. Introduza o código de activação, recebido de uma nova licença previamente adquirida.

VER INFORMAÇÕES SOBRE A LICENÇA E RESPECTIVO PERÍODO DE VALIDADE

É possível ver o número da chave, o prazo de validade da licença e outras informações sobre a licença.

As informações sobre a licença podem ser visualizadas quando utiliza uma versão de avaliação ou versão Premium da aplicação.

Para verificar o prazo da licença e ver as informações da licença:

No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Definições adicionais** > **Licenciamento** > **Sobre a licença**.

VISUALIZAR OS RELATÓRIOS DE FUNCIONAMENTO DA APLICAÇÃO

Os eventos dos componentes Scanner (Anti-Virus), Protecção de Internet e Filtro de Texto e Chamadas são registados em relatórios.

Os relatórios são agrupados por data de criação. Pode optar pode visualizar os relatórios de cada componente separadamente. Os relatórios podem incluir até 50 entradas. Quando o relatório excede as 50 entradas, as entradas mais antigas são eliminadas e substituídas por novas.

Para visualizar os relatórios de funcionamento das aplicações:

No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Definições adicionais** > **Relatórios**.

ALTERAR O CÓDIGO SECRETO

A aplicação solicitada que especifique o código secreto durante a configuração inicial do Anti-Roubo (consulte a secção "Efectuar a configuração inicial do Anti-Roubo" na página <u>27</u>) ou quando iniciar a Protecção de Privacidade pela primeira vez. Pode alterar o código secreto em qualquer altura.

- Para alterar o código secreto:
 - 1. No painel de início rápido na janela principal do Kaspersky Internet Security, toque em **Configurações** > **Definições adicionais** > **Alterar código secreto**.
 - 2. Introduza o código secreto actual no campo Introduza o código secreto actual e toque em Seg.
 - 3. Introduza o novo código secreto no campo Crie um novo código secreto e clique em Seg.
 - 4. Reintroduza o código novo no campo Reintroduzir o novo código e toque em Introduzir.

RECUPERAÇÃO DO CÓDIGO SECRETO

- Para recuperar o código secreto da aplicação:
 - 1. Abra a Web Management em https://anti-theft.kaspersky.com em qualquer dispositivo.
 - 2. Inicie sessão em Web Management com a sua Conta Kaspersky utilizada durante a configuração inicial da aplicação.
 - 3. Seleccione o dispositivo cujo código secreto tem de ser recuperado.
 - 4. Prima o botão Recuperação do código secreto.

O código de recuperação é apresentado em Web Management.

- 5. Inicie o Kaspersky Internet Security no dispositivo.
- No painel de início rápido na janela principal do Kaspersky Internet Security, toque em Configurações > Anti-Roubo.
- 7. Quando lhe for solicitado que introduza o código secreto, toque em Menu > Recuperação do código secreto.
- 8. Introduza o código de recuperação apresentado em Web Management.

O código secreto é apresentado no ecrã do dispositivo.

9. Introduza o código secreto no campo Introduza o código secreto restaurado.

A aplicação abre a janela Definições de Anti-Roubo.

CONTACTAR O SERVIÇO DE SUPORTE TÉCNICO

Esta secção fornece informações sobre como obter suporte técnico e sobre os requisitos para receber ajuda do Suporte Técnico.

NESTA SECÇÃO

Obter suporte técnico	<u>46</u>
Suporte Técnico por telefone	<u>46</u>
Obter suporte técnico através da Conta Kaspersky	<u>46</u>

OBTER SUPORTE TÉCNICO

Se não encontrar uma solução para o seu problema na documentação da aplicação ou numa das fontes de informação acerca da aplicação (consulte a secção "Fontes de informação sobre a aplicação" na página <u>8</u>), recomendamos que contacte o Serviço de Suporte Técnico da Kaspersky Lab. Os especialistas do Serviço de Apoio Técnico responderão a todas as suas dúvidas sobre a instalação e a utilização da aplicação.

Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte (http://support.kaspersky.com/support/rules).

Se não conseguir encontrar uma solução para o seu problema, por favor contacte o Serviço de Suporte Técnico da Kaspersky Lab através de uma das seguintes formas:

- Por telefone: (351) 22 510 6476 ou (351) 21 381 09 22. Este método permite contactar os nossos especialistas de Suporte Técnico internacional.
- Enviando uma questão a partir da sua Conta Kaspersky no site do Serviço de Suporte Técnico. Este método
 permite-lhe contactar os especialistas do Suporte Técnico através de um formulário de pedido.

O suporte técnico apenas está disponível para os utilizadores que adquiriram uma licença para utilizar a aplicação. Não é fornecido suporte técnico a utilizadores de versões de avaliação.

SUPORTE TÉCNICO POR TELEFONE

Se surgir uma questão urgente, pode contactar os especialistas de Suporte Técnico por telefone:(351) 22 510 6476; (351) 21 381 09 22. (<u>http://support.kaspersky.com/support/contacts</u>).

Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte (<u>http://support.kaspersky.com/support/rules</u>). Isto permitirá que os nossos especialistas o possam ajudar de forma mais rápida.

OBTER SUPORTE TÉCNICO ATRAVÉS DA CONTA Kaspersky

A Conta Kaspersky é a sua área pessoal (https://my.kaspersky.pt) no site do Serviço de Suporte Técnico.

Para obter acesso à Conta Kaspersky, deve efectuar o procedimento de registo na página de registo (<u>https://my.kaspersky.com/pt/registration</u>). Insira o seu endereço de e-mail e uma password para iniciar sessão em A Minha Conta Kaspersky.

Em Conta Kaspersky, pode executar as seguintes acções:

- Contactar o Serviço de Suporte Técnica e o Virus Lab.
- contactar o Serviço de Suporte Técnico sem utilizar o e-mail;
- acompanhar o estado do seu pedido em tempo real;
- ver um histórico detalhado dos seus pedidos ao Serviço de Suporte Técnico;
- receber uma cópia do ficheiro da chave se tiver sido perdido ou removido.

Enviar a sua dúvida por correio electrónico para o Serviço de Apoio Técnico

Pode enviar um pedido online para o Serviço de Suporte Técnico em russo, inglês, alemão, francês ou espanhol.

Deve especificar os seguintes dados nos campos do formulário do pedido online:

- tipo de pedido;
- nome e número da versão da aplicação;
- descrição do pedido;
- ID e password do cliente;
- endereço de e-mail.

O especialista do Serviço de Suporte Técnico envia a resposta à sua questão para a sua Conta Kaspersky e para o endereço de e-mail que especificou no seu pedido online.

Pedido online ao Virus Lab

Alguns pedidos têm de ser enviados para o Virus Lab em vez do Suporte Técnico.

Pode enviar pedidos ao Virus Lab nas seguintes circunstâncias:

- Suspeita de que um ficheiro ou recurso da Internet contém um vírus, mas o Kaspersky Internet Security não detecta a ameaça. Os especialistas do Virus Lab verificam o ficheiro ou recurso da Internet que enviou. Se detectarem um vírus desconhecido, adicionam a correspondente descrição à base de dados, que será disponibilizada na actualização das aplicações antivírus da Kaspersky Lab.
- O Kaspersky Internet Security determina que um ficheiro ou recurso da Internet contém um vírus, mas o utilizador tem a certeza de que não é perigoso.

Pode também enviar pedidos para o Virus Lab a partir da página com o formulário de pedido (<u>http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt</u>) sem estar registado na Conta Kaspersky. Nesta página, não tem de especificar o código de activação da aplicação.

GLOSSÁRIO

A

ACTIVAR A APLICAÇÃO

Mudar a aplicação para o modo de funcionamento total. A activação é efectuada pelo utilizador antes ou após a instalação da aplicação. Para activar a aplicação, é necessário introduzir o código de activação recebido com a aplicação, ou comprar uma licença numa loja online.

CÓDIGO DE ACTIVAÇÃO

Um código recebido ao adquirir uma licença para o Kaspersky Internet Security. Este código é necessário para a activação da aplicação.

O código de activação é uma sequência alfanumérica de caracteres latinos no formato xxxxx-xxxxx-xxxxx.

BASES DE DADOS DE ANTIVÍRUS

Estas bases de dados contêm informações acerca de ameaças à segurança do computador conhecidas pela Kaspersky Lab na altura da disponibilização da base de dados. Os registos das bases de dados permitem detectar código malicioso em objectos verificados. As bases de dados são criadas por especialistas da Kaspersky Lab e são actualizadas de hora em hora.

CÓDIGO SECRETO DA APLICAÇÃO

O código secreto é pedido nas seguintes situações:

- Para aceder às configurações de Anti-Roubo e Protecção de Privacidade
- Ao enviar um comando de SMS de outro dispositivo móvel para remotamente activar o alarme do dispositivo, bloquear o dispositivo, localizá-lo no mapa, eliminar dados ou ocultar contactos confidenciais e as informações relacionadas

ARQUIVO

Um ou vários ficheiros compactados sob a forma de um ficheiro comprimido único. É necessária uma aplicação especial intitulada "arquivador" para compactar ou descompactar dados.

D

ELIMINAÇÃO DE UM OBJECTO

Um método de processamento de objectos em que os objectos são removidos fisicamente da sua localização original. É aconselhável aplicar este método de processamento a todos os objectos maliciosos que não for possível desinfectar.

DESINFECTAR OBJECTOS

Um método de processamento de objectos infectados que resulta numa recuperação total ou parcial dos dados. Nem todos os objectos infectados podem ser desinfectados.

OBJECTO INFECTADO

Um objecto em que um segmento do respectivo código corresponde na íntegra a um segmento de código de uma ameaça conhecida. A Kaspersky Lab não recomenda a utilização de tais objectos.

Κ

KASPERSKY SECURITY NETWORK (KSN)

Uma infra-estrutura de serviços online que permite o acesso à base de conhecimento da Kaspersky Lab, que contém informações acerca da reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network garante uma resposta mais rápida das aplicações da Kaspersky Lab face a ameaças desconhecidas, melhora a eficácia de alguns componentes de protecção e reduz o risco de falsos diagnósticos positivos.

L

PRAZO DA LICENÇA

O prazo da licença é o período durante o qual o utilizador tem acesso às funcionalidades da aplicação e direitos de utilização dos serviços adicionais. Os serviços disponíveis dependem do tipo de licença.

LISTA DE CONTACTOS PERMITIDOS

A lista de contactos permitidos contém contactos dos quais não pretende receber mensagens.

As entradas nesta lista contêm as seguintes informações:

- Número de telefone a partir do qual o Filtro de Texto e Chamadas permite receber chamadas e/ou SMS.
- Tipos de eventos que o Filtro de Texto e Chamadas entrega deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.
- Expressão-chave utilizada pelo Filtro de Texto e Chamadas para classificar uma SMS como solicitada (não spam). O Filtro de Texto e Chamadas apenas entrega SMS que contenham a expressão-chave, sendo que bloqueia todas as outras SMS.

LISTA DE CONTACTOS BLOQUEADOS

A lista de contactos bloqueados contém contactos dos quais não pretende receber mensagens.

As entradas nesta lista contêm as seguintes informações:

- Número de telefone a partir do qual o Filtro de Texto e Chamadas bloqueia chamadas e (ou) SMS.
- Tipos de eventos que o Filtro de Texto e Chamadas bloqueia deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.
- Expressão-chave que o Filtro de Texto e Chamadas utiliza para classificar uma SMS como não solicitada (spam). O Filtro de Texto e Chamadas apenas bloqueia SMS que contenham a expressão-chave, sendo que entrega todas as outras SMS.

Ν

NÚMERO NÃO NUMÉRICO

Um número de telefone que inclui letras ou é constituído apenas por letras.

U

ACTUALIZAR AS BASES DE DADOS

Uma das funções que a aplicação da Kaspersky Lab executa e que mantém a protecção actualizada. As bases de dados antivírus são copiadas dos servidores de actualização da Kaspersky Lab para o dispositivo e automaticamente ligadas à aplicação.

KASPERSKY LAB

O software da Kaspersky Lab é internacionalmente reconhecido pela sua protecção contra vírus, software malicioso, spam, ataques de rede e de hackers e outras ameaças.

Em 2008, a Kaspersky Lab foi classificada entre as quatro primeiros fornecedores mundiais de software de segurança de informação para utilizadores finais (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é o fornecedor favorito dos utilizadores domésticos na Rússia em termos de sistemas de protecção de computadores, de acordo com o inquérito "TGI-Rússia 2009" da COMCON.

A Kaspersky Lab foi fundada na Rússia em 1997. Actualmente, é um grupo internacional de empresas sediado em Moscovo com cinco divisões regionais que gerem a actividade da empresa na Rússia, Europa Ocidental e de Leste, Médio Oriente, África, América do Norte e do Sul, Japão, China e outros países na região Ásia-Pacífico. A empresa emprega mais de 2000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab fornecem protecção para todos os sistemas – de computadores domésticos até grandes redes empresariais.

A gama de produtos pessoais inclui aplicações antivírus para computadores de secretária, portáteis e de bolso e para smartphones e outros dispositivos móveis.

A Kaspersky Lab oferece aplicações e serviços para protecção de estações de trabalho, servidores de ficheiros e Internet, gateways de e-mail e firewalls. Quando utilizadas juntamente com o sistema de gestão centralizada da Kaspersky Lab, estas soluções asseguram uma protecção automática eficaz contra ameaças informáticas para empresas e organizações. Os produtos da Kaspersky Lab são certificados pelos maiores laboratórios de teste, são compatíveis com o software de muitos fornecedores de aplicações informáticas e são optimizados para funcionar em muitas plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham 24 horas por dia. Todos os dias descobrem centenas de novas ameaças informáticas, criam ferramentas para detectar e desinfectar as mesmas e incluem-nas nas bases de dados utilizadas pelas aplicações da Kaspersky Lab. *A base de dados antivírus da Kaspersky Lab é actualizada a cada hora*; e a *base de dados Anti-Spam a cada cinco minutos*.

Tecnologias. Muitas das tecnologias que são agora parte integrante das ferramentas modernas de antivírus foram inicialmente desenvolvidas pela Kaspersky Lab. É portanto lógico que muitas empresas programadoras de software utilizem o kernel do Kaspersky Anti-Virus nas suas próprias aplicações. Essas empresas incluem: SafeNet (EUA), Alt-N Technologies (EUA), Blue Coat Systems (EUA), Check Point Software Technologies (Israel), Clearswift (Reino Unido), CommuniGate Systems (EUA), Critical Path (Irlanda), D-Link (Taiwan), M86 Security (EUA), GFI (Malta), IBM (EUA), Juniper Networks (EUA), LANDesk (EUA), Microsoft (EUA), NETASQ (França), NETGEAR (EUA), Parallels (Rússia), SonicWALL (EUA), WatchGuard Technologies (EUA) e ZyXEL Communications (Taiwan). Muitas das tecnologias inovadoras da empresa estão patenteadas.

Êxitos. Ao longo dos anos, a Kaspersky Lab ganhou centenas de prémios pelos seus serviços no combate contra ameaças informáticas. Em 2010, o Kaspersky Anti-Virus recebeu os mais destacados prémios Advanced + após testes realizados pela AV-Comparatives, um laboratório de antivírus austríaco de referência. Contudo, o grande feito da Kaspersky Lab é a lealdade dos seus utilizadores em todo o mundo. Os produtos e tecnologias da empresa protegem mais de 300 milhões de utilizadores e o seu número de clientes empresariais é superior a 200.000.

Site da Web da Kaspersky Lab:	http://www.kaspersky.com/pt/_
Enciclopédia de Vírus:	http://www.securelist.com
Laboratório antivírus:	newvirus@kaspersky.com (para enviar ficheiros provavelmente infectados apenas no formato de arquivo)
	http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt
	(para colocar questões aos analistas de vírus)
Fórum na Internet da Kaspersky Lab:	http://forum.kaspersky.com/index.php?showforum=86

INFORMAÇÃO SOBRE CÓDIGO DE TERCEIROS

A informação sobre o código de terceiros está incluída no bloco Sobre, localizada na configuração da aplicação.

AVISOS DE MARCAS COMERCIAIS

As marcas comerciais e de serviços registadas são propriedade dos seus respectivos detentores.

Android e Google são marcas comerciais da Google, Inc.

ÍNDICE

Α

Activar a aplicação código de activação comprar o código de activação online licença	
Actualizaçãoiniciar manualmente	
Actualizar início agendado	
Agendamento Actualização Verificações a pedido	
Alarme	
Anti-Roubo Alarme Bloquear e Localizar Fotografia de identificação. Limpeza de Dados Prot. Cartão SIM	

С

Código	
Alterar o código secreto da aplicação	45
Recuperar o código secreto	45
Código secreto da aplicação	45
Conta Kaspersky	27
Contrato de Licença	22

D

Determinar a localização do dispositivo	28, 36
E	
Enviar comando de SMS	8, 34, 35
Executar Actualizar manualmente	32
Verificar o dispositivo manualmente	
Verificar o dispositivo mediante agendamento	31
I	
Ícone na barra de estado	20
Iniciar a aplicação	25
J	
Janela principal	16
κ	
Kaspersky Lab	50
L	
Licença Acordo de Licença de Utilizador Final22 activar a aplicação	2, 43, 44 43

informações renovação renovar online	
Ν	
Notificações da aplicação	21
P	
Protecção de Privacidadeinício remoto	33, 34 34
R	
Relatórios	44
Renovar licença	43
V	
Verificações a pedido	31
W	
Widget do ecrã inicial	20