Kaspersky Internet Security for Android

User Guide

Dear User,

Thank you for choosing our product. We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

Date revision date: 6/26/2013

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

TABLE OF CONTENTS

ABOUT THIS GUIDE

This document is the User Guide to Kaspersky Internet Security for Android (hereafter "Kaspersky Internet Security").

The User Guide is meant for users of Kaspersky Internet Security who are familiar with the operating system interface, possess basic system usage skills, and know how to use the Internet.

The User Guide serves the following purposes:

- Getting to know the app interface.
- Finding quick solutions to common Kaspersky Internet Security issues.
- Describe additional sources of information about the app and ways of receiving technical support.

IN THIS SECTION

IN THIS DOCUMENT

This guide includes the following sections.

Sources of information about the app

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

Kaspersky Internet Security

This section describes the application's features and provides brief information about the application's functions and components. You will learn what items are included in the distribution kit, and what services are available for registered users of the application. This section provides information about software and hardware requirements that a device should meet to allow installing the application on it.

Installing and uninstalling the app

This section contains step-by-step instructions for installing and removing Kaspersky Internet Security.

App interface

This section covers the main graphical user interface elements of the app: main window, protection status indicator is shaped as a shield, quick launch panel, app icon, widget, and notification windows.

Licensing the app

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the License Agreement, ways of activating the app, and license renewal.

Starting and stopping the app

This section contains information about how to launch the application and how to stop using it.

Quick Start

This section describes how you can start using the app quickly after it was installed:

- Information about the main features of the app;
- Instructions for neutralizing a malicious object
- Information on how to protect your data against unauthorized access
- Instructions to be followed when your device gets lost or stolen.

Dealing with standard tasks

This section contains step-by-step instructions for carrying out the basic user tasks that the app deals with.

Contacting the Technical Support service

This section describes how you can contact Kaspersky Lab Technical Support.

Glossary

This section contains a list of terms mentioned in the document and their respective definitions.

Kaspersky Lab ZAO

This section contains information about Kaspersky Lab ZAO.

Information about third party code

This section provides information about the third-party code used in the application.

Trademark notifications

This section lists trademarks of third-party right-owners used herein.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

The text herein is accompanied by semantic elements that should be given particular attention – warnings, hints, examples.

Document conventions are used to highlight semantic elements. Document conventions and examples of their use are shown in the table below.

Table 1. Document conventions

SAMPLE TEXT	DESCRIPTION OF DOCUMENT CONVENTION
Note that...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss, failures in equipment operation or operating system problems.
We recommended that you use...	Notes are boxed. Notes may contain useful hints, recommendations, specific values for settings, or important special cases in operation of the app.
Example: ...	Examples are given on a yellow background under the heading "Example".
Update means... The *Databases are out of date* event occurs.	The following semantic elements are italicized in the text: • New terms • Names of app statuses and events
Click the **Enable** button.	Names of app interface elements, such as entry fields, menu items, and buttons, are in bold.
➡ *To configure a task schedule:*	Introductory phrases of instructions are italicized and marked with the arrow sign.
<User name>	Variables are in angle brackets. It is required to replace each variable by the corresponding value, omitting angle brackets.
Send an SMS message to your device with the following text: find: <code>.	The different font style highlights the text of the SMS command.

SOURCES OF INFORMATION ABOUT THE APP

This section describes sources of information about the application and lists websites that you can use to discuss the application's operation.

You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to find information about the application:

- App page on the Kaspersky Lab website
- App page on the Technical Support website (Knowledge Base)
- Online help
- Documentation

If you cannot solve an issue on your own, we recommend that you contact Kaspersky Lab Technical Support (see section "Technical support by phone" on page 42).

An Internet connection is required to use information sources on the Kaspersky Lab website.

App page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On this page (http://www.kaspersky.com/android-security), you can view general information about the app, its functions and features.

The page http://www.kaspersky.com features a URL to the eStore. There you can purchase or renew the application.

The application's page at the Technical Support Service website (Knowledge Base).

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. Knowledge Base comprises reference articles grouped by topics.

On the page of the app in the Knowledge Base (http://support.kaspersky.com/mobile/kisandroid), you will find articles that provide useful information, advice, and answers to frequently asked questions on how to purchase, install, and use the app.

Articles answer questions relating not just to Kaspersky Internet Security, but also to other Kaspersky Lab apps. They also may contain news from Technical Support.

Online help

The application's online help consists of help files.

The context help contains data on each of the windows in the application: a list of settings and their respective descriptions, as well as a list of tasks to perform.

The complete help contains detailed information on how to manage protection, how to configure the application settings and how to address the user's basic tasks.

The installed Documentation

The User Guide describes the app interface and ways to perform common tasks while using the app.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users on our Forum (http://forum.kaspersky.com).

In this forum you can view existing topics, leave your comments, create new topics.

CONTACTING THE SALES DEPARTMENT

If you have any questions on how to select, purchase, or renew the application, you can contact our Sales Department specialists in one of the following ways:

- By calling our central office in Moscow by phone (http://www.kaspersky.com/contacts).
- By emailing your question to sales@kaspersky.com.

Service is provided in Russian and in English.

CONTACTING TECHNICAL WRITING AND LOCALIZATION UNIT BY EMAIL

To contact the Documentation Development Group, please send your message to docfeedback@kaspersky.com . Please use "Kaspersky Help Feedback: Kaspersky Internet Security for Android" as the subject line in your message.

KASPERSKY INTERNET SECURITY

Kaspersky Internet Security offers the following main features:

Protection against viruses and other malware

The device is protected against viruses and other malware by the Scanner (Anti-Virus) component.

The component is called Scanner in the free version and Anti-Virus in the premium version.

Scanner only lets you scan the entire device, the installed apps, or a specific folder for threats, configure scheduled scans of the device, as well as update the anti-virus databases for up-to-date protection of your data.

Anti-Virus combines the full functionality of Scanner with the following additional features:

- Protects your device in real time
- Scans newly installed apps before they are launched for the first time, using anti-virus databases and the Kaspersky Security Network online cloud service
- Supports automatic updates of anti-virus databases

Hiding confidential contacts and related call history and SMS correspondence

The Privacy Protection component serves to hide confidential contacts and related information.

Privacy Protection is available only with the premium version of Kaspersky Internet Security on devices with an inserted SIM card.

Privacy Protection allows you to hide temporarily your confidential contacts and all related call history and SMS correspondence. You can enable hiding of contacts and related information using app settings or remotely by means of a special SMS command.

Data protection in the event of loss or theft of the device

The Anti-Theft protect your data against unauthorized access and helps you to locate the device when it gets lost or stolen.

Anti-Theft allows you to remotely turn on the device alarm, lock the device, determine its location, wipe device data, and take a mugshot of the person currently using your device. Anti-Theft lets you remotely start the functions on the device by means of special SMS commands or via Web Management at https://anti-theft.kaspersky.com. For devices with a SIM card slot, when the SIM card is replaced or the device is turned on without a SIM card, Anti-Theft can send you the new phone number of the device in an SMS message or email, or lock the device.

Blocking unsolicited calls and text messages

Call&Text Filter is used to block unsolicited calls and text messages.

The Call&Text Filter component is available only on devices with an inserted SIM card.

Protection against online threats

The Web Protection and Text Anti-Phishing components provide protection against online threats.

Web Protection and Text Anti-Phishing components are available only for the premium version of Kaspersky Internet Security.

The Text Anti-Phishing component is available only on devices with an inserted SIM card.

Web Protection blocks malicious websites, which aim to distribute malicious code, and fake (phishing) websites, which aim to steal your confidential data and gain access to your financial accounts.

Text Anti-Phishing blocks SMS links to malicious and spoofed websites.

IN THIS SECTION

WHAT'S NEW

Kaspersky Internet Security offers the following new features:

- One application for tablets and smartphones.
- The user interface has been redesigned.
- The device protection status window has been added, providing the following options:
  - Viewing all security-related issues in a single window, and fixing them in one step.
  - Viewing details on scans performed, updates of anti-virus databases, and the current application version.
- Enabling Alarm via the Web Management.
- Running Lock & Locate with one command via the Web Management.

HARDWARE AND SOFTWARE REQUIREMENTS

The device should meet the following requirements to support Kaspersky Internet Security:

- Smartphone or tablet with a screen resolution of 320x480 pixels or higher.
- 15 MB of free disk space in the main memory of the device.
- Android™ operating system versions 2.3 – 4.2.

The app is installed to the main memory of the device only.

The SIM card must be inserted in the device to enable the use of Call&Text Filter, Privacy Protection, SIM Watch, and Text Anti-Phishing.

DISTRIBUTION KIT

You can purchase the application in one of the following ways:

- **In a box**. Sold through our partners' stores.
- **Through an online store**. Distributed at online stores of Kaspersky Lab (for example, http://www.kaspersky.com, section **eStore**) or partner companies.
- **via Google Play**. Downloaded to the device via the Google Play service.

If you purchase the application in a box, the distribution kit includes the following components:

- sealed envelope with a QR-code for app installation
- quick start guide containing the activation code for the app
- license agreement setting out the terms on which you can use the app

The content of the distribution kit may vary depending on the region in which the app is sold.

If you purchase Kaspersky Internet Security at an online store, you copy the app from the website of the store. The information required to activate the app, including the activation code, is sent to you by email following payment.

For more details on purchase methods and the distribution kit, contact the Sales Department sales@kaspersky.com .

USER SERVICE

By purchasing a license to use the application, you can access the following services during the license validity period:

- updating databases and providing new versions of the app;
- consulting by phone and by email on issues related to installation, configuration, and use of the app;
- announcements of new Kaspersky Lab releases and of new viruses and outbreaks. To use this service, subscribe to the Kaspersky Lab newsletter on the Technical Support website.

No consulting services are provided on issues related to the functioning of operating systems, third-party software and technologies.

INSTALLING AND UNINSTALLING THE APP

This section contains step-by-step instructions for installing and removing Kaspersky Internet Security.

IN THIS SECTION

INSTALLING THE APP

Kaspersky Internet Security for Android can be installed from Google Play or from the app distribution package saved on the device.

To install Kaspersky Internet Security for Android from Google Play:

1. Open Google Play and locate Kaspersky Internet Security in the list of apps.
2. Tap **Install** or **Buy** depending on the app version.

The app is installed automatically with the parameters recommended by Kaspersky Lab.

To install Kaspersky Internet Security for Android from the distribution package:

1. Copy the app distribution package to your device. Perform one of the following actions:
   - If the app distribution package was previously downloaded and saved on a desktop computer, connect the device to the computer and copy the app distribution package to the device.
   - Download the app distribution package to the device from the Kaspersky Lab online store (http://www.kaspersky.com/store).
2. Start installation of the app. For this purpose open the APK archive on the device.

The app installation wizard starts. After the wizard operation is complete, the app is installed with the settings recommended by Kaspersky Lab specialists.

UNINSTALLING THE APP

To uninstall Kaspersky Internet Security for Android:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Additional settings** > **Uninstall app**.
2. Enter the secret code.
3. If you forget the app secret code, you can restore it (see section "Recovering the app secret code" on page 41).

Kaspersky Lab does not recommend uninstalling Kaspersky Internet Security for Android. This will compromise the security of your device and personal data.

APP INTERFACE

This section covers the main graphical user interface elements of the app: main window, protection status indicator is shaped as a shield, quick launch panel, app icon, widget, and notification windows.

IN THIS SECTION

MAIN WINDOW OF KASPERSKY INTERNET SECURITY

The main app window (see figure below) contains the interface elements for accessing the main app functions.

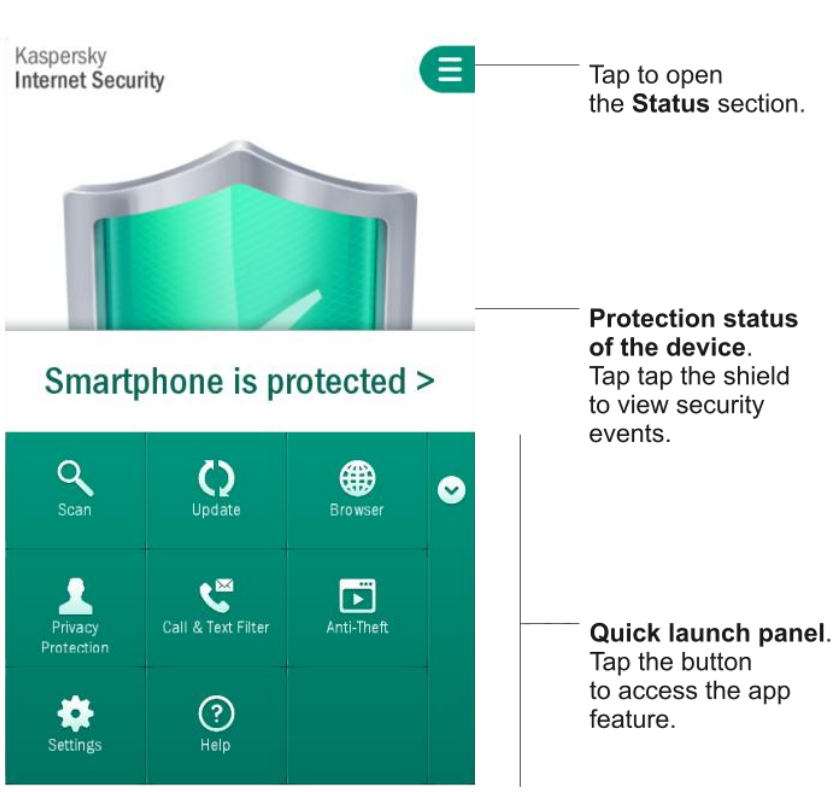

Figure 1. Main window

The number of buttons on the quick launch panel can vary depending on the available functions.

PROTECTION STATUS INDICATOR SHAPED AS A SHIELD

The protection status indicator is shaped as a shield and located in the center of the main window (see figure below).

The shield color changes with the status of device protection:

- Green – the device is adequately protected. All protection components operate according to the settings recommended by Kaspersky Lab specialists. Kaspersky Internet Security databases are up to date. No malicious objects have been detected during a scan of the device, or all detected malicious objects have been neutralized by the app.

- Yellow – the level of protection is below normal, and there are certain problems in the operation of Kaspersky Internet Security. For example, the device has not been scanned for more than 14 days, or you have installed a new app that has not been scanned.

- Red – there are problems that may lead to infection of the device and loss of data. For example, certain protection components have been paused or anti-virus databases have not been updated for more than 14 days.

By tapping the shield in the main app window, you can open the **Status** section (see figure below). The **Status** section provides detailed information on the status of device protection and proposes ways to address problems and threats.

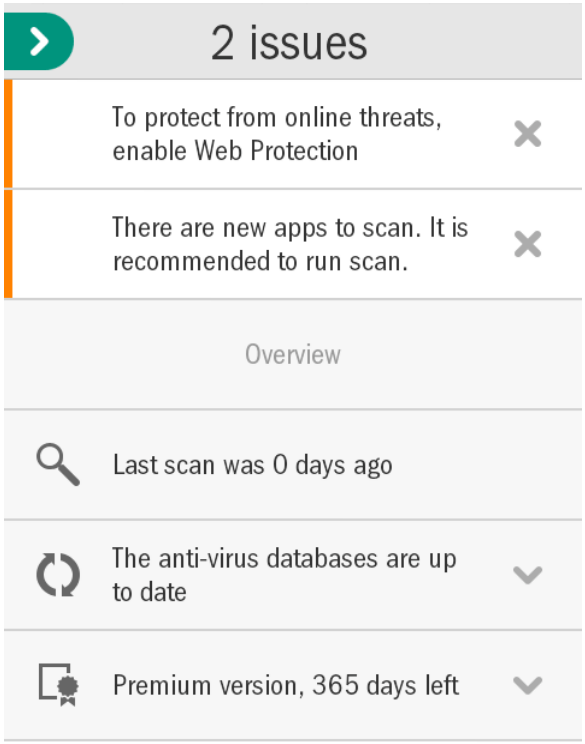

Figure 2. Status section

Protection-related problems are grouped by categories. For each problem, actions are listed that you can use to solve the problem.

There are two types of protection problems:

- *Notification problems*. Highlighted in yellow. Notification problems notify the user about events that can potentially affect device security (for example, the fact that the last scan was performed more than 14 days ago or that a new app has not been scanned). You can hide a notification problem by swiping it to the left. After this, information about the problem can be accessed via the **Hidden problems** menu.

- *Critical*. Highlighted in red. Critical problems notify the user about events of critical importance to device security (such as the release of a new app version or the fact that the anti-virus databases have not been updated for a long time). A critical problem cannot be hidden.

QUICK LAUNCH PANEL

The quick launch panel provides quick access to the main app functions (see figure below).

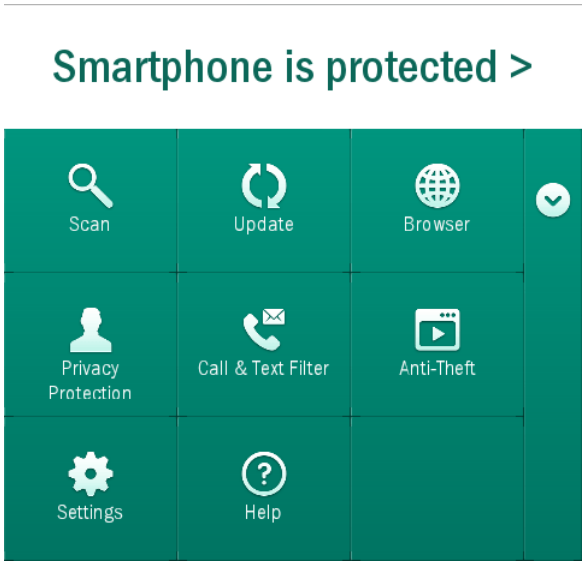

Figure 3. Quick launch panel

The quick launch panel is minimized by default. You can maximize the quick launch panel by pulling it up or tapping the button.

The number of buttons on the quick launch panel can vary depending on the available functions.

The meaning of each quick launch panel button is explained in the table below.

Table 2. Functions of quick launch panel buttons

BUTTON	FUNCTION
(**Scan**)	Lets you scan the entire device, the installed apps only, a selected folder or file.
(**Update**)	Starts updating the anti-virus database of the app to ensure up-to-date protection of the device.
(**Browser**)	Opens the default Android browser with enabled scanning of websites for viruses and phishing.
(**Privacy Protection**)	Temporarily hides or displays pre-selected confidential contacts and information relating to them.
(**Call & Text Filter**)	Opens the Call & Text Filter mode selection window.
(**Anti-Theft Web Management**)	Opens Web Management for remote management of Anti-Theft functions on the device.

BUTTON	FUNCTION
 (**Settings**)	Opens the app settings window.
 (**Help**)	Opens the app help.

ICON IN NOTIFICATION AREA

After the first run wizard finishes, the icon of Kaspersky Internet Security appears in the status bar.

The icon reflects the operation of the app and provides access to the main window of the app.

Indication that the app is running

The icon indicates that the app is running. In the premium version, it reflects the protection status of your device:

-  (color icon): protection is enabled;
-  (black and white icon): protection is disabled;
-  (color icon with an exclamation mark): there are protection problems. For example, the anti-virus databases are outdated, or a newly installed app has not been scanned.

In the free version of the app, the icon does not reflect the device protection status.

Access to the main window of the app

You can open the application main window through the application icon in the notification area.

WIDGET FOR THE DEVICE HOME SCREEN

Kaspersky Internet Security includes the device home screen widget (see fig. below).

Figure 4. Home screen widget

The widget is used to switch to the main window of the app.

In the premium version of the app, the color of the home screen widget indicates the protection status of your device. In the premium version of the app, the color of the widget can also inform you of hidden confidential contacts and related information if it has been allowed in the widget options.

The widget uses the following color codes:

- a green shield signifies that Protection is enabled;
- a gray shield indicates that Protection is disabled;
- a green background signifies that the app is hiding confidential contacts and related information;
- a gray background signifies that the app is displaying confidential contacts and related information.

In the free version of the app, the widget color does not indicate the device protection status.

NOTIFICATIONS

Kaspersky Internet Security for Android notifies you about significant events that occur during its operation by means of *notification windows* and *pop-up notifications* that appear in the status bar.

Kaspersky Internet Security for Android displays *notification windows* when you have different options to choose from when responding to an event. For example, when the app detects a malicious object that it cannot disinfect, you can delete the object, skip it, or view help on how to handle the object (see figure below). The app prompts you to choose an action. The notification window will only disappear from the screen after you have selected one of the proposed actions.

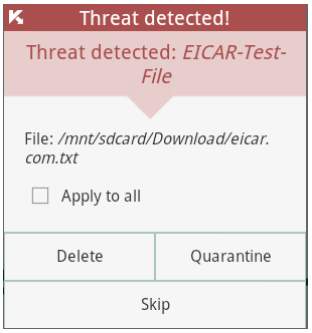

Figure 5. Notification windows

Kaspersky Internet Security for Android displays *pop-up notifications* in the status bar to inform you about events that do not require you to select an action (see figure below). You can view the notifications later in your device's notification bar.

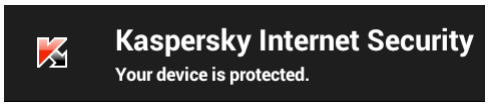

Figure 6. Pop-up notifications

Depending on the level of importance of an event, notifications are divided into three types in terms of device security:

- Critical notifications inform you about events of primary importance to the device's security (for example, the detection of a malicious file). Critical notifications are highlighted in red.
- Important notifications inform you about events of potential importance to the device's security (for example, the launch of a scan or update). Important notifications are highlighted in green.
- Informative notifications inform you about events not of primary importance to the device's security. Information notifications are not highlighted.

LICENSING THE APP

This section provides information about general terms related to the application activation. Read this section to learn more about the purpose of the License Agreement, ways of activating the app, and license renewal.

IN THIS SECTION

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

Read through the terms of the License Agreement carefully before you start using the application.

It is considered that you accept the terms of the License Agreement by confirming that you agree with the text of the License Agreement when installing the app. If you do not accept the terms of the End User License Agreement, you have to abort the installation of the app and refrain from using it.

ABOUT LICENSE

License– a right to use the app, provided according to the License agreement.

The license includes the right to benefit from the following services:

- Use the app on one or several devices.

  The number of devices on which you can use the app is specified in the terms of the License Agreement.

- Contacting Kaspersky Lab Technical Support for assistance.
- Other services available from Kaspersky Lab or its partners during the license period. (see section «Service for registered users» on page 12)

The scope of available services and app usage term depend on the app version.

The following app versions are available:

- *Free version*. The free version offers limited functionality of Kaspersky Internet for an unlimited time. The limitations of the free version are described in the License Agreement. The free version is available as soon as you install the app. You can switch to the free version or premium version of the app from the trial version.
- *Trial version.* The trial version lets you use full app functionality during a trial period without paying a fee.

  You can switch to the premium version or free version of the app from the trial version. When the trial period expires, the app automatically switches to the free version.

- *Premium version.* The premium version offers full app functionality. The premium version is available to buyers of the app license. The premium license is valid for a limited time.

  You can continue using the app after the license expires. To do so, renew the premium license or switch to the free version. To renew the license, enter a new activation code that comes with the licensed product, or purchase a new license online.

  When the license expires, the app automatically switches to the free version.

ABOUT THE ACTIVATION CODE

Activation code is a code that you receive on acquiring the premium license for Kaspersky Internet Security. The code is required for activation of the app.

The activation code is a unique sequence of 20 Latin characters and numbers in the format xxxxx-xxxxx-xxxxx-xxxxx.

Depending on the way of purchasing the application, the following options are available for receiving an activation code:

- If you have purchased the boxed version of Kaspersky Internet Security, the activation code is specified in the documentation or on the box containing the setup CD.

- If you have purchased Kaspersky Internet Security at an online store, the activation code is sent to the email address that you have specified when ordering the product.

The license validity period is calculated from the date on which the application is activated. If you have acquired a license intended for the use of Kaspersky Internet Security on several devices, the term of the license starts counting down from the moment you have first applied the activation code.

If you have lost or accidentally deleted your activation code after the activation, contact Kaspersky Lab Technical Support to restore it.

STARTING AND STOPPING THE APP

Kaspersky Internet Security for Android launches when the operating system starts up and protects your device during the entire session.

You can stop using the app by removing Kaspersky Internet Security or disabling all of its components.

Kaspersky Lab does not recommend disabling all components of Kaspersky Internet Security. This will compromise the security of your device and personal data.

QUICK START

This section describes how you can start using the app quickly after it was installed:

- Information about the main features of the app;
- Instructions for neutralizing a malicious object
- Information on how to protect your data against unauthorized access
- Instructions to be followed when your device gets lost or stolen.

IN THIS SECTION

WHAT TO DO WHEN A MALICIOUS OBJECT HAS BEEN DETECTED

If a security threat is detected at the launch of an app (such as a game), Kaspersky Internet Security prompts to you choose an action to be taken on this app. You can select one of the following actions:

- **Quarantine**: the app is moved to Quarantine.
- **Delete**: the app is deleted.
- **Skip**: no action is taken on the app.

Kaspersky Lab recommends neutralizing the threats as they are detected.

If a malicious object is detected during a file scan, Kaspersky Internet Security for Android moves it to Quarantine by default and notifies the user that the threat has been neutralized.

You can view information about malicious objects detected in the **Status** and **Reports** sections.

HOW TO PROTECT DATA AGAINST UNAUTHORIZED ACCESS

Kaspersky Internet Security for Android protects your private data against unauthorized access using the following methods of protection:

- Specifying a secret code that prevents unauthorized access to Anti-Theft and Privacy Protection settings
- Configuring Anti-Theft settings

Anti-Theft is controlled by means of SMS commands and commands sent from the Web Management at https://anti-theft.kaspersky.com. Controlling the Anti-Theft functions from the Web Management requires creating an account at the Web Management.

To protect your data against unauthorized access, create an account at the Web Management to control the Anti-Theft component, specify a secret code to restrict access to app settings, and properly configure the device.

IN THIS SECTION

PURPOSE OF THE SECRET CODE

The secret code is requested in the following instances:

- To access Anti-Theft and Privacy Protection settings
- When sending an SMS command from another mobile device to remotely turn on the device alarm, lock the device, locate it on the map, wipe data, or hide confidential contacts and related information

You will be prompted to specify the secret code during initial configuration of Anti-Theft (see section "Performing initial configuration of Anti-Theft" on page 24) or at the first launch of Privacy Protection. You can later change the secret code installed.

The secret code is comprised of numerals. The minimum number of secret code characters is four.

If you forget the app secret code, you can restore it (see section "Recovering the app secret code" on page 41).

WHAT IS A KASPERSKY ACCOUNT

An account lets you use Web Management at https://anti-theft.kaspersky.com to remotely turn on the alarm on the device, lock the device, locate it on a map, wipe data, or secretly take the mugshot of the person who is using your device at the moment. You can also use Web Management to restore a forgotten secret code to Kaspersky Internet Security.

Kaspersky Account is a single account for accessing all Kaspersky Lab services. If you have a registered My Account or an account with Web Management at anti-theft.kaspersky.com, this means that you already have a Kaspersky Account.

You have to specify the account during initial configuration of Anti-Theft (see section "Performing initial configuration of Anti-Theft" on page 24). Your email address serves as your user name. If you have forgotten your account password when logging into the Web Management, you can restore it.

PERFORMING INITIAL CONFIGURATION OF ANTI-THEFT

Anti-Theft functions are disabled by default after the app has been installed: you cannot start them remotely via Web Management or SMS commands. To enable Anti-Theft functions, you have to perform initial configuration of Anti-Theft.

After initial configuration, all Anti-Theft functions will be enabled with the settings recommended by Kaspersky Lab specialists.

The Anti-Theft initial configuration wizard can be started only once. You can later configure Anti-Theft in app settings.

To perform initial configuration of Anti-Theft:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Anti-Theft**.

   This starts the Anti-Theft initial configuration wizard.

2. Follow the wizard's instructions.

To edit the Anti-Theft settings after initial configuration:

On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Theft**.

WHAT TO DO IF THE DEVICE IS LOST OR STOLEN

If the device has been lost or stolen, you can remotely hide contacts and related information as well as launch Anti-Theft functions: turn on the alarm, lock your device, remove data stored on it, get its location on the map, or secretly take the mugshot of the person currently using your device.

You can remotely activate Anti-Theft via Web Management at https://anti-theft.kaspersky.com or using special SMS commands sent from any device.

You can remotely hide contacts and related information only using a special SMS command.

You can hide contacts and related information only if the premium version of Kaspersky Internet Security for Android is activated on your device.

You can send a command to take the mugshot of the person currently using your device only via Web Management at https://anti-theft.kaspersky.com. This command cannot be sent via SMS.

The outgoing SMS message is billed at the rates of the mobile operator serving the device used to send the SMS command.

The remote start of Anti-Theft functions on the device is possible if the following conditions are met:

- Kaspersky Internet Security has been set as a Device Administrator;
- The device is picking up a mobile network signal;
- Anti-Theft and Privacy Protection functions are allowed on the device.

To remotely launch Anti-Theft via Web Management:

1. Open Web Management at https://anti-theft.kaspersky.com on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device for which you need to remotely launch the Anti-Theft functions.
4. In the sections in the upper part of Web Management window, selection the actions to be performed on the device.

To remotely hide contact information and start Anti-Theft functions using SMS commands, perform one of the following:

- If Kaspersky Internet Security is installed on another device, use it to create and send an SMS command to your device (see section "Sending SMS commands from Kaspersky Internet Security" on page 32).

  When creating the SMS command, use the secret code to Kaspersky Internet Security installed on your device.

- Send an SMS message to your device with the following special text:

  - hide: <code> – to hide confidential contacts and related information;
  - alarm: <code> – code for turning on the alarm and locking the device (where <code> is the secret code to Kaspersky Internet Security on your device);
  - find: <code> – to lock the device and get its coordinates;
  - wipe: <code> – to delete personal data and memory card data;
  - fullreset: <code> – to delete all data from the device and revert the device to factory settings

After all data has been removed and the device has been reset to factory settings, it will no longer be able to receive and perform remote commands.

DEALING WITH STANDARD TASKS

This section contains step-by-step instructions for carrying out the basic user tasks that the app deals with.

IN THIS SECTION

SCANNER (ANTI-VIRUS)

The component is called Scanner in the free version and Anti-Virus in the premium version.

Scanner (Anti-Virus) is designed to scan the device, detect and neutralize threats. Kaspersky Internet Security for Android allows performing a full or partial scan of the device included – i.e. scan the content of the device's built-in memory only or a specific folder (including that located on the storage card).

The app scans the device for malicious objects using the app anti-virus database with descriptions of all currently known malicious apps and other unwanted objects and the ways to neutralize them. It is extremely important to keep your anti-virus databases up-to-date. It is recommended to regularly update the application databases.

Kaspersky Internet Security for Android performs app database updates from Kaspersky Lab update servers. These are special Internet sites which contain updates for databases for all Kaspersky Lab products.

To update the app anti-virus databases, you must have an Internet connection configured on your device. Traffic at anti-virus databases update is billed according to your tariff

IN THIS SECTION

FULL SCAN OF THE DEVICE

A full scan of the entire device for viruses and other malware helps to protect your personal data and money, as well as detect and eliminate threats on your device (in both installed apps and installation packages).

The majority of malware threatens the user's personal data on the device; it collects the device owner's personal data and all the information on the device (for example, GPS coordinates and messages) and sends it to a malicious user.

It is recommended to scan the device entire file system for viruses at least once after installing the app, to ensure that personal data is protected.

- *To scan the device entire file system for viruses and other malware:*

  On the quick launch panel in the main window of Kaspersky Internet Security, tap **Scan** > **Full scan**.

QUICK SCAN

A quick scan can be used to scan installed apps only.

If you are using the free version, Kaspersky Lab recommends running a quick scan as soon as new apps have been installed.

- *To run a quick scan,*

  on the quick launch panel in the main window of Kaspersky Internet Security, tap **Scan** > **Quick scan**.

SCANNING FILES AND FOLDERS

You can scan a file or folder in the internal memory of the device or on the memory card.

- *To scan a folder or file:*

  1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Scan** > **Folder scan**.
  2. Select a folder or file to scan.

AUTOMATIC SCHEDULED SCAN

You can configure an automatic launch of a full scan of the device and create a schedule for its launch, choose how often the scan is to be launched, as well as the day and time of launch if necessary. The app will automatically scan the device entire file system according to the schedule.

For a full scan to launch automatically, the device needs to be switched on.

- *To configure automatic launching of a scheduled scan:*

  1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Virus** > **Scan Settings**.
  2. Configure the scan frequency. Do so by selecting a value for the **Schedule** setting.
  3. Set the day and time for the scan to start. To do so, select values for the **Start day** and **Start time** settings.

     Scans will be started according to schedule.

UPDATING ANTI-VIRUS DATABASES AND VERSION OF THE APP

Kaspersky Internet Security uses anti-virus databases when searching for malware. The anti-virus databases of the app contain descriptions of malware currently known to Kaspersky Lab and ways to neutralize it, as well as descriptions of other malicious objects. It is recommended to regularly update the databases.

As well as the anti-virus databases, Kaspersky Internet Security allows you to update the app version. Application version updates remove vulnerabilities from Kaspersky Internet Security, add new functions, or improve existing functions.

To update the app anti-virus databases, you must have an Internet connection configured on your device.

If you download Kaspersky Internet Security for Android from Google Play, the app updates anti-virus databases only. App version is updated via Google Play.

Updating the app anti-virus databases and version

On the quick launch panel in the main window of Kaspersky Internet Security, tap **Update**.

AUTOMATIC SCHEDULED UPDATES

You can configure the automatic updates of the app version and anti-virus databases (hereafter "update"). To do this, you can create a schedule for their launch: choose how often, as well as the day and time of launch if necessary. The app will automatically update its anti-virus databases and version according to the schedule.

Automatic updates are available only for the premium version of Kaspersky Internet Security.

An Internet connection is required for updates.

To automatically update at the chosen time, the device needs to be switched on at that time.

To configure a scheduled automatic update:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Virus** > **Update**.
2. Configure the update frequency. To do so, select a value for the **Schedule** setting.
3. Select a day and time for starting updates. To do so, select values for the **Start day** and **Start time** settings.

   Updates will be started according to schedule.

PRIVACY PROTECTION

You can hide your confidential contacts and all related call history and SMS correspondence using the Privacy Protection component.

Privacy Protection is available only for the premium version of Kaspersky Internet Security.

Privacy Protection supports the following functions:

- Maintains a list of confidential contacts, which includes contacts to be hidden;
- Hides phonebook entries, incoming text messages that have been read, outgoing text messages that have been sent, and text message drafts, as well as contact info in phone logs;
- Blocks incoming SMS notification signals and calls from confidential numbers (in this case the calling party hears the "busy" tone)

To view incoming calls and text messages for a period when Privacy Protection was enabled, Privacy Protection should be disabled. If you re-enable Privacy Protection, your confidential information is again hidden.

You can enable Privacy Protection from within the app, or remotely by sending an SMS command from another mobile device. You can send a standard SMS message with a special code or send an SMS message from Kaspersky Internet Security if the app is installed on the other device.

You can allow or block the remote launch of Privacy Protection on your device. If the remote start of Privacy Protection is blocked, the function cannot be launched remotely using an SMS command.

You can disable Privacy Protection only in the application installed on your device.

Access to Privacy Protection settings is protected with a secret code (see section "Purpose of the secret code" on page 24). The secret code is specified during initial configuration of Anti-Theft (see section "Performing initial configuration of Anti-Theft" on page 24) or when Privacy Protection is opened for the first time.

IN THIS SECTION

HIDING CONTACT-RELATED INFORMATION

To hide contacts and related information:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Privacy Protection**.
2. Enter the secret code.

   If you forget the app secret code, you can restore it (see section "Recovering the app secret code" on page 41).
3. Tap **Contacts to hide**.
4. To create a list of hidden contacts press **Add**.

   The list contains contacts whose details you want to hide. Skip this step if you have already created a list of contacts.
5. Toggle the **Privacy Protection** switch to **on**.

REMOTELY LAUNCHING PRIVACY PROTECTION FROM ANOTHER DEVICE

If necessary, you can hide contacts and related information on the device remotely. You can do so by sending a special SMS command from another device.

Remote launching of Privacy Protection function is possible if the following conditions are met:

- The premium version of the app is activated on the device receiving the SMS command;
- The device is picking up a mobile network signal;
- Remote launch of Privacy Protection is allowed on the device.

To launch Privacy Protection on your device remotely, perform one of the following operations:

- Create a command on another device and send it to your device from Kaspersky Internet Security using the SMS command function (if the app is installed on another device).
- On another device, create and send an SMS message with the text hide:<code>, where <code> is the secret code to Kaspersky Internet Security on your device.

You will receive a command execution report in the return SMS message.

Outgoing SMS commands are billed according to the price plan of the other mobile device.

ANTI-THEFT

Anti-Theft protects your data against unauthorized access and helps to locate the device if it gets lost or stolen.

You can remotely perform the following operations using Web Management at https://anti-theft.kaspersky.com or using special SMS commands:

- Lock the device and determine its location
- Turn on a loud alarm on the device
- Wipe data from the device
- Take a mugshot of the person currently using the device

Also, if the SIM card is replaced or the device is turned on without it, you can remotely lock the device and get the new phone number. This enables you to launch other Anti-Theft functions on the lost device.

IN THIS SECTION

ADDING A DEVICE TO WEB MANAGEMENT ACCOUNT

You can manage several devices at the same time through your Kaspersky Account with Web Management at https://anti-theft.kaspersky.com.

To add a device to your user account, enter your user account details during the initial configuration of Kaspersky Internet Security on the new device.

The new device will be associated automatically with your user account. Then, when you enter the Web Management, a new tab will appear with the name of the device.

SENDING SMS COMMANDS FROM KASPERSKY INTERNET SECURITY

If your device has been lost or stolen, you can remotely launch Anti-Theft or Privacy Protection functions on the device. To do so, send special commands to your device either via the Web Management at https://anti-theft.kaspersky.com or via SMS.

You can send a standard SMS with a special code from another device to your device (see section "What to do if the device is lost or stolen" on page 25). If Kaspersky Internet Security is installed on the other device, you can send an SMS command from the app. To send an SMS command, you need to know the secret code to Kaspersky Internet Security on your device.

Outgoing SMS commands are billed according to the price plan of the other mobile device.

To remotely launch Anti-Theft and Privacy Protection functions from a device with Kaspersky Internet Security installed:

1. Open Kaspersky Internet Security for Android on the other device.
2. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Theft**.
3. Enter the secret code.
4. If you forget the app secret code, you can restore it (see section "Recovering the app secret code" on page 41).
5. Tap **Sending SMS commands**.
6. Tap **Send SMS command**, form the command and send it to your device. When creating the SMS command, use the secret code to Kaspersky Internet Security installed on your device.

You will receive a command execution report in the return SMS message.

CONTROLLING THE SIM CARD REMOTELY

If the SIM card is replaced or the device is turned on without it, you can remotely lock the device and get the new phone number. This enables you to launch other Anti-Theft functions on the lost device.

You can get the new phone number via SMS or email. If this function is enabled, the app automatically locks the lost device when it is turned on without a SIM card. When the SIM card is replaced, the app automatically sends an SMS and email with the new phone number to the phone number and email address you specified.

To send an email message, the app sends an SMS to the dedicated number of the MTS mobile carrier (Russia). The MTS mobile carrier (Russia) sends the new phone number to your email address. The mobile account attached to the newly installed SMS card is billed for the SMS message sent to the dedicated number.

To enable SIM Watch, perform the following operations in advance:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Theft**.
2. Enter the secret code.
3. If you forget the app secret code, you can restore it (see section "Recovering the app secret code" on page 41).
4. Select the **SIM Watch** check box.
5. In the **Ways to receive new phone number and device location** section, fill the **Phone number** and **Email address** fields to receive the new phone number via SMS or email when your SIM card is replaced.
6. In the **Lock options** section select the **Lock when SIM card is replaced** check box to have the app lock the device when your SIM card is replaced or the device is switched on without it.

   If necessary, in the **Text when locked** field, enter the message to be displayed on the screen of the locked device.

LOCKING AND LOCATING THE DEVICE REMOTELY

If your device gets lost or stolen, you can lock the device and get the coordinates of its location via Web Management at https://anti-theft.kaspersky.com or the “find: <code>” SMS command (where <code> is the secret code to Kaspersky Internet Security on your device).

Outgoing SMS commands are billed according to the price plan of the other mobile device.

A device can be locked and located remotely when the following conditions are met:

- Kaspersky Internet Security for Android is installed as a Device Administrator;
- The device is picking up a mobile network signal;
- start of this function is allowed on the device.

Kaspersky Lab also recommends enabling GPS in your device settings so the app can determine the location of your device via GPS.

To lock the device and get its coordinates via Web Management:

1. Open Web Management at https://anti-theft.kaspersky.com on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device that you want to lock and locate.

4. Tap the **Lock & Locate** button.
5. If necessary, in the **Lock & Locate** section enter the text that you want to be displayed on the screen of the locked device. Also enter the email address where you would like to receive the device coordinates on the map.
6. Tap the **Lock & Locate** button.

When Kaspersky Internet Security for Android locates your device, you will see its coordinates in Web Management and receive them in your mailbox.

In Web Management, you can view only the most recently detected map location of the device. The previous GPS coordinates of the device remain in your mailbox and are removed from Web Management.

To lock your device and get its coordinates using an SMS command, perform one of the following:

- If Kaspersky Internet Security is installed on another device, use it to create and send an SMS command to your device (see section "Sending SMS commands from Kaspersky Internet Security" on page 32). When creating the SMS command, use the secret code to Kaspersky Internet Security installed on your device.
- Send an SMS message to your device with the following text: find: <code>, where <code> is the secret code to Kaspersky Internet Security on your device.

When Kaspersky Internet Security for Android locates your device, you will get its coordinates in the return SMS message and an email sent to the address you specified.

TURNING ON THE DEVICE ALARM REMOTELY

If your device gets lost or stolen, you can remotely turn on the device alarm (even if the device is muted) and lock the device via Web Management at https://anti-theft.kaspersky.com or the “alarm: <code>” SMS command (where <code> is the secret code to Kaspersky Internet Security on your device).

Outgoing SMS commands are billed according to the price plan of the other mobile device.

The remote launch of Alarm is possible if the device is picking up a mobile network signal, and the remote launch of this function is allowed on the device.

To turn on the alarm on the device and lock the device via Web Management:

1. Open Web Management at https://anti-theft.kaspersky.com on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device where you want to turn on the alarm and lock the device.
4. Tap the **Alarm** button.
5. If necessary, in the **Alarm** section enter the text that you want to be displayed on the screen of the locked device.
6. Tap the **Turn on Alarm** button.

To turn on the device alarm an lock the device using an SMS command, perform one of the following:

- If Kaspersky Internet Security is installed on another device, use it to create and send an SMS command to your device (see section "Sending SMS commands from Kaspersky Internet Security" on page 32). When creating the SMS command, use the secret code to Kaspersky Internet Security installed on your device.
- Send an SMS message to your device with the following text: alarm: <code>, where <code> is the secret code to Kaspersky Internet Security on your device.

You will receive a command execution report in the return SMS message.

REMOTELY WIPING DATA FROM THE DEVICE

If your device gets lost or stolen, you can remotely wipe device data via Web Management at https://anti-theft.kaspersky.com or by means of SMS commands.

You can delete the following information:

- personal data (for example, contacts, correspondence and Google™ account data) and memory card data;
- all data, including memory card data (resetting the device to factory settings).

Outgoing SMS commands are billed according to the price plan of the other mobile device.

Data can be wiped remotely if the following conditions are met:

- Kaspersky Internet Security for Android is installed as a Device Administrator;
- The device is picking up a mobile network signal;
- start of this function is allowed on the device.

To remotely wipe the data from the device via Web Management:

1. Open Web Management at https://anti-theft.kaspersky.com on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device from which you want to delete data.
4. Tap the **Data Wipe** button.
5. In the **Data Wipe** section, select the data that you want to delete from the device.
   - To delete personal data (for example, Google account data, contacts and correspondence) and to format the memory card, select **Only personal data**.
   - To delete all data including data on the memory card and revert the device to factory settings, select **All data from your device**.

   After all data has been wiped from the device, Kaspersky Internet Security for Android is also removed. The device will no longer be able to execute remote commands.
6. Press the **Wipe** button.

To wipe data from your device remotely using an SMS command, perform one of the following:

- If Kaspersky Internet Security is installed on another device, use it to create and send an SMS command to your device (see section "Sending SMS commands from Kaspersky Internet Security " on page 32). You may choose to wipe personal data or all data. When creating the SMS command, use the secret code to Kaspersky Internet Security installed on your device.
- Send an SMS message to your device with the following special text:
  - wipe: <code> – to delete personal data and data stored on memory card;
  - fullreset: <code> – to delete all data from the device and reset the device to factory defaults.

    <Code> – this is the secret code to Kaspersky Internet Security on your device.

You will receive a command execution report in the return SMS message.

TAKING A MUGSHOT

If your device gets lost or stolen, you take a mugshot of the person who is using your device and lock the device and via Web Management at https://anti-theft.kaspersky.com.

The mugshot function is supported if your device has a front camera. This function can be started via Web Management only. It cannot be started via an SMS command.

Remote launching of the Anti-Theft functions is possible if the following conditions are fulfilled:

- Kaspersky Internet Security has been set as a Device Administrator;
- The device is picking up a mobile network signal;
- remote launch of this function is allowed on the device.

To obtain photographs of the person who is currently using your device:

1. Open Web Management at https://anti-theft.kaspersky.com on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device where you want to launch the Mugshot function and lock the device.
4. Press the **Mugshot** button.
5. If necessary, in the **Mugshot** section enter the text that you want to be displayed on the screen of the locked device.
6. Tap the **Get mugshot** button.

When Kaspersky Internet Security for Android performs the command, the mugshot is uploaded to the Web Management. You can resend the command after getting the mugshot.

CALL&TEXT FILTER

Call&Text Filter is available only on devices with an inserted SIM card.

Call & Text Filter allows you to block unsolicited incoming calls and text messages. The app filters calls and text messages based on the lists of allowed and blocked contacts and in accordance with the selected filter mode.

IN THIS SECTION

STANDARD FILTERING OF CONTACTS

Use standard filtering mode to receive calls and text messages from allowed contacts and block calls and text messages from blocked contacts.

If you receive a call or text message from a contact who is not on the lists of allowed and blocked contacts, the app prompts you to choose an action to take on the call or text message from this contact. The app will subsequently process calls and text messages from this contact automatically according to your choice.

To enable standard filtering mode:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Call&Text Filter mode** > **Standard**.
2. Create a list of blocked contacts. To this end, on the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Blocked contacts**.
3. Create a list of allowed contacts. To this end, on the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Allowed contacts**.
4. If necessary, enable additional filtering settings. To this end, on the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Call&Text Filter**.

   To allow calls and text messages from all contacts in the device phonebook, select the **Allow Contacts** check box.

   To block text messages from phone numbers that contain letters, select the **Block non-numeric numbers** check box.

BLOCKING ALL CONTACTS EXCEPT ALLOWED ONES

To block calls and text messages from all contacts except allowed ones, use filtering in allowed contacts mode.

To enable filtering in allowed contacts mode:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Call&Text Filter mode** > **Allowed contacts**.
2. Create a list of allowed contacts. To this end, on the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Allowed contacts**.
3. If necessary, allow calls and text messages from contacts in the device phonebook:
   a. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Call&Text Filter**.
   b. Select the **Allow Contacts** check box.

BLOCKING BLOCKED CONTACTS ONLY

To block calls and text messages from blocked contacts only, use filtering in blocked contacts mode.

To enable filtering in blocked contacts mode:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Call&Text Filter mode** > **Blocked contacts**.
2. Create a list of blocked contacts. To this end, on the quick launch panel in the main window of Kaspersky Internet Security, tap **Call&Text Filter** > **Blocked contacts**.

3. If necessary, enable automatic blocking of text messages from numbers containing letters:

   a. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Call&Text Filter**.

   b. Select the **Block non-numeric numbers** check box.

WEB PROTECTION AND TEXT ANTI-PHISHING

With Web Protection and Text Anti-Phishing, you can visit trusted websites and use personal data on the network safely.

Web Protection and Text Anti-Phishing are available only for the premium version of Kaspersky Internet Security.

The Text Anti-Phishing is available only on devices with an inserted SIM card.

Web Protection blocks malicious websites, which aim to distribute malicious code, and fake (phishing) websites, which aim to steal your confidential data and gain access to your financial accounts.

Text Anti-Phishing blocks SMS links to malicious or phishing websites.

Web Protection checks websites before they are opened. Text Anti-Phishing also checks links in SMS messages before they are opened. Web Protection and Text Anti-Phishing perform checks using the Kaspersky Security Network cloud service (a dedicated Kaspersky Lab online service that contains information about the reliability of files, apps, and web resources).

IN THIS SECTION

CONSTANT SCANNING OF WEBSITES

Web Protection only checks websites in the standard Android browser and does not check them in other browsers. To use Web Protection at all times while browsing the web, set the standard Android browser as the default browser.

To enable real-time scanning of websites:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Web Protection**.
2. Flip the **Web Protection** toggle switch to **On**.
3. Tap **Change browser** (this button is displayed if Web Protection is enabled and the standard Android browser is not set as the default browser).

   The default browser selection wizard starts.
4. Follow the wizard's instructions.

   When the wizard finishes, the standard Android browser is set as the default browser.

CONSTANT SCANNING OF SMS LINKS

The Text Anti-Phishing is available only on devices with an inserted SIM card.

To enable the scanning of SMS links:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Web Protection**.
2. Flip the **Text Anti-Phishing** toggle switch to **On**.

OTHER TASKS

You also can do the following:

- activate the premium version of the app;
- purchase a license or renew an existing license;
- view information about the license;
- view reports on the operation of the app (for example, reports on scans performed, threats detected, SMS messages, calls or websites blocked);
- change the app secret code;
- restore the app secret code.

IN THIS SECTION

PURCHASING A LICENSE ONLINE AND RENEWING A LICENSE

If you choose to use the premium version of Kaspersky Internet Security, you can purchase a license for the app in the Kaspersky Lab eStore or from partner companies. When you buy a license, you get an activation code that you have to use to activate the premium version of the app.

When the license is due to expire, you can renew it. You can do so by either buying a new license from an online store or using an activation code (see section "About the activation code" on page 21) for a previously purchased license.

When the license expires, the app automatically switches to the free version.

- *To purchase a license from an online store:*

  1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Additional settings** > **Licensing**.
  2. Select **Purchase license**.
  3. Press **Open**.

     The web page of the online store opens, where you are able to purchase a new license.

- *To renew the license with the activation code:*

  1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Additional settings** > **Licensing**.
  2. Select **Enter activation code**.
  3. Enter an activation code for a previously purchased license.

ACTIVATING THE PREMIUM VERSION OF THE APP

To use all functions of the app, you need to activate the premium version of Kaspersky Internet Security.

Activation – is switching the app into full-function mode. To activate the app, you have to enter the activation code that you received when purchasing the app, or purchase a license from an online store.

You can activate the premium version of the app at first startup or at any other time.

To activate the premium version, you have to enter the activation code (see section "About the activation code" on page 21) received with the license or buy a license from an online store (see section "Buying or renewing a license" on page 39).

You will need a working Internet connection to activate the app.

- *To activate the premium version of the application with the activation code:*

  1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Additional settings** > **Licensing** > **Enter activation code**.
  2. Enter the activation code in the window that opens and tap **Activate**.

     The app sends an activation request to the Kaspersky Lab activation server. On receiving successful confirmation of the request, the app will notify you and display the license information.

VIEWING INFORMATION ABOUT THE LICENSE AND ITS VALIDITY PERIOD

You can view the key number, license validity period, and other information about the license.

License information can be viewed when you use a trial or premium version of the app.

- *To check the license term, and to view license information:*

  On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Licensing** > **About license**.

VIEWING APP OPERATION REPORTS

Scanner (Anti-Virus), Web Protection, and Call&Text Filter events are logged in reports.

Reports are grouped by time of creation. You can choose to display reports for each component separately. Reports can contain up to 50 entries. Once the number of entires exceeds 50, older entries are deleted and replaced by new ones.

To view app operation reports:

On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Reports**.

CHANGING THE SECRET CODE

The app prompts you to specify the secret code during initial configuration of Anti-Theft (see section "Performing initial configuration of Anti-Theft" on page 24) or at the first launch of Privacy Protection. You can change the secret code at any time.

To change the secret code:

1. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Additional settings** > **Change secret code**.
2. Enter the current secret code in the **Enter current secret code** field and tap **Next**.
3. Enter a new secret code in the **Create a new secret code** field and tap **Next**.
4. Re-enter the new code in the **Re-enter the new code** field and tap **Enter**.

SECRET CODE RECOVERY

To safely recover the secret code to the app:

1. Open the https://anti-theft.kaspersky.com website on any device.
2. Sign in to Web Management with your Kaspersky Account that you used during initial configuration of the app.

   If you have forgotten your password, you can recover it.
3. Select the tab with the name of the device for which you need to recover the secret code.
4. Press the **Recovery of secret code** button.

   The recovery code is displayed in Web Management.
5. Launch Kaspersky Internet Security for Android on the device.
6. On the quick launch panel in the main window of Kaspersky Internet Security, tap **Settings** > **Anti-Theft**.
7. When prompted to enter the secret code, tap **Menu** > **Recovery of secret code**.
8. Enter the recovery code displayed in Web Management.

   Your secret code appears on the device screen.
9. Enter your recovered secret code.

CONTACTING THE TECHNICAL SUPPORT SERVICE

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION

OBTAINING TECHNICAL SUPPORT

If you have not found a solution to your problem in the app documentation or in one of information sources about the app (see the Information sources about the app section on page 8), we recommend to contacting the Kaspersky Lab Technical Support service. Technical Support Service specialists will answer any of your questions about installing and using the application.

Before contacting the Technical Support Service, please read the technical support rules (http://support.kaspersky.com/support/rules).

You can contact the Technical Support Service in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a query from your Kaspersky Account on the Technical Support Service website. This method allows you to contact Technical Support specialists through a request form.

Technical support is only provided to users who have purchased a license to use the app. Technical support is not provided to users of trial versions.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support by phone (http://support2.kaspersky.com/us/support/contacts).

Before contacting Technical Support, please read the support rules (http://support.kaspersky.com/support/rules). This will enable our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA MY KASPERSKY ACCOUNT

My Kaspersky Account is your personal area (https://my.kaspersky.com) on the Technical Support Service website.

To gain access to My Kaspersky Account, you should follow the registration procedure on the registration page (https://my.kaspersky.com/registration). Enter your email address and a password to log in to My Kaspersky Account.

In My Kaspersky Account, you can perform the following actions:

- Send requests to Technical Support Service and Anti-Virus Lab;
- contact the Technical Support Service without using email;
- track the status of your request in real time;
- view a detailed history of your requests to the Technical Support Service;
- receive a copy of the key file if it has been lost or removed.

E-mailing your question to the Technical Support Service

You can send an online request to the Technical Support Service in Russian, English, German, French, or Spanish.

You should specify the following data in the fields of the online request form:

- request type;
- application name and version number;
- request description;
- customer ID and password;
- email address.

A specialist from the Technical Support Service sends an answer to your question to your My Kaspersky Account and to the email address that you have specified in your online request.

Electronic request to the Anti-Virus Laboratory

Some requests are to be sent to the Anti-Virus Laboratory and not to the Technical Support service.

You can send the following types of requests to the Anti-Virus Laboratory:

- *Unknown malicious program* – you suspect that a file contains a virus but Kaspersky Internet Security for Android has not identified it as infected.

  Specialists of Anti-Virus Laboratory analyze received malicious code and in case the unknown virus is detected, add its description to the database available for updating the Anti-Virus software.

- *False alarm* – Kaspersky Internet Security for Android classifies the file as a virus, yet you are sure that the file is not a virus.

- *Request for description of malicious program* – you want to receive the description of a virus detected by Kaspersky Internet Security, using the name of the virus.

You can also send requests to the Anti-Virus Lab from the page with the request form (http://support.kaspersky.com/virlab/helpdesk.html) without registering in My Kaspersky Account. On this page, you do not have to specify the application activation code.

GLOSSARY

A

ACTIVATING THE APP

Switching the application into full-function mode. Activation is carried out by the user before or after the application installation. To activate the app, you have to enter the activation code that you received with the app, or purchase a license from an online store.

ACTIVATION CODE

A code that you receive when buying a license for Kaspersky Internet Security. This code is required for activation of the application.

The activation code is an alphanumeric string of Latin characters in xxxxx-xxxxx-xxxxx-xxxxx format.

ANTI-VIRUS DATABASES

Databases that contain information about computer security threats that are known to Kaspersky Lab at the time of release of the databases. Records in databases allow detecting malicious code in objects being scanned. Databases are compiled by Kaspersky Lab specialists and updated hourly.

APP SECRET CODE

The secret code is requested in the following instances:

To access Anti-Theft and Privacy Protection settings

When sending an SMS command from another mobile device to remotely turn on the device alarm, lock the device, locate it on the map, wipe data, or hide confidential contacts and related information

ARCHIVE

One or several files packed into a single compressed file. A special app named archiver is required to pack or unpack data.

D

DELETION OF AN OBJECT

A method of processing objects that involves physically removing them from their original location. You are advised to apply this processing method to any malicious objects which cannot be disinfected.

DISINFECTING OBJECTS

A method of processing infected objects that results in full or partial data recovery. Not any infected object can be disinfected.

I

INFECTED OBJECT

An object a segment of whose code fully matches a code segment of a known threat. Kaspersky Lab does not recommend using such objects.

K

KASPERSKY SECURITY NETWORK (KSN)

Infrastructure of online services providing access to the current knowledge base of Kaspersky Lab describing the reputation of files, web sites and software. The use of data from Kaspersky Security Network ensures faster response by Kaspersky Lab applications to unknown threats, improves the effectiveness of some protection components, and reduces the risk of false positives.

L

LICENSE TERM

License term is a time period during which you have access to the app features and rights to use additional services. The services you can use depend on the type of the license.

LIST OF ALLOWED CONTACTS

The list of allowed contacts contains contacts from which you want to receive incoming messages.

The entries in this list contain the following information:

Phone number from which Call & Text Filter delivers calls and / or SMS.

Type of events that Call & Text Filter delivers from this number. The following types of events are available: calls and SMS, calls only, and SMS only.

Key phrase used by Call & Text Filter to classify an SMS as solicited (not spam). Call & Text Filter only delivers SMS containing the key phrase, while blocking all other SMS.

LIST OF BLOCKED CONTACTS

The list of blocked contacts contains contacts from which you do not want to receive incoming messages.

Entries in this list contain the following information:

Phone number from which Call & Text Filter blocks calls and (or) SMS.

Types of events that Call & Text Filter blocks from this number. The following types of events are available: calls and SMS, calls only, and SMS only.

Key phrase that Call & Text Filter uses to classify an SMS as unsolicited (spam). Call & Text Filter only blocks SMS containing the key phrase, while delivering all other SMS.

N

NON-NUMERIC NUMBER

A phone number that includes letters or consists only of letters.

U

UPDATING DATABASES

One of the functions that Kaspersky Lab app performs which keeps protection up to date. Anti-virus databases are copied from Kaspersky Lab update servers onto the device and the app is automatically connected to them.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab entered the Top-4 world leading vendors of software solutions for endpoint data protection (according to the rating by "IDC Worldwide Endpoint Security Revenue by Vendor"). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today Kaspersky Lab is an international group of companies headquartered in Moscow and running five regional divisions that manage the company's activities in Russia, Western and Eastern Europe, the Middle East, Africa, Northern and Southern America, Japan, China, and other countries of the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab products protect both home computers and enterprise networks.

The range of personal products includes anti-virus applications for desktop, laptop, and pocket computers, for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab products are certified by the major test laboratories, are compatible with the software of many vendors, and are optimized to run on many hardware platforms.

Kaspersky Lab virus analysts work 24/7. Every day they find hundreds of new computer threats, create tools for detecting and neutralizing them, and add them to databases used by Kaspersky Lab applications. *The anti-virus database of Kaspersky Lab is updated hourly*, *the Anti-Spam database is updated every 5 minutes*.

Technologies. Many technologies that are now part of modern anti-virus tools were originally developed by Kaspersky Lab. It is therefore logical for many third-party software developers to use the kernel of Kaspersky Anti-Virus in their own applications. Those companies include SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), and ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years at war with computer threats Kaspersky Lab has earned hundreds of awards. In 2010, Kaspersky Anti-Virus received several highest awards Advanced + after the tests carried out by AV-Comparatives, an authoritative Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:	http://www.kaspersky.com
Virus encyclopedia:	http://www.securelist.com
Anti-virus laboratory:	newvirus@kaspersky.com (to send probably infected files in the archived form only)
	http://support.kaspersky.com/virlab/helpdesk.html
	(for queries addressed to virus analysts)
Kaspersky Lab's web forum:	http://forum.kaspersky.com

INFORMATION ABOUT THIRD PARTY CODE

Information about third-party code is contained in the **About** block, which is located in the application settings.

TRADEMARK NOTIFICATIONS

Registered trade and service marks are the property of their respective owners.

Android and Google are trademarks of Google, Inc.

INDEX

R

S

U