

# Kaspersky Internet Security for Mac



## User Guide

APPLICATION VERSION: 15.0 MAINTENANCE RELEASE 1

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

Attention! This document is the property of Kaspersky Lab and all rights to this document are reserved by the copyright laws of the Russian Federation and international treaties. Illegal reproduction and distribution of this document or parts hereof will result in civil, administrative or criminal liability by applicable law.

Any type of reproduction and distribution of any materials, including translation thereof, is allowed only with the written permission of Kaspersky Lab.

This document and graphic images related to it can be used exclusively for information, non-commercial or personal purposes.

Kaspersky Lab reserves the right to change the document at any time without notice. You can find the latest version of this document at the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document for which the rights are held by third parties, or for any potential damages associated with the use of such documents.

Document revision date: 2/10/2015

© 2015 Kaspersky Lab ZAO. All Rights Reserved.

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

# CONTENT

ABOUT THIS GUIDE .....	6
In this document.....	6
Document conventions .....	8
SOURCES OF INFORMATION ABOUT THE APPLICATION.....	9
Sources of information to research on your own .....	9
Discussing Kaspersky Lab applications on the Forum.....	10
KASPERSKY INTERNET SECURITY .....	11
About Kaspersky Internet Security .....	11
Distribution kit .....	12
User service.....	13
Hardware and software requirements.....	13
INSTALLING AND UNINSTALLING THE APPLICATION .....	14
Preparing for installation .....	14
Installing the application .....	14
Installing the application downloaded from My Kaspersky portal .....	15
About the account for signing in to My Kaspersky portal.....	16
About My Kaspersky portal .....	16
Installing the application from the distribution kit.....	17
Preparing the application for use.....	18
Uninstalling the application .....	18
APPLICATION INTERFACE .....	19
Kaspersky Internet Security icon.....	19
Main application window.....	20
Application preferences window.....	21
Parental Control preferences window.....	22
Safe Money window .....	22
Notification windows and pop-up messages .....	23
About notification windows .....	23
About event types .....	23
About pop-up messages .....	24
Disabling notifications .....	24
News Agent .....	24
APPLICATION LICENSING .....	25
About the End User License Agreement.....	25
About the license.....	25
About subscription.....	26
About the activation code .....	27
About the key .....	27
About data submission .....	27
Viewing license information .....	31
Purchasing a license .....	32
Renewing a license .....	32
Renewing subscription .....	32
Updating subscription status.....	33

Activating Kaspersky Internet Security .....	33
Activating the trial version of the application.....	34
Activating the application with an activation code .....	34
Activating the application using a Kaspersky Small Office Security activation code.....	35
About participation in Kaspersky Security Network.....	36
STARTING AND STOPPING THE APPLICATION.....	37
COMPUTER PROTECTION STATUS.....	38
Assessing the status of computer protection.....	38
Disabling computer protection.....	38
Resuming computer protection .....	39
Using Protection Center.....	40
PERFORMING COMMON TASKS .....	41
Performing a full scan of the computer for viruses .....	41
Performing a quick scan of the computer.....	42
Scanning a file, folder or disk for viruses .....	42
Purchasing a license .....	42
Renewing a license .....	43
Updating application databases .....	43
Preventing interception of data entered using the hardware keyboard .....	44
Protecting financial transactions or purchases on the website of a bank, payment system, or online store.....	44
Limiting Internet use time for a child or teenager.....	45
Restricting website visits and file downloads for a child or teenager .....	46
Restricting contacts and messaging on social networks for a child or teenager .....	46
Blocking transmission of personal data by a child or teenager.....	47
What to do if file access is blocked.....	47
Restoring a file that has been deleted or disinfected by the application.....	48
Viewing the report on the application's operation .....	49
What to do if notification windows or pop-up messages appear.....	49
MANAGING THE APPLICATION FROM THE COMMAND LINE .....	50
Viewing Help.....	51
Virus Scan .....	51
Updating the application .....	53
Rolling back the last update.....	53
Starting / stopping a protection component or task.....	54
Component or task operation statistics.....	55
Exporting protection preferences .....	55
Importing protection preferences.....	55
Closing the application .....	56
Return codes of the command line.....	56
CONTACTING TECHNICAL SUPPORT .....	57
Ways to receive technical support.....	57
Technical support by phone.....	57
Contacting Technical Support from My Kaspersky Portal .....	58
Using a trace file .....	58
Creating a trace file .....	59
Sending files with error information to Kaspersky Lab .....	59

GLOSSARY .....	60
KASPERSKY LAB ZAO .....	62
INFORMATION ABOUT THIRD-PARTY CODE .....	63
TRADEMARK NOTICES.....	64
INDEX.....	65

# ABOUT THIS GUIDE

This document is the User Guide for Kaspersky Internet Security for Mac.

For proper use of Kaspersky Internet Security users should be acquainted with the interface of the Mac OS X operating system, master basic OS X skills, and know how to use email and the Internet.

This guide is intended to:

- Help you install, activate, and use Kaspersky Internet Security.
- Ensure quick search of information on issues related to Kaspersky Internet Security.
- Describe additional sources of information about the application and ways of contacting Technical Support.

## IN THIS SECTION:

---

In this document .....	<a href="#">6</a>
Document conventions .....	<a href="#">8</a>

## IN THIS DOCUMENT

The Kaspersky Internet Security User Guide is comprised of the following sections:

### Sources of information about the application (see page [9](#))

This section lists the sources of information about the application.

### Kaspersky Internet Security (see page [11](#))

This section describes the functions, components, and distribution kit of Kaspersky Internet Security, and provides a list of hardware and software requirements of Kaspersky Internet Security and user service information.

### Installing and uninstalling the application (see page [14](#))

This section provides step-by-step instructions on how to install and uninstall Kaspersky Internet Security.

### Application interface (see page [19](#))

This section describes the basic GUI components of Kaspersky Internet Security: application icon and context menu of the application icon, main application window and application preferences window, Parental Control window, Safe Money window, and News Agent window. This section also describes notification windows and pop-up messages of the application.

### Application licensing (see page [25](#))

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the ways to activate the application and renew the license.

**Starting and stopping the application (see page [37](#))**

This section provides you with information on how to start the application and quit it.

**Computer protection status (see page [38](#))**

This section provides information on how to determine whether or not computer security threats or problems exist and how to configure the security level. Read this section to learn more about how to enable and disable protection when using the application.

**Solving typical tasks (see page [41](#))**

This section contains step-by-step instructions for performing common user tasks with the application.

**Working with the application from the command line (see page [50](#))**

This section describes how to manage Kaspersky Internet Security from the command line.

**Contacting Technical Support (see page [57](#))**

This section describes the ways to get technical support and the terms on which it is available.

**Glossary**

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

**Kaspersky Lab ZAO (see page [62](#))**

This section provides information about Kaspersky Lab.

**Information about third-party code (see page [63](#))**

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

**Trademark notices (see page [64](#))**

This section lists trademarks of third-party right holders used in this document.

**Index**

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

# DOCUMENT CONVENTIONS

This document uses the following conventions (see table below).

Table 1. Document conventions

SAMPLE TEXT	DOCUMENT CONVENTIONS DESCRIPTION
Please note that...	Warnings are highlighted with red color and boxed. Warnings show information about actions that may have unwanted consequences.
It is recommended to use...	Notes are boxed. Notes provide additional and reference information.
<b>Example:</b> ...	Examples are set out on a yellow background under the heading "Example".
Update means... The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none"> <li>new terms;</li> <li>names of application statuses and events.</li> </ul>
<b>Command-A.</b>	The names of keys appear in a bold typeface. Key names joined by a - (minus) sign represent key combinations.
Click the <b>Enable</b> button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and accompanied by the arrow sign.
kav update	The following types of text content are set off with a special font: <ul style="list-style-type: none"> <li>text in the command line;</li> <li>text of messages displayed on the screen by the application;</li> <li>Data to be entered using the keyboard.</li> </ul>
<IP address of your computer>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.



# SOURCES OF INFORMATION ABOUT THE APPLICATION

This section lists the sources of information about the application.

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

## IN THIS SECTION:

Sources of information to research on your own .....	<a href="#">9</a>
Discussing Kaspersky Lab applications on the Forum .....	<a href="#">10</a>

## SOURCES OF INFORMATION TO RESEARCH ON YOUR OWN

You can use the following sources of information to research on your own:

- Kaspersky Internet Security page on the Kaspersky Lab website
- Kaspersky Internet Security page on the Technical Support website (Knowledge Base)
- Online help

If you cannot find a solution to your problem, we recommend that you contact Kaspersky Lab Technical Support. To use information sources on the website of Kaspersky Lab, an Internet connection is required.

### Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page devoted to each application.

On the Kaspersky Internet Security page on the Kaspersky Lab website (<http://www.kaspersky.com/security-mac>), you can view general information about the application, its functions and features.


The page <http://www.kaspersky.com> contains a link to the online store. Here you can purchase the application or renew your license.

### Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. The Knowledge Base contains reference articles that are grouped by topic.

On the page of the application in the Knowledge Base (<http://support.kaspersky.com/kis15mac>), you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

The articles may provide answers to questions that are related not only to Kaspersky Internet Security but also to other Kaspersky Lab products, or may contain Technical Support news.

To switch to the Knowledge Base, open the main application window (on page [20](#)), click the  button and click the **Technical Support** button in the window that opens.

## Online help

The online help of the application comprises context help files.


The context help provides information about each window and tab of Kaspersky Internet Security: a list of parameters with descriptions and a list of tasks being solved.

## DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an immediate answer, you can discuss it with Kaspersky Lab experts and other users on our forum (<http://forum.kaspersky.com/index.php?showforum=117>).

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

➡ *To go to the forum:*

1. Open the main application window (on page [20](#)).
2. In the main application window click the button .
3. In the window that opens, click the **Forum** button.

# KASPERSKY INTERNET SECURITY

This section describes the functions, components, and distribution kit of Kaspersky Internet Security, and provides a list of hardware and software requirements of Kaspersky Internet Security and user service information.

## IN THIS SECTION:

---

About Kaspersky Internet Security.....	<a href="#">11</a>
Distribution kit.....	<a href="#">12</a>
User service .....	<a href="#">13</a>
Hardware and software requirements .....	<a href="#">13</a>

## ABOUT KASPERSKY INTERNET SECURITY

Kaspersky Internet Security for Mac is intended for use on computers that run on Mac OS X, to protect your Mac against viruses and other computer security threats.

The application includes the following components:

### File Anti-Virus

The File Anti-Virus component protects the file system of the computer in real time: intercepts and analyzes attempts to access files. You can configure the actions to be performed by the application on infected and probably infected files. By default, Kaspersky Internet Security displays a notification window prompting you to select an action to take on the object detected.

### Web Anti-Virus

The Web Anti-Virus component protects information that is sent and received by your computer over the HTTP and HTTPS protocols in Safari, Google Chrome™ or Firefox™ browsers. This component includes web browser extensions that you can install: Kaspersky URL Advisor and Virtual Keyboard. Kaspersky URL Advisor scans links in open websites for phishing threats and malicious web addresses. Virtual Keyboard protects data input against interception.

### Network Attack Blocker

The Network Attack Blocker component protects the computer against intrusions into the operating system. This component provides protection against malicious activity of criminals themselves (such as port scanning and brute force attacks) and activity of malware installed by criminals on the computer under attack (such as transmission of sensitive information to criminals).

### Parental Control

The Parental Control component monitors the activity of different users on the computer and on the Internet. The component lets you limit Internet usage time for each user, restrict access to web resources and applications, create lists of contacts blocked or allowed for messaging over social networks, and monitor transmission of specific personal data. The Parental Control component also allows viewing user activity reports.

## Safe Money

The Safe Money component protects payment data and financial transactions as you visit websites of banks, payment systems, and online stores with integrated payment systems, that is, online stores where you enter bank card data. The Safe Money component authenticates websites of banks, payment systems, and online stores and checks certificates used to establish the secure connection based on data from Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page [36](#)).

The following functions are implemented in the application:

## Virus Scan

Kaspersky Internet Security detects and neutralizes viruses and other computer security threats on demand in the specified scan scope. You can configure the actions to be performed by the application on infected and probably infected files. By default, Kaspersky Internet Security displays a notification window prompting you to select an action to take on the object detected. Kaspersky Internet Security runs a full scan of the computer, a quick scan of critical areas of the computer, and a scan of the specified scan scope.

## Update

Kaspersky Internet Security updates anti-virus databases from Kaspersky Lab update servers and creates backup copies of all updated files to allow a rollback of the last update. The application can also download and install new versions of Kaspersky Internet Security automatically.

## Quarantine

Kaspersky Internet Security creates a copy of the infected file in Quarantine prior to attempting to disinfect or delete the file, so you can restore it.

## Reports

Kaspersky Internet Security generates a report on the operation of application components.

## Notifications

Kaspersky Internet Security notifies the user about certain events in the operation of Kaspersky Internet Security using notification windows and pop-up messages. Notification windows can be accompanied by sound alerts.

## Protection Center

Kaspersky Internet Security displays protection status messages in the Protection Center window during its operation. Protection Center shows information on the current status of computer protection and lets you proceed to eliminating computer security problems and threats.

## Remote management via My Kaspersky portal

My Kaspersky portal lets you remotely manage protection of computers with Kaspersky Total Security installed: receive information on the current status of computer protection and remotely fix issues and respond to computer security threats, enable or disable protection components (File Anti-Virus, Web Anti-Virus, Network Attack Blocker), run virus scan tasks, update application databases, and manage Kaspersky Internet Security licenses.

# DISTRIBUTION KIT

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

- Boxed. Distributed via stores of our partners.
- At the online store. Distributed at online stores of Kaspersky Lab (for example, <http://www.kaspersky.com>, section eStore) or via partner companies.

If you purchase the boxed version of the application, the distribution package contains the following items:

- A brief user guide with instructions on downloading and installing the application, along with the application activation code.
- End User License Agreement that stipulates the terms, on which you can use the application.

The contents of the distribution package may vary with the region in which the application is distributed.

If you purchase Kaspersky Internet Security at an online store, you download the application from the website of the store. Information needed to activate the application, including the activation code, will be emailed to you when you complete payment.

If you purchase Kaspersky Internet Security on My Kaspersky portal, you download the latest version of the application from My Kaspersky portal. Information required to activate the application, including the activation code, is displayed on the web page of My Kaspersky portal and sent to your email address after you complete your purchase. You can also download an application version with a preset activation code from My Kaspersky portal.

## USER SERVICE

By purchasing a license for the application, you can benefit from the following services during the entire term of the license:

- Database updates and new versions of the application
- Support on issues related to the installation, configuration and use of the application by phone or via email
- Announcements of new Kaspersky Lab releases and information about new viruses and outbreaks To use this service, you should be subscribed to the news delivery from Kaspersky Lab on the Technical Support website.

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

## HARDWARE AND SOFTWARE REQUIREMENTS

Kaspersky Internet Security has the following hardware and software requirements:

- Mac OS X 10.7, OS X 10.8, 10.9, 10.10 operating system.
- 550 MB free disk space (depending on the anti-virus databases size).

# INSTALLING AND UNINSTALLING THE APPLICATION

This section provides step-by-step instructions on how to install and uninstall Kaspersky Internet Security.

The Kaspersky Internet Security distribution package includes the Installer and the Uninstaller.

## IN THIS SECTION:

Preparing for installation .....	<a href="#">14</a>
Installing the application.....	<a href="#">14</a>
Preparing the application for use .....	<a href="#">18</a>
Uninstalling the application.....	<a href="#">18</a>

## PREPARING FOR INSTALLATION

Before installing Kaspersky Internet Security on your computer, we recommend that you take these preparatory steps:

- Make sure that your computer meets the hardware and software requirements (see section "Hardware and software requirements" on page [13](#)).
- Check the Internet connection on your computer. Internet access is required to log in to My Kaspersky portal (see section "About My Kaspersky portal" on page [16](#)), download a new version of Kaspersky Internet Security to the computer, activate the application using the activation code, and receive updates.
- Remove any other anti-virus applications to avoid system conflicts and maximize system performance.

## INSTALLING THE APPLICATION

Kaspersky Lab experts recommend installing Kaspersky Internet Security only in ways described in this guide.

The following methods of installation are available:

- Installing the application downloaded from My Kaspersky portal (see section "Installing the application downloaded from My Kaspersky portal" on page [15](#)).

This is performed using the account for signing in to My Kaspersky portal (see section "About the account for signing in to My Kaspersky portal" on page [16](#)). It lets you download a new version of Kaspersky Internet Security from My Kaspersky portal (see section "About My Kaspersky portal" on page [16](#)) and install it on the computer.

- Installing the application from a distribution kit downloaded from the Kaspersky Lab website or a partner website (see section "Installing the application from the distribution kit" on page [17](#)).

This is done using the Installation Assistant. It lets you check My Kaspersky portal (see section "About My Kaspersky portal" on page [16](#)) for a new version of Kaspersky Internet Security, download it to the computer, and install the application.

**IN THIS SECTION:**

Installing the application downloaded from My Kaspersky portal.....	<a href="#">15</a>
Installing the application from the distribution kit.....	<a href="#">17</a>

## INSTALLING THE APPLICATION DOWNLOADED FROM MY KASPERSKY PORTAL

The **End User License Agreement** and **Participation in Kaspersky Security Network** windows of the Installation Assistant are shown only for German- and Russian-language versions of Kaspersky Internet Security. In other cases, you can view the text of the License Agreement and information about participation in Kaspersky Security Network by clicking the corresponding links in the window of the Kaspersky Internet Security Installation Assistant.

➡ *To install Kaspersky Internet Security from My Kaspersky portal:*

1. Sign in to My Kaspersky portal (see section "About My Kaspersky portal" on page [16](#)) under your account (see section "About the account for signing in to My Kaspersky portal" on page [16](#)).
2. Download the file Kaspersky Internet Security.dmg from My Kaspersky portal.

A window with the contents of the distribution package opens automatically.

If the window with the contents of the distribution package has not opened automatically, open the folder containing the Kaspersky Internet Security.dmg file on your computer and open it manually.

3. Double-click **Install Kaspersky Internet Security** in the window with the contents of the distribution kit.

The Kaspersky Security Installation Assistant starts.

4. Click the **Download and install** button.

The Installer downloads the new version of Kaspersky Internet Security from My Kaspersky portal and installs it on the computer.

5. In the **End User License Agreement** window, read through the text of the Kaspersky Internet Security End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:

- If you accept the terms of the License Agreement, click the **Accept** button.

Installation of Kaspersky Internet Security will continue.

- If you do not accept the terms of the End User License Agreement, click the **Cancel** button.

Installation will be aborted.

6. In the **Participation in Kaspersky Security Network** window, read information about participation in Kaspersky Security Network.

When you participate in Kaspersky Security Network, information about new threats detected on your computer, started applications, applications with signatures being loaded, the unique ID of your copy of Kaspersky Internet Security, and system information, is automatically sent to Kaspersky Lab. It is guaranteed that personal data are not sent.

7. If you agree with all the terms of the Kaspersky Security Network Data Collection Statement, select the **I agree to participate in Kaspersky Security Network** check box.

If you do not accept the terms of participation in Kaspersky Security Network, clear the **I agree to participate in Kaspersky Security Network** check box.

As you use Kaspersky Internet Security subsequently, you can join Kaspersky Security Network at any time or opt out of participation in Kaspersky Security Network.

8. To proceed with installation of the application, click the **Install** button.
9. Confirm installation of Kaspersky Internet Security in the window prompting you for administrator account credentials.


Kaspersky Internet Security starts installing on the computer.

10. Click the **Finish** button to exit the Installer.

Kaspersky Internet Security starts automatically when installation is complete. You do not have to restart the computer.

## ABOUT THE ACCOUNT FOR SIGNING IN TO MY KASPERSKY PORTAL

The account for signing in to My Kaspersky portal (see section "About My Kaspersky portal" on page [16](#)) is your Single Sign On account for accessing all Kaspersky Lab services.

To proceed to creating an account for signing in to My Kaspersky portal, open the main application window (on page [20](#)), click the  button, and click the **My Kaspersky** button in the window that opens.

An account for signing in to My Kaspersky portal is your email address and password that you specified upon creating the account. The password must contain at least eight characters, one numeral, and one upper-case letter.

After your account for signing in to My Kaspersky portal has been created, a message is sent to your email address, containing a link for activation of your account.

After activating the account, you can use it to sign in to My Kaspersky portal. If you do not activate your account by clicking the link in the email within one week, the account will be removed.

If you already have an account for signing in to My Kaspersky portal, you can use it to manage Kaspersky Internet Security.

## ABOUT MY KASPERSKY PORTAL

My Kaspersky portal is a single online resource for managing the protection of all your devices and licenses for Kaspersky Lab applications.

On My Kaspersky portal, you can buy a license or renew an existing license for Kaspersky Internet Security, download a new application version to your computer, and view information about the anti-virus databases used by the application. You can also remotely manage protection of computers with Kaspersky Total Security installed: receive information on the current status of computer protection and remotely fix issues and respond to computer security threats, enable or disable protection components (File Anti-Virus, Web Anti-Virus, Network Attack Blocker), run virus scan tasks, and update application databases.

Use your account to sign in to My Kaspersky portal (see section "About the account for signing in to My Kaspersky portal" on page [16](#)).



## INSTALLING THE APPLICATION FROM THE DISTRIBUTION KIT.

The **End User License Agreement** and **Participation in Kaspersky Security Network** windows of the Installation Assistant are shown only for German- and Russian-language versions of Kaspersky Internet Security. In other cases, you can view the text of the License Agreement and information about participation in Kaspersky Security Network by clicking the corresponding links in the window of the Kaspersky Internet Security Installation Assistant.

➡ *To install Kaspersky Internet Security from the distribution package:*

1. Open the contents of the Kaspersky Internet Security distribution package.

If you have purchased Kaspersky Internet Security at an online store and downloaded the application distribution package in DMG format on the Kaspersky Lab website, open the DMG file.

2. Double-click **Install Kaspersky Internet Security** in the window with the contents of the distribution kit.

The Kaspersky Security Installation Assistant starts. The Installer starts checking My Kaspersky portal for a new version of Kaspersky Internet Security.

3. Select an action following the check for a new version:

- To skip the check for a new version of Kaspersky Internet Security on My Kaspersky portal, click the **Skip** button and then the **Install** button.

The Installer starts installing the version of Kaspersky Internet Security on the computer from the distribution kit.

- If the Installer has detected a new version of Kaspersky Internet Security on My Kaspersky portal, you can install it after downloading it to the computer. To do so, click the **Download and install** button.
- If the Installer has not detected a new version of Kaspersky Internet Security on My Kaspersky portal, you can install the Kaspersky Internet Security version from the distribution package. To do so, click the **Install** button.

4. In the **End User License Agreement** window, read through the text of the Kaspersky Internet Security End User License Agreement between you and Kaspersky Lab. After reviewing the text of the End User License Agreement, do one of the following:

- If you accept the terms of the License Agreement, click the **Accept** button.

Installation of Kaspersky Internet Security will continue.

- If you do not accept the terms of the End User License Agreement, click the **Cancel** button.

Installation will be aborted.

5. In the **Participation in Kaspersky Security Network** window, read information about participation in Kaspersky Security Network.

When you participate in Kaspersky Security Network, information about new threats detected on your computer, started applications, applications with signatures being loaded, the unique ID of your copy of Kaspersky Internet Security, and system information, is automatically sent to Kaspersky Lab. It is guaranteed that personal data are not sent.

6. If you agree with all the terms of the Kaspersky Security Network Data Collection Statement, select the **I agree to participate in Kaspersky Security Network** check box.

If you do not accept the terms of participation in Kaspersky Security Network, clear the **I agree to participate in Kaspersky Security Network** check box.

As you use Kaspersky Internet Security subsequently, you can join Kaspersky Security Network at any time or opt out of participation in Kaspersky Security Network.

7. To proceed with installation of the application, click the **Install** button.
8. Confirm installation of Kaspersky Internet Security in the window prompting you for administrator account credentials.

Kaspersky Internet Security starts installing on the computer.

9. Click the **Finish** button to exit the Installer.

Kaspersky Internet Security starts automatically when installation is complete. You do not have to restart the computer.

## PREPARING THE APPLICATION FOR USE

After Kaspersky Internet Security is installed, you are recommended to do the following:

- Activate Kaspersky Internet Security (see section "Activating Kaspersky Internet Security" on page [33](#)). Activating the application allows you to update the Anti-Virus databases and software modules regularly and provides access to Technical Support.
- Assess the current status of computer protection (see section "Assessing status of computer protection" on page [38](#)).
- Update Kaspersky Internet Security (see section "Updating application databases" on page [43](#)).
- Start a full scan of the computer for viruses and other computer security threats (see section "Performing a full scan of the computer for viruses" on page [41](#)).

## UNINSTALLING THE APPLICATION

Removing Kaspersky Internet Security will expose your computer and data to security threats.

➡ *To uninstall Kaspersky Internet Security:*

1. Open the contents of the Kaspersky Internet Security distribution package.

If you have purchased Kaspersky Internet Security at an online store and downloaded the application distribution package in DMG format on the Kaspersky Lab website, open the DMG file.

2. Double-click **Uninstall Kaspersky Internet Security** in the window with the contents of the distribution kit.

The Kaspersky Internet Security Uninstaller starts. Follow the steps to uninstall Kaspersky Internet Security.

3. In the **Introduction** window, click **Uninstall**.

4. Confirm uninstallation of Kaspersky Internet Security in the window prompting you for administrator account credentials.

The process of uninstalling Kaspersky Internet Security from the computer starts.

5. In the **Completion** window, read the information about the completion of the uninstallation process termination. Click the **Finish** button to quit the Uninstall Assistant.

No restart of the computer is necessary after Kaspersky Internet Security is uninstalled.

# APPLICATION INTERFACE

This section describes the basic GUI components of Kaspersky Internet Security: application icon and context menu of the application icon, main application window and application preferences window, Parental Control window, Safe Money window, and News Agent window. This section also describes notification windows and pop-up messages of the application.

## IN THIS SECTION:

---

Kaspersky Internet Security icon .....	<a href="#">19</a>
Main application window .....	<a href="#">20</a>
Application preferences window .....	<a href="#">21</a>
Parental Control preferences window .....	<a href="#">22</a>
Safe Money window.....	<a href="#">22</a>
Notification windows and pop-up messages.....	<a href="#">23</a>
News Agent.....	<a href="#">24</a>

## KASPERSKY INTERNET SECURITY ICON

As soon as Kaspersky Internet Security has been installed, the application icon appears in the menu bar. The application icon is an indicator of the application's operation. If the application icon is active, it means that real-time protection against malware is enabled for the computer. The inactive application icon indicates that protection is disabled.

The Kaspersky Internet Security icon is always present in the menu bar. If an application window is open, the Kaspersky Internet Security icon also appears on the **Dock** quick launch panel.

The context menu of the application icon provides access to the main commands of Kaspersky Internet Security:

- disabling computer protection;
- resuming computer protection;
- switching to Protection Center;
- starting the update task;
- starting a quick scan;
- switching to the Parental Control preferences window;
- switching to the Safe Money window;
- switching to the application preferences window.

➡ *To open the context menu of the Kaspersky Internet Security icon,*  
click the application icon in the menu bar.

# MAIN APPLICATION WINDOW

➡ *To open the main application window:*

1. Click the Kaspersky Internet Security icon in the menu bar.

The context menu of the application icon opens.

2. Select **Kaspersky Internet Security**.

## Purpose of the main application window

The main window of Kaspersky Internet Security lets you view information about the status of computer protection, the operation of File Anti-Virus and Web Anti-Virus, and progress of virus scan and update tasks.

In the main application window you can also do the following:

- manage virus scan tasks and update tasks;
- manage application keys;
- open the Protection Center window, application preferences window, and reports window;
- view news about Kaspersky Internet Security and protection against computer threats in general;
- open the Parental Control preferences window;
- open the Safe Money window;
- go to My Kaspersky portal.

## Controls of the main application window

The main application window includes the following controls:

- protection status indicator shaped as a computer;
- buttons in the lower part of the main application window;
- navigation panel in the upper part of the main application window;

The protection status indicator reflects the current status of computer protection (see section "Assessing status of computer protection" on page [38](#)).

- green indicates that computer protection is at an optimal level;
- yellow and red warn of the presence of various problems related to Kaspersky Internet Security configuration or operation.

In addition to the computer protection status indicator, the right part of the main application window contains a block of text that describes the computer protection status and lists computer security issues and threats detected by Protection Center. (see section "Using Protection Center" on page [40](#)). If a virus scan or update task is running, information on their progress (percentage complete) is also displayed in the right part of the main application window.

You can perform the following actions by using the buttons in the lower part of the main application window:



Open the Update window.



Switch to virus scan tasks: Quick Scan, Full Scan, and Custom Scan.



Open the Licensing window (see section "Viewing license information" on page [31](#)).



Open the Safe Money window (see section "Safe Money window" on page [22](#)).



Open the Parental Control preferences window (on page [22](#)).

The top part of the main application window contains a navigation panel. You can use the navigation panel to perform the following actions:



Open the Kaspersky Internet Security reports window.



Open the application preferences window (on page [21](#)).



Open the Kaspersky Internet Security help system.




Open the Technical Support window (see section "Contacting Technical Support" on page [57](#)).



Open the News Agent window (see section "News Agent" on page [24](#)) with a list of news items. The button is displayed after Kaspersky Internet Security receives a news item.

## APPLICATION PREFERENCES WINDOW


➡ To open the Kaspersky Internet Security preferences window:


- Click the  button in the main application window (see section "Main application window" on page [20](#)).
- Select **Preferences** in the context menu of the Kaspersky Internet Security icon (see section "Kaspersky Internet Security icon" on page [19](#)).

Application preferences can be accessed quickly using the following tabs in the upper part of the preferences window:

- **Protection.** You can configure File Anti-Virus, Web Anti-Virus, and Network Attack Blocker preferences on this tab.
- **Scan.** You can configure virus scan task preferences on this tab.
- **KSN.** You can connect to Kaspersky Security Network or opt out of participating in Kaspersky Security Network on this tab.
- **Threats.** You can select the categories of objects to be detected and form the trusted zone on this tab.
- **Browsers.** This tab lets you install Kaspersky URL Advisor and Virtual Keyboard as plug-ins for web browsers.
- **Update.** You can configure update task preferences on this tab.
- **Reports.** This tab lets you configure Kaspersky Internet Security report and Quarantine settings, enable or disable the logging of debugging information in the trace file, and configure automatic delivery of the error report to Kaspersky Lab.
- **Appearance.** On this tab, you can configure the way notification windows of Kaspersky Internet Security are displayed.




By using the  button, you can prohibit users without administrator rights from editing the preferences of Kaspersky Internet Security. This button is located in the lower part of the preferences window. You will need to enter the administrator's user name and password to remove the restrictions on modifying preferences.

The  button provides access to the Kaspersky Internet Security help system with a description of the preferences for the current application window. You can also open Help for the currently active application window by selecting **Open Help for This Window** in the **Help** menu.

## PARENTAL CONTROL PREFERENCES WINDOW

➤ To open the Parental Control preferences window, do one of the following:

- Select **Parental Control** in the context menu of the Kaspersky Internet Security icon (see section "Kaspersky Internet Security icon" on page [19](#)).
- Click the  button in the lower part of the main application window (see section "Main application window" on page [20](#)).

The left part of the Parental Control preferences window contains a list of user accounts on the computer. Next to the name of each account, a Parental Control indicator is displayed. A green-colored indicator means that Parental Control is enabled, while red means that Parental Control is disabled. By default, Parental Control is disabled for all user accounts on the computer. You can enable it.

If Parental Control is enabled for a user account, you can select the user operations on the computer and on the Internet that you want to control, by opening the **Preferences** tab in the right part of the Parental Control preferences window.


Kaspersky Internet Security controls the following user operations by categories:

- **Web Control** – control of websites visited and files downloaded.
- **Time control** – control of Internet browsing time.
- **Personal data** – control of use of personal data.
- **Social networks** – control of use of social networks.

By default, control of user operations is disabled for all categories. You can enable control for each category of user operations separately, and proceed to detailed configuration of a selected category in the right part of the Parental Control preferences window.


On the **Reports** tab in the right part of the Parental Control preferences window, you can also view user activity reports for each user account that is covered by Parental Control, for each category individually.

Users cannot configure Parental Control without administrator rights on the computer. To configure and view reports on

Parental Control, click the  button and enter administrator credentials.

## SAFE MONEY WINDOW

➤ To open the Safe Money window, do one of the following:





- Select **Safe Money** in the context menu of the Kaspersky Internet Security icon (see section "Kaspersky Internet Security icon" on page [19](#)).
- Click the  button in the lower part of the main application window (see section "Main application window" on page [20](#)).

The Safe Money component protects payment data and financial transactions as you visit websites of banks, payment systems, and online stores with integrated payment systems, that is, online stores where you enter bank card data.

In the Safe Money window, you can do the following:

- Add, edit and delete bank, payment system and online store details.
- Open the website of the bank, payment system, or online store directly in the browser window.
- View the list of details you have added.

You can perform the following actions by using the buttons in the Safe Money window:

-  Open the window where you can add bank, payment system or online store details and select the action to be performed by the application when you open the website of a bank, payment system, or online store that you have added.
-  Delete the bank, payment system and online store details selected in the list.
-  Open the website of a bank, payment system or online store.
-  Open the window where you can edit the bank, payment system or online store details selected in the list.

## NOTIFICATION WINDOWS AND POP-UP MESSAGES

Events having different levels of importance occur during the operation of Kaspersky Internet Security.

The application informs you about events via *notification windows* and *pop-up messages*. Notification windows can be accompanied by sound alerts.

### IN THIS SECTION:

About notification windows.....	<a href="#">23</a>
About event types.....	<a href="#">23</a>
About pop-up messages .....	<a href="#">24</a>
Disabling notifications .....	<a href="#">24</a>

## ABOUT NOTIFICATION WINDOWS

Kaspersky Internet Security displays notifications when the user needs to be prompted to choose an action in response to an event. For example, when the application detects a malicious object, it prompts you to delete or disinfect the object. A notification window disappears from the screen only after you select one of the actions.

## ABOUT EVENT TYPES

Kaspersky Internet Security events are divided into three types in terms of their importance:

- **Critical** – events posing a dangerous threat to computer security (detection of malicious objects, vulnerabilities, Kaspersky Internet Security problems). Critical events require the immediate attention of the user. It is recommended not to disable critical event notifications.
- **Important** – events that do not require the immediate attention of the user, but may pose a threat to computer security in the future.
- **Information events** – events designed to inform the user.

## ABOUT POP-UP MESSAGES


Kaspersky Internet Security displays *pop-up messages* to inform you of events that do not prompt you to select an action. Depending on the version of the operating system installed on the computer, pop-up messages appear under the application icon in the menu bar or in the Notification Center of the Mac OS X operating system (for operating system of the Mac OS X 10.8 version or later versions).

## DISABLING NOTIFICATIONS


By default, Kaspersky Internet Security notifies (see section "Notification windows and pop-up messages" on page [23](#)) you about critical events only. You can disable notifications or select types of events about which you want to be notified, as well as disable sound notifications.

Regardless of whether notification delivery is enabled or disabled, information about events that occur during the operation of Kaspersky Internet Security is logged in an application operation report.


➤ *To disable notifications:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Appearance** tab of the application preferences window, in the **Notifications** section clear the **Enable notifications** check box to stop receiving notifications in the form of notification windows.

➤ *To select types of events that you do not want to be notified of:*


1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Appearance** tab of the application preferences window, in the **Notifications** section clear the check boxes opposite the types of events (see section "About event types" on page [23](#)) about which you do not want to be notified.

➤ *To disable sound alerts that accompany notification windows:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Appearance** tab of the application preferences window, in the **Notifications** section, clear the **Enable notification sound** check box.

## NEWS AGENT

Using News Agent, Kaspersky Lab informs you of news related to Kaspersky Internet Security and protection against computer threats.

The application notifies you of news by displaying an icon  in the top part of the main application window (see section "Main application window" on page [20](#)). Clicking this icon opens the **News** window.



# APPLICATION LICENSING

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, how to activate the application and renew subscription.

## IN THIS SECTION:

About the End User License Agreement .....	<a href="#">25</a>
About the license .....	<a href="#">25</a>
About subscription .....	<a href="#">26</a>
About the activation code .....	<a href="#">27</a>
About the key .....	<a href="#">27</a>
About data submission .....	<a href="#">27</a>
Viewing license information .....	<a href="#">31</a>
Purchasing a license .....	<a href="#">32</a>
Renewing a license .....	<a href="#">32</a>
Renewing subscription .....	<a href="#">32</a>
Updating subscription status .....	<a href="#">33</a>
Activating Kaspersky Internet Security .....	<a href="#">33</a>

## 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.

You are advised to carefully read the End User License Agreement before using the application.

You can review the terms of the End User License Agreement in the following ways:

- During installation of Kaspersky Internet Security.
- By reading the license.txt file. This file is included in the application's distribution kit.

By confirming that you agree with the End User License Agreement when installing the application, you signify your acceptance of the terms of the End User License Agreement. If you do not accept the terms of the End User License Agreement, you must abort application installation and must not use the application.

## ABOUT THE LICENSE

The *license* is a right to use the application, limited in time, and provided to you on the basis of the End User License Agreement. The unique activation code for your copy of Kaspersky Internet Security is linked to a license.

A license includes the right to receive the following types of services:

- Using the application in full functionality mode on one or several devices.

The number of devices on which you are allowed to use the application is defined by the terms of the End User License Agreement.

- Assistance from Kaspersky Lab Technical Support.
- Benefiting other services provided by Kaspersky Lab or its partners during the entire validity term of the license (see section "Service for users" on page [13](#)).

To use the application in full functionality mode, you have to buy a license for the application and activate the application.

The license is valid for a limited time. When the license expires, the application continues to operate with limited functionality (for example, updates and Kaspersky Security Network are unavailable). You can still use all application components and run virus scans, but only with anti-virus databases that were installed before the license expired. To continue using Kaspersky Internet Security in fully functional mode, you have to renew the license.

You are advised to renew your license on the day when it expires, or earlier, to ensure maximum protection against all security threats.

Before buying a license, you can test run a trial version of Kaspersky Internet Security free of charge. The trial version of Kaspersky Internet Security remains functional for a short trial period. When the trial period expires, all Kaspersky Internet Security features are disabled. To continue using the application, you have to buy a license.

## ABOUT SUBSCRIPTION

*Subscription for Kaspersky Internet Security* is a purchase order for the application with specific parameters (expiry date, number of devices protected). You can order a subscription for Kaspersky Internet Security from your service provider (such as your ISP). You can pause and resume subscription, renew it automatically, or opt out of your subscription. You can manage subscription via the member area on the service provider's website.

A subscription can be limited (for one year, for example) or unlimited (without an expiration date). To keep Kaspersky Internet Security working after expiry of the limited subscription term, you have to renew it manually. Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

If you use the application under limited subscription, upon its expiry you will be offered a grace period to renew subscription during which the application retains its functionality.

Service providers can offer two types of subscription for Kaspersky Internet Security: subscription for updates and subscription for updates and protection. If you have purchased subscription for updates, after your subscription expires and after the grace period for subscription renewal ends, Kaspersky Internet Security retains its functionality but stops updating application databases. If you have purchased subscription for updates and protection, after your subscription expires and after the grace period for subscription renewal ends, Kaspersky Internet Security stops updating application databases and stops protecting the computer and running virus scan tasks.

To use Kaspersky Internet Security under subscription, you have to apply the activation code received from the service provider. In some cases, the activation code can be applied automatically. When you use the application under subscription, you cannot use a different activation code for renewing subscription. You can apply a different activation code only after subscription expires or if you cancel subscription. To cancel your subscription, contact the vendor from which you bought Kaspersky Internet Security.

If at the time of subscription registration you are already using Kaspersky Internet Security under a valid license, remove the current active key to activate the application using a subscription key. The activation code that was previously used to activate the application on this computer can be used on a different computer.

The possible subscription management options may vary with each vendor. Some vendors may also choose not to provide a grace period during which subscription can be renewed.

## ABOUT THE ACTIVATION CODE

The *activation code* is a code that you receive when purchasing a license for Kaspersky Internet Security. This code is required for activating the application.

An activation code is a unique combination of twenty Latin alphanumeric characters in the form xxxxx-xxxxx-xxxxx-xxxxx.

Depending on how you purchased the application, you can obtain the activation code in one of the following ways:

- If you have purchased the boxed version of Kaspersky Internet Security, the activation code is specified in the documentation or on the box.
- If you have purchased Kaspersky Internet Security at an online store, the activation code is sent to the email address that you specified when ordering the product.

The license period countdown starts from the date when you activate the application. If you have purchased a license that allows using Kaspersky Internet Security on several devices, the license countdown starts when you apply the activation code for the first time.

If you have lost or accidentally deleted your activation code after activating the application, contact Technical Support Service at Kaspersky Lab.

## ABOUT THE KEY

A *key* is a sequence of bits with which you can activate and subsequently use the application in accordance with the terms of the End User License Agreement. A key is generated by Kaspersky Lab.

To add a key to the application, you have to enter an *activation code*. After you add a key to the application, the key is displayed in the application interface as a unique alphanumeric sequence.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key has been black-listed, you have to add a different key to continue using the application.

There are two types of keys: active and reserve.

An *active key* is the key that is currently used by the application. The application can have no more than one active key.

A *reserve key* is a key that entitles the user to use the application, but is not currently in use. A reserve key automatically becomes active when the license associated with the current active key expires. A reserve key can be added only if the active key is available. A reserve key cannot be added if you are using a subscription key. A subscription key cannot be added as a reserve key.

A key for a trial license can be added only as the active key. A key for a trial license cannot be installed as a reserve key.

## ABOUT DATA SUBMISSION

Software means software including any Updates and related materials.

Rightholder (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

Computer(s) means hardware, including personal computers, laptops, workstations, personal digital assistants, "smart phones", handheld devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.

End User (You/Your) means individual(s) installing or using the Software on their own behalf or who are legally using a copy of the Software. If the Software is being downloaded or installed on behalf of an organization, such as an employer, "You" further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf.

Update(s) means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs, etc.

Trace files mean data containing information on work of the Software or its components.

Memory dump files mean the contents of system memory of the Software processes at the time of generation.

System information files mean data containing information about Computer.

By accepting the terms of the End User License Agreement, you agree to submit information about the copy of Kaspersky Internet Security installed on your computer, application version and preferences, and activation of the application to Kaspersky Lab, which is done to improve real-time protection.

If you participate in Kaspersky Security Network (see section "Participating in the Kaspersky Security Network" on page [36](#)), the following information relating to Kaspersky Internet Security operation is automatically sent from the computer to Kaspersky Lab:

- Information about the operating system (OS) installed on the computer and installed updates.
- Information about the Right Holder's installed software and the anti-virus protection status, including the version of the Software, the unique software identifiers on the computer, information about updates.
- Information about all scanned objects and actions, including the name of the scanned object, the date and time of the scan, the URL and Referrer from which it was downloaded, the names and size of scanned files and the paths to them, a sign in the archive, the date and time of file creation, the name of the packer (if the file was packed), the file's entropy, the file's type, the file type code, identifier and format, the URL from which the object is downloaded, the object's checksum (MD5), the type and value of the object's supplementary checksum, data about the object's digital signature (certificate), number of starts of the object since the last statistics sending the task identifier of the software that performed the scan.

For executable files: sign of sending service information, reputation verification flag or file signature flag, name, type, ID, type, checksum (MD5) and the size of the application that was loaded by the object being validated, the application path and template paths, a sign of the Autorun list, date of entry, the list of attributes, name of the Packer, information about the digital signature of the application, including the publisher certificate, the name of the uploaded file in the MIME format.

- Information about the running applications and their modules, including checksums (MD5) of running files, size, attributes, creation date, and PE-file header information, names of packers (if the file was packed), code of the account under which the process has been started, command line parameters used to start the process, names of files and their modules.
- If threats or vulnerabilities are detected, in addition to information about the detected object, information is provided about the identifier, version, and type of the record in the anti-virus database, the name of the threat based on the Right Holder's classification, the checksum (MD5) of the application file that requested the URL where the threat was detected, the IP address (IPv4 or IPv6) of the detected threat, the identifier of the type of traffic on which the threat was detected, the vulnerability identifier and its threat level, the URL of the web page where the vulnerability was detected, the number of the script on the page, the identifier of the danger, type, and status of the detected vulnerability, the intermediate results of object analysis.
- Information about network attacks, including the IP address of the attacking computer and the user's computer's port number at which the network attack is directed, the identifier of the protocol used to carry out the attack, and the name and type of attack.
- The URL and IP address of the web page where harmful or suspicious content was detected, the name, size, and checksum of the file that requested the URL, the identifier and weight of the rule used to reach a verdict, the objective of the attack.

- Information about changes made by the user in the list of web sites protected by the Safe Money component, including the URL of the web site, a flag indicating a web site has been added, modified, or deleted, the mode in which Safe Money runs for the web site.
- Aggregated data from the results of scanning using the local and cloud KSN databases, including the number of unique unknown objects, the number of unique trusted objects, the number unique untrusted objects; the total number of verdicts "unknown object", "trusted object" and "untrusted objects", the number of objects trusted based on validation of a certificate, designated as trusted based on a trusted URL, recognized as trusted based on the transfer of trust from a trusted process; the number of unknown objects for which no decision regarding trust has been made, the number of objects that the user has designated as trusted. Version of the local KSN database on the computer at the time the statistics are sent, the software's database settings identifier, information about successful/unsuccessful requests to KSN, the duration of sessions with KSN, the amount of data sent and received, the times at which the collection of information to be sent to KSN was started and stopped.

The Kaspersky Security Network service may process and submit whole files, included objects detected through malicious links which might be used by criminals to harm your computer and/or their parts, to Kaspersky Lab for additional examination.

Additionally, to prevent incidents and investigate those that do occur, trusted executable and non-executable files, application activity reports, portions of the computer's RAM, and the operating system's boot sector may be sent.

To improve the quality of the product, the User agrees to provide Kaspersky Lab with the following information:

- Information about the use of the product's user interface, including information about the opening of the interface's windows (including identifiers and names of windows and used control elements) and switching between windows, information that determines the reason for opening a window, the date and time the interface was started and the stages of interface's startup, the time and type of the user's interaction with the interface, information about changes to settings and product parameters (including the name of the setting or parameter, and the old and new values).
- The ID of the application in interactive mode.

You agree to submit the following information for the purpose of product identification during database and module updates:

- Application ID (AppID)
- Active license ID
- Unique product installation ID (InstallationID)
- Unique update task launch ID (SessionID)
- Full version of application (BuildInfo)

To help with collecting data on the global distribution of software, you agree to submit the following information to the Rightholder automatically:

- Software installation and activation dates
- ID of the partner that provided the software activation license
- Software ID, version of software installed, including versions of software upgrades installed, and ID of the language localization of software
- Unique ID of the computer and unique ID of software installation
- Type of computer
- Serial number of software license installed

Any information transferred does not contain any private data and other types of confidential information of the User. The Rightholder protects any information received in this way as prescribed by law.

If Kaspersky Internet Security returns an error, the user can send a file containing the following data to Kaspersky Lab:

- Process name and ID
- Path to the executable module
- Application version
- Bit version of the process (32- or 64-bit)
- Parent process name and ID
- Application crash date and time
- Operating system version
- Report version
- Type of error that caused the application crash
- Error information
- Number of the thread in which the error occurred
- Call stacks for each thread during the application crash (frame number, module name, address in the code, name of the function at the corresponding address)
- Registry values of the thread in which the error occurred
- List of loaded modules with the address at which the module is loaded, module name, module version, UUID, and path to the module

The following information is additionally specified for the Mountain Lion and Yosemite operating systems:

- User ID (UID)
- Call statistics of specific system calls for interaction of other processes with this process
- Memory distribution (statistics of the amount of memory allocated for specific areas)

Kaspersky Internet Security saves the following information in the trace file:

- Information about the anti-virus protection status of the computer, as well as all potentially malicious objects and actions (including the name of the detected object, date and time of detection, the URL address from which it was downloaded, the names and sizes of infected files and paths to them, the IP address of the attacking computer and the number of the computer port targeted by the network attack, list of malware activity, potentially malicious URLs) and the decisions taken by the product and the user on them.
- Information about applications downloaded by the user (URL, attributes, file size, information about the process that downloaded the file).
- Information about the applications launched and their modules (size, attributes, creation date, PE header details, region, name, location, packers).
- Information about interface errors and usage of the interface of the installed Kaspersky Lab product.
- Information about network connections, including the IP address of the remote computer and the user's computer, the numbers of ports through which the connection was established, and the network protocol of the connection.

- Information about network packets received and sent by the computer over the IT and telecom network.
- Information about email and IM messages sent and received.
- Information about URLs visited, including when the connection was established using an open protocol, data on the website access login and password, and the content of cookies.
- Server public certificate.


Data recorded in memory dump files contain all information present in the operating memory of application processes at the time of dump creation.

Files (or their parts) that may be exploited by intruders to harm the computer or data can be also sent to Kaspersky Lab to be examined additionally.

Kaspersky Lab protects any information received in this way as prescribed by law and applicable rules of Kaspersky Lab. Kaspersky Lab uses any retrieved information in anonymized form and as general statistics only. General statistics are automatically generated using original collected information and do not contain any personal data or other confidential information. Original collected information is stored in encrypted form and destroyed as it is accumulated (twice per year). General statistics are stored indefinitely.

## VIEWING LICENSE INFORMATION

➡ *To view license information:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

The **Licensing** window contains the following information:

- Active key (see section "About the key" on page [27](#))
- Reserve key (if any)
- Key or subscription status
- The number of computers on which you can use the application under the current license or under subscription
- License expiry date and time
- Number of days until license expiry

If the application is not activated, the relevant information is displayed in the **Licensing** window. You can activate the application (see section "Activating Kaspersky Internet Security" on page [33](#)).

If you are using the trial version of the application, you can purchase a license (see section "Purchasing a license" on page [32](#)).


If no reserve key has been added and the license linked to the active key is about to expire, you can renew it (see section "Renewing a license" on page [32](#)).

If your subscription for Kaspersky Internet Security has expired and the grace period during which subscription renewal is available is over, you can renew your subscription manually (see section "Renewing subscription" on page [32](#)). When you use the application under subscription, you can update subscription status (see section "Updating subscription status" on page [33](#)).

## PURCHASING A LICENSE

If you do not have a license for Kaspersky Internet Security or you are using a trial version of the application, you can purchase a license.

➡ *To purchase a license:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window, click the **Buy** button.


This opens a webpage with information on the terms of license purchases through the Kaspersky Lab online store, My Kaspersky portal, or Kaspersky partners. When you buy a license from an online store, an activation code for Kaspersky Internet Security (see section "About the activation code" on page [27](#)) is sent to the email address specified in the order form after you complete payment.

## RENEWING A LICENSE

You have to renew the license if the license associated with the active key has expired and no reserve key has been added. When the license expires, the application continues to operate with limited functionality (for example, updates and Kaspersky Security Network are unavailable). You can still use all application components and run virus scans, but only with anti-virus databases that were installed before the license expired.

**When anti-virus databases are outdated, your computer is exposed to the risk of infection.**

➡ *To renew a license:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window, click the **Renew** button.

This opens a webpage with information on the terms of license renewal through the Kaspersky Lab online store, My Kaspersky portal, or Kaspersky partners. When you renew a license through an online store, an activation code for Kaspersky Internet Security (see section "About the activation code" on page [27](#)) is sent to the email address specified in the order form after you complete payment.

## RENEWING SUBSCRIPTION

When you use the application under subscription, Kaspersky Internet Security automatically contacts the activation server at specific intervals until your subscription expires.


If you use the application under unlimited subscription, Kaspersky Internet Security checks the activation server for a renewed key in background mode (without user involvement) and adds it by replacing the previous key. In this way, unlimited subscription for Kaspersky Internet Security is renewed without user involvement.

If your subscription has expired and the grace period during which subscription renewal is available is over, Kaspersky Internet Security notifies you accordingly and stops attempting to renew subscription automatically. Kaspersky Internet Security stops updating the application databases (in the case of subscription for updates) and stops protecting the computer and running scan tasks (in the case of subscription for updates and protection).



You can renew your subscription manually by contacting the vendor that sold you Kaspersky Internet Security.

➤ *To renew subscription:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.


3. In the **Licensing** window, click the **Visit Service Provider Website** button.

This page shows complete information on the terms of subscription renewal.

## UPDATING SUBSCRIPTION STATUS

Subscription status can become outdated. In this case, you need to update the status of subscription manually. Until the time when subscription is renewed or resumed, Kaspersky Internet Security stops updating the application databases (in the case of subscription for updates) and stops protecting the computer and running virus scan tasks (in the case of subscription for updates and protection).

➤ *To update subscription status:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window that opens, click the **Verify Subscription Status** button.

## ACTIVATING KASPERSKY INTERNET SECURITY

Before activating Kaspersky Internet Security, make sure that the current system date value on your computer matches the actual date and time.

Activating the application involves adding a key (see section "About the key" on page [27](#)) to the application.

If the application has not been activated, all options of Kaspersky Internet Security are available, except the retrieval of updates. Anti-Virus databases can be updated only once after the application is installed.

### IN THIS SECTION:

Activating the trial version .....	<a href="#">34</a>
Activating the application with an activation code .....	<a href="#">34</a>
Activating the application using a Kaspersky Small Office Security activation code .....	<a href="#">35</a>
About participation in Kaspersky Security Network.....	<a href="#">36</a>


## ACTIVATING THE TRIAL VERSION OF THE APPLICATION

A trial version of Kaspersky Internet Security can be activated only if the application has not been previously activated on this computer.

You are advised to activate the trial version of the application if you want to test run the application before deciding whether to purchase a license. The trial version of Kaspersky Internet Security remains functional for a short trial period. When the trial period expires, all Kaspersky Internet Security features are disabled. You will be provided with a free key to for activating the trial version of the application.

An Internet connection is required to activate the application.

➡ To activate the trial version, do the following:

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.  
The **Licensing** window opens.
3. In the **Licensing** window, click the **Try** button.
4. In the **Activate Trial Version** window click the **Activate Trial Version** button.

Kaspersky Internet Security connects to Kaspersky Lab activation servers and sends data for verification. If the verification succeeds, the application receives and adds a free key.

5. Click the **Finish** button to finish activating the application.

After successful activation of the trial version of the application, in the **Licensing** window you can view the following information:

- Key status
- Limitation on the number of computers on which the application can be used
- License expiry date and time
- Number of days until license expiry


When the trial license for Kaspersky Internet Security expires, a corresponding notification appears on the screen. To continue using the application, you have to purchase a license (see section "Purchasing a license" on page [32](#)).

## ACTIVATING THE APPLICATION WITH AN ACTIVATION CODE

Using the activation code, the application obtains and automatically adds a key that unlocks Kaspersky Internet Security functionality for the duration of the license validity period.

An Internet connection is required to activate the application.

➡ To activate the application with your activation code:

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window, click the **Activate** button.
4. In the **Application Activation** window, enter the activation code that you received when purchasing Kaspersky Internet Security.

An activation code is a unique combination of twenty Latin alphanumeric characters in the form xxxxx-xxxxx-xxxxx-xxxxx.

Kaspersky Internet Security connects to Kaspersky Lab activation servers and sends the activation code to verify its authenticity. If activation code verification succeeds, the application automatically receives and adds the key.

Depending on the activation code that you have received, you may need to fill out a registration form or register on My Kaspersky portal.

If activation code verification fails, a corresponding notification is displayed on the screen. In this case, contact the software vendor that supplied you with this activation code.

After the application has been activated successfully using the activation code, in the **Licensing** window you can view the following information:


- Key
- Key or subscription status
- Limitation on the number of computers on which the application can be used
- License expiry date and time
- Number of days until license expiry

## ACTIVATING THE APPLICATION USING A KASPERSKY SMALL OFFICE SECURITY ACTIVATION CODE

You can activate Kaspersky Internet Security using a Kaspersky Small Office Security activation code. If you activate Kaspersky Internet Security using a Kaspersky Small Office Security activation code, you have to confirm your participation in Kaspersky Security Network (see section "About participation in Kaspersky Security Network" on page [36](#)).

An Internet connection is required to activate the application.

➡ To activate the application using a Kaspersky Small Office Security activation code:

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window of the **Application activation** section, enter the Kaspersky Small Office Security activation code.

An activation code is a unique combination of twenty Latin alphanumeric characters in the form xxxxx-xxxxx-xxxxx-xxxxx.

4. Click the **Activate** button.
5. If you accepted the terms of participation in Kaspersky Security Network when installing Kaspersky Internet Security on the computer, the application prompts you to confirm your participation in Kaspersky Security Network. In the **Kaspersky Security Network Statement** window that opens, click the **Accept** button.

To opt out of participating in Kaspersky Security Network, click the **Cancel** button in the **Kaspersky Security Network Statement** window.

If you rejected participation in Kaspersky Security Network when installing Kaspersky Internet Security on the computer, the application does not show the **Kaspersky Security Network Statement** window.

Kaspersky Internet Security connects to Kaspersky Lab activation servers and sends the activation code to verify its authenticity. If activation code verification succeeds, the application automatically receives and adds the key.

After the application has been activated successfully using a Kaspersky Small Office Security activation code, the **Licensing** window displays the following information:

- Key
- Key status
- Limitation on the number of computers on which the application can be used
- License expiry date and time
- Number of days until license expiry

## ABOUT PARTICIPATION IN KASPERSKY SECURITY NETWORK

To increase reliability of your computer protection, Kaspersky Internet Security uses data provided by users from all over the world. A network named Kaspersky Security Network is designed to analyze such data.

Kaspersky Security Network (KSN) is an infrastructure of online services that provides access to the online Kaspersky Lab Knowledge Base, which contains information about the reputation of files, web resources, and software. Use of data from the Kaspersky Security Network ensures a faster response time for Kaspersky Internet Security when encountering new types of threats, improves performance of some protection components, and reduces the risk of false alarms.

Users participating in Kaspersky Security Network provide Kaspersky Lab with information about the types and sources of new threats, which helps Kaspersky Lab to find new ways of neutralizing them, and minimize the number of false positives.

In addition, participation in Kaspersky Security Network provides you with access to information about the reputation of various applications and websites.

When you participate in Kaspersky Security Network, the statistics based on protection of your computer by Kaspersky Internet Security are sent to Kaspersky Lab automatically.

No personal data is collected, processed, or stored.

Participation in Kaspersky Security Network is voluntary. The decision on whether or not to participate is made when you install Kaspersky Internet Security. However, you can change your decision later at any time.

# STARTING AND STOPPING THE APPLICATION

The application starts up immediately after the installation, and the Kaspersky Internet Security icon (on page [19](#)) appears in the Menu Bar.

◆ *To stop Kaspersky Internet Security:*

1. Click the Kaspersky Internet Security icon in the menu bar (see page [19](#)).
2. In the context menu that opens, select **Quit**.

The application stops running, and the process is unloaded from the computer RAM.

After Kaspersky Internet Security quits, the computer keeps running in unprotected mode and may become infected, thus putting your data at risk of loss.

# COMPUTER PROTECTION STATUS

This section provides information on how to determine whether or not computer security threats or problems exist and how to configure the security level. Read this section to learn more about how to enable and disable protection when using the application.

Your computer's protection status indicates the presence or absence of threats, giving you a summary of your computer's overall security level. These threats include detected malicious programs, outdated anti-virus databases, instances of File Anti-Virus or Web Anti-Virus being disabled, and an expiring license.

The Protection Center (see section "Using Protection Center" on page [40](#)) helps you review all the current threats and start neutralizing them.

## IN THIS SECTION:

---

Assessing the status of computer protection .....	<a href="#">38</a>
Disabling computer protection .....	<a href="#">38</a>
Resuming computer protection.....	<a href="#">39</a>
Using Protection Center.....	<a href="#">40</a>

## ASSESSING THE STATUS OF COMPUTER PROTECTION

The computer protection status indicator shaped as a computer and located in the main application window informs you about computer protection problems (see section "Main application window" on page [20](#)). Depending on the condition of computer protection, the color of the indicator may change. If any security threats are detected, the change of the indicator color is supplemented with a message about threats.

The indicator can take the following values:

- **Green.** Your computer's protection is at an appropriate level.

A green indicator signifies that the anti-virus application databases are up to date and all application components have been configured as recommended by Kaspersky Lab. No malicious objects have been detected, or detected malicious objects have been neutralized. Parental Control runs in standard mode.

- **Yellow.** The level of computer protection is reduced.

A yellow indicator signifies a problem with Kaspersky Internet Security. Such problems include, for example: slight deviations from the recommended operation preferences or that the application databases have not been updated for several days.

- **Red.** Your computer is at risk of infection.

A red indicator signifies that there are dangerous problems that may lead to the infection of your computer and loss of data. For example, the anti-virus application databases are obsolete, the application is not activated, or malicious objects have been detected.

You are advised to fix the problems and security threats.

## DISABLING COMPUTER PROTECTION

By default, Kaspersky Internet Security is started when the operating system loads, and protects your computer until it is turned off. All protection components (File Anti-Virus, Web Anti-Virus, and Network Attack Blocker) are enabled and running.

You can fully or partly disable protection provided by Kaspersky Internet Security.

Kaspersky Lab strongly advises against disabling real-time protection provided by protection components, since this may lead to infection of your computer and data loss.

The following signs indicate that computer protection is disabled:

- inactive application icon (see section "Kaspersky Internet Security icon" on page [19](#)) in the Menu bar;
- red color of the computer protection status indicator in the main application window.

Computer protection is examined in the context of operation of File Anti-Virus, Web Anti-Virus, and Network Attack Blocker. Disabling or pausing those protection components does not affect the performance of virus scan tasks or the update task.


You can completely disable computer protection in one of the following ways. You can disable protection components on the **Protection** tab of the application preferences window.

➤ *The following methods can be used to disable computer protection:*

- In the menu bar, click the Kaspersky Internet Security icon (see page [19](#)). In the context menu that opens, select **Turn Protection Off**.
- Open the application preferences window (on page [21](#)), select the **Protection** tab and clear the **Enable protection** check box in the **General** section.

If you have disabled computer protection, it will not be re-enabled automatically when Kaspersky Internet Security starts again. You have to enable computer protection manually (see section "Resuming computer protection" on page [39](#)).

➤ *To disable a protection component:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Protection** tab of the application preferences window, in the **<component name>** section, clear the **Enable <component name>** check box.

If you have disabled a protection component, it will not be re-enabled automatically when Kaspersky Internet Security starts again. You have to enable protection components manually (see section "Resuming computer protection" on page [39](#)).


## RESUMING COMPUTER PROTECTION

If computer protection or a protection component (File Anti-Virus, Web Anti-Virus, or Network Attack Blocker) has been disabled, it can be re-enabled only manually, at the user's request. Computer protection or a protection component will not be re-enabled automatically when Kaspersky Internet Security is started again.

➤ *The following methods can be used to enable computer protection:*

- In the menu bar, click the Kaspersky Internet Security icon (see page [19](#)). In the context menu that opens, select **Turn Protection On**.
- Open the application preferences window (on page [21](#)), select the **Protection** tab, and select the **Enable protection** check box in the **General** section.

➤ *To enable a protection component:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Protection** tab of the application preferences window, in the **<component name>** section, select the **Enable <component name>** check box.

Also, to enable computer protection or protection components, you can use the Protection Center (see section "Using Protection Center" on page [40](#)). Disabling computer protection or disabling protection components dramatically increases the risk of computer infection. Therefore, information about instances of disabled protection is stored in Protection Center.

## USING PROTECTION CENTER

*Protection Center* is a Kaspersky Internet Security feature that lets you analyze and fix unresolved problems and computer security threats.

➤ *To open Protection Center,*

Click the **Learn More** button in the main application window (see section "Main application window" on page [20](#)).

In the Protection Center window you can view a list of existing problems and security threats. For each problem or threat, actions are suggested that you can perform to resolve the problem or threat. You can fix a problem or neutralize a threat immediately or postpone doing so.

➤ *To fix a problem or neutralize a threat immediately,*

click the button with the name of the recommended action to fix the problem or neutralize the threat.

For example, if infected files have been detected on the computer, you should click the **Disinfect** button. If the anti-virus databases used by the application are out of date, you should click the **Update** button. The application performs the chosen operation.

➤ *To fix the problem or neutralize the threat later,*

click the **Hide** button.

The problem or threat notification will be hidden in the list. You can return to neutralizing this problem or threat later.

You cannot postpone neutralizing dangerous computer security threats. Examples of dangerous threats include unprocessed malicious objects, protection component faults, or corrupted databases of Kaspersky Internet Security.

If you close Protection Center without neutralizing dangerous threats, the color of the computer protection status indicator in the main application window continues to indicate their presence.

In the Protection Center window, you can also view information about the update task or current virus scan tasks and stop or restart any of those tasks, if necessary.



# PERFORMING COMMON TASKS

This section contains step-by-step instructions for performing common user tasks with the application.

## IN THIS SECTION:

Performing a full scan of the computer for viruses .....	<a href="#">41</a>
Performing a quick scan of the computer for viruses .....	<a href="#">42</a>
Scanning a file, folder or disk for viruses.....	<a href="#">42</a>
Purchasing a license.....	<a href="#">42</a>
Renewing a license.....	<a href="#">43</a>
Updating application databases.....	<a href="#">43</a>
Preventing interception of data entered using the hardware keyboard .....	<a href="#">44</a>
Protecting financial transactions or purchases on the website of a bank, payment system, or online store .....	<a href="#">44</a>
Limiting Internet usage time for a child or teenager .....	<a href="#">45</a>
Restricting website visits and file downloads for a child or teenager .....	<a href="#">46</a>
Restricting contacts and messaging on social networks for a child or teenager .....	<a href="#">46</a>
Blocking transmission of personal data by a child or teenager .....	<a href="#">47</a>
What to do if file access is blocked .....	<a href="#">47</a>
Restoring a file that has been deleted or disinfected by the application .....	<a href="#">48</a>
Viewing the application operation report .....	<a href="#">49</a>
What to do if notification windows or pop-up messages appear .....	<a href="#">49</a>


## PERFORMING A FULL SCAN OF THE COMPUTER FOR VIRUSES

The full scan task created by default is included in Kaspersky Internet Security. While running this task, the application scans all the internal drives of the computer for viruses and other threats.

➡ *To launch a full computer scan:*

1. Open the main application window (on page [20](#)).

2. Click the  button.

3. In the **Scan** window that opens, select the  **Full Scan** task.

A full scan of the computer starts automatically.

You can view the results of the task in the reports window.


## PERFORMING A QUICK SCAN OF THE COMPUTER

The quick scan task created by default is included in Kaspersky Internet Security. While running this task, the application performs scanning for viruses and other types of malware in critical areas of your computer, such as folders that contain operating system files and system libraries, which may, when infected with malware, cause corruption of your operating system.

► To launch a quick scan of your computer:

1. Open the main application window (on page [20](#)).

2. Click the  button.

3. In the **Scan** window that opens, select the  **Quick Scan** task.

A quick scan of the computer starts automatically.

You can view the results of the task in the reports window.


## SCANNING A FILE, FOLDER OR DISK FOR VIRUSES

If you want to scan an individual object (such as an internal drive, folder, file, or removable device) for viruses and other types of malware, you can use the integrated **Custom Scan** task.

► To scan an individual object for viruses and other malware:

1. Open the main application window (on page [20](#)).

2. Click the  button.

3. In the **Scan** window that opens, select the  **Custom Scan** task.

This opens a drop-down list that lets you select a scan scope.

4. In the drop-down list, select the option you need (for example, **All removable drives**) or drag into the window the files and folders that you want to scan for viruses and other malware.

The application automatically starts scanning the specified scan scope.


Another way to start a scan is by dragging a file or folder to the application icon on the **Dock** quick launch panel or into the main application window (on page [20](#)).

You can view the results of the task in the reports window.

## PURCHASING A LICENSE

If you have installed Kaspersky Internet Security without a license for the application, you can purchase it after installation. When purchasing a license, you receive an activation code that you should use to activate the application (see section "Activating Kaspersky Internet Security" on page [33](#)).

➤ *To purchase a license:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.


3. In the **Licensing** window, click the **Buy** button.

This opens My Kaspersky portal or the web page of the Kaspersky Lab online store or a partner of Kaspersky Lab where you can purchase a license.

## RENEWING A LICENSE

If the license under which Kaspersky Internet Security was activated expires, you can renew it. When renewing a license, you receive an activation code that you should use to activate the application (see section "Activating Kaspersky Internet Security" on page [33](#)).

➤ *To renew a license:*

1. Open the main application window (on page [20](#)).
2. In the lower right part of the main application window, click the  button.

The **Licensing** window opens.

3. In the **Licensing** window, click the **Renew** button.

This opens My Kaspersky portal or the web page of the Kaspersky Lab online store or a partner of Kaspersky Lab where you renew your license.


## UPDATING APPLICATION DATABASES

Kaspersky Lab updates Kaspersky Internet Security anti-virus databases by using update servers. *Kaspersky Lab update servers* are Kaspersky Lab HTTP servers where Kaspersky Internet Security updates are regularly published.

An Internet connection is required to download updates from the update servers.

By default, Kaspersky Internet Security periodically checks for updates on Kaspersky Lab's servers. If a set of the latest updates is stored on a server, Kaspersky Internet Security downloads them in background mode and installs them to your computer.

➤ *To start an update of Kaspersky Internet Security:*

1. Open the main application window (on page [20](#)).
2. Click the  button.
3. In the **Update** window that opens, click the **Update** button.

You can view the results of the update task run in the reports window.

## PREVENTING INTERCEPTION OF DATA ENTERED USING THE HARDWARE KEYBOARD

Thieves can intercept your data during input using the hardware keyboard. For example, thieves can intercept your bank card details when you enter them using the hardware keyboard while shopping online. Virtual Keyboard prevents interception of data input.

Kaspersky Internet Security ensures safe data input by means of a virtual keyboard that you can install in Safari, Firefox, and Google Chrome browsers.


Virtual Keyboard cannot protect your data if the website on which you enter such data has been hacked, because in this case the information ends up directly in the hands of criminals.

Virtual Keyboard is used as follows:

- Click the keys of Virtual Keyboard with the mouse pointer.
- Unlike a hardware keyboard, you cannot activate multiple keys on Virtual Keyboard simultaneously. Therefore, to enter a character that would require a combination of keys (including the **ALT** key and/or **SHIFT** key) on a hardware keyboard, first click the first key (for example, **ALT**) and then click the key with the required character.
- You can use the key in the lower left corner to switch between input languages on Virtual Keyboard. You can click this key and select an input language from the drop-down list.

By default, Virtual Keyboard appears on the screen automatically if a password-entry field is selected in the browser window.


➡ To open Virtual Keyboard,

Click the  button on the browser toolbar.


## PROTECTING FINANCIAL TRANSACTIONS OR PURCHASES ON THE WEBSITE OF A BANK, PAYMENT SYSTEM, OR ONLINE STORE

If you want Kaspersky Internet Security to start protecting your financial transactions or purchases on the website of a bank, payment system or online store, you have to add the relevant website to the list of sites protected by the application.

➡ To add the bank, payment system or online store details to the list of websites protected by Kaspersky Internet Security, do the following in the Safe Money window:

1. Open the main application window (on page [20](#)).
2. In the lower part of the main application window, click the  button.

The **Safe Money** window opens.

3. Click the  button.

A window opens, where you have to specify the details of the website you are adding and select the action to be performed by the application when you visit this website.

4. In the **Website address** field, enter the web address of the bank, payment system or online store.

You can add only websites that use the HTTPS connection.

5. In the **Name** field, enter the name of the bank, payment system or online store.
6. Select the **Use protected mode (verify website identity)** option.

The application starts the browser in protected mode when you visit this website. In this mode, Kaspersky Internet Security checks the authenticity of websites of banks, payment systems, and online stores and also checks certificates used to establish a secure connection.

7. Click the **Add** button.

➡ *To add the bank, payment system or online store details to the list of websites protected by Kaspersky Internet Security, do the following in the web browser window:*

1. In a web browser, open the website of the bank, payment system or online store that you want to add.

You can add only websites that use the HTTPS connection.

A Kaspersky Internet Security message appears in the browser window, letting you enable the protected browser mode for this website. In this mode, Kaspersky Internet Security checks the authenticity of websites of banks, payment systems, and online stores and also checks certificates used to establish a secure connection.

2. Click the **Use protected mode** button.

## LIMITING INTERNET USE TIME FOR A CHILD OR TEENAGER

Excessive duration of computer use by children and teenagers may endanger their health. If you need to limit the Internet surfing time for a user, you can use the Time control category of Parental Control.

➡ *To limit Internet usage time for a user:*

1. Open the Parental Control preferences window (on page [22](#)).
2. In the left part of the window, select a user account for which you want to limit time spent on the Internet.
3. In the right part of the window, click the **Enable parental control** button.
4. In the right part of the window, on the **Preferences** tab, select the **Time control** category. If time control is disabled, enable it.
5. In the **Daily Internet use limit** section select the **Maximum time on Internet** check box.
6. By moving the slider, select the number of hours per day during which Internet usage is allowed.
7. In the **Internet use schedule limit** section, select the **Allow Internet use based on day of week** check box.
8. Impose a time limit on Internet use on weekdays and weekends.

You can view the report on Internet use by the user during the allowed and blocked periods on the **Reports** tab of the Parental Control preferences window.

## RESTRICTING WEBSITE VISITS AND FILE DOWNLOADS FOR A CHILD OR TEENAGER

You can restrict the following operations in order to protect children and teenagers who use the computer:

- access to websites that could waste time (chat rooms, games) or money (e-stores, auctions);
- access to websites targeting an adult audience, such as those displaying pornography, extremism, firearms, drug abuse, and explicit violence;
- downloads of certain file types.

You can use the Web control category of Parental Control.

➡ *To restrict website visits and file downloads from the Internet:*

1. Open the Parental Control preferences window (on page [22](#)).
2. In the left part of the window, select a user account for which you want to restrict access to websites and file downloads from the Internet.
3. In the right part of the window, click the **Enable parental control** button.
4. In the right part of the window, on the **Preferences** tab, select the **Web Control** category. If Web Control is disabled, enable it.
5. Select the **Web Control** check box and the check boxes in the list below next to the names of the categories of websites to which you want to block access.
6. Select the **Control of downloaded files** check box and the check boxes for categories of files that are allowed to be downloaded.

If necessary, you can allow access to some websites included in a blocked category, or block access to specified websites, by creating a list of exclusions.


You can view the report on attempts to visit blocked websites and download prohibited categories of files on the **Reports** tab of the Parental Control preferences window.

## RESTRICTING CONTACTS AND MESSAGING ON SOCIAL NETWORKS FOR A CHILD OR TEENAGER

Controlling the contacts and messaging of children and teenagers on social networks, such as Facebook and Twitter, helps to prevent contact with strangers who may attempt to extract personal information by pretending to be the same age. If you need to restrict a user's contacts and messaging on social networks, you can use the Social Networks category of Parental Control.

➡ *To restrict contacts and messaging over social networks:*

1. Open the Parental Control preferences window (on page [22](#)).
2. In the left part of the window, select a user account for which you want to restrict messaging over social networks.
3. In the right part of the window, click the **Enable parental control** button.
4. In the right part of the window, on the **Preferences** tab, select the **Social Networks** category. If social networks control is disabled, enable it.

5. Create a list of blocked and allowed contacts. To do this, click the  button and, in the **ID** column of the field, enter the ID of a contact from social networks. In the **Name** column of the field, enter the real name of the contact.

You can look up the contact's ID on social networks on the **Reports** tab for the **Social Networks** category of user activity.

After the contact has been added to the list, Parental Control blocks correspondence with this contact on social networks.

6. If you want to allow messaging with a contact temporarily, select one from the list and clear the check box in the **Blocked** column.

Messaging with this contact will remain allowed until the check box is selected again.

If messaging with a contact is prohibited, Parental Control blocks all messages sent to or received from that contact.


You can view the following information on the **Reports** tab of the Parental Control preferences window:

- information about messages received from or sent to any blocked contact;
- information about inclusion of personal data in messages;
- logs of messaging with each contact.

## BLOCKING TRANSMISSION OF PERSONAL DATA BY A CHILD OR TEENAGER

Kaspersky Internet Security allows you to reduce the risks associated with use of computers and the Internet. You can block transmission of data that contains personal information through social networks and when submitting data to websites, by using the Personal data category of Parental Control.

➡ *To block transmission of personal data:*

1. Open the Parental Control preferences window (on page [22](#)).
2. In the left part of the window, select a user account for which you want to block transmission of personal data.
3. In the right part of the window, click the **Enable parental control** button.
4. In the right part of the window, on the **Preferences** tab, select the **Personal data** category. If personal data control is disabled, enable it.
5. Create a list of personal data. To do this, click the  button and enter data in the **Description** and **Data** columns of the field. For example, you can create records for your bank card number, home address, and phone number.


After personal data has been added to the list, Parental Control blocks the transmission of such data via social networks or to websites.

Kaspersky Internet Security blocks all attempts to send the data that has been added to the list. You can view information about blocked messages on the **Reports** tab of the Parental Control preferences window.

## WHAT TO DO IF FILE ACCESS IS BLOCKED

Kaspersky Internet Security blocks access to infected and probably infected files and applications. If a file is infected, it must be disinfected before it can be accessed.

➡ *To disinfect detected objects:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.

The Kaspersky Internet Security reports window opens.

3. Select **Detected objects** in the left part of the reports window.

The **Active** group in the right part of the window displays a list of detected objects with their respective statuses. You can expand the list of objects by clicking the icon ►.

4. Disinfect all or one of the infected objects detected:

- To disinfect all detected objects, click the **Disinfect all** button.

The application starts disinfecting detected objects. While object disinfection is in progress, the application shows a notification window where you can choose the action to be taken on the object. If you select the **Apply to all** check box in the notification window after choosing the action to be taken on the object, the application applies this action to all files of this type.

- To disinfect one of the infected objects detected, select this object in the list and click the **Disinfect** button.

The application starts disinfecting the selected object. While object disinfection is in progress, the application shows a notification window where you can choose the action to be taken on the object.


If you know for sure that the files being blocked by File Anti-Virus are safe, you can include them in a trusted zone.

## RESTORING A FILE THAT HAS BEEN DELETED OR DISINFECTED BY THE APPLICATION

*We recommend that you avoid restoring deleted and disinfected files unless it is extremely necessary, because they may threaten your computer.*

Sometimes it is not possible to save files in their entirety during the disinfection process. If a disinfected file contained important information that is partly or completely inaccessible following disinfection, you can attempt to restore the original file from its backup copy.

➡ *To restore a file that has been deleted or modified by the application during disinfection:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.

The Kaspersky Internet Security reports window opens.

3. In the left part of the reports window, select **Quarantine**.

The right part of the window displays the contents of Quarantine in the form of a list of copies of files.

4. Select the backup copy of the file you require in the list and click the **Restore** button. Confirm the action in the window that opens.

The file is restored to its original location with its original name. If there is a file with the same name in the original location (this situation is possible when restoring a file that had been copied prior to disinfection), a warning appears. You can change the location of the file that is being restored or rename it.




We recommend that you scan the file for viruses immediately after restoring it. It is possible that the file will be disinfected by using the updated databases, without losing its integrity.

## VIEWING THE REPORT ON THE APPLICATION'S OPERATION

Information about events that have occurred in the operation of File Anti-Virus, Web Anti-Virus, Network Attack Blocker or while running the virus scan or update tasks, is displayed in the reports window.

➡ *To open the reports window,*

open the main application window (on page [20](#)) and click the  button.

## WHAT TO DO IF NOTIFICATION WINDOWS OR POP-UP MESSAGES APPEAR

Application notifications (see section "Notification windows and pop-up messages" on page [23](#)) appearing as notification windows inform you of events that occur during the operation of the application and require your attention.

If such a notification is displayed on the screen, select one of the suggested options. The optimal option is the one recommended as the default option by Kaspersky Lab experts.

# MANAGING THE APPLICATION FROM THE COMMAND LINE

You can manage Kaspersky Internet Security from the command line.

After the updates of Kaspersky Internet Security modules have been installed, the version of the application client in the command line may differ from the installed version of the application.

Command line syntax:

```
kav <command> [parameters]
```

The following commands can be inserted as <command>:

- **help** – helps with command syntax, displays the list of commands;
- **scan** – scans objects for malware;
- **update** – starts the application update;
- **rollback** – rolls back the latest update to Kaspersky Internet Security (administrator rights are required to run this command);
- **start** – starts a component or task;
- **stop** – stops a component or task (administrator rights are required to run this command);
- **status** – displays the current status of a component or task on the screen;
- **statistics** – displays operational statistics of a component or task;
- **export** – exports the parameters of a component or task;
- **import** – imports the parameters of a component or task (administrator rights are required to run this command);
- **addkey** – activates the application by using a key file (administrator rights are required to run this command);
- **exit** – quits the application (administrator rights are required to run this command).

Each command has its own range of parameters.

## IN THIS SECTION:

Viewing Help .....	<a href="#">51</a>
Virus Scan.....	<a href="#">51</a>
Updating the application.....	<a href="#">53</a>
Rolling back the last update .....	<a href="#">53</a>
Starting / stopping a protection component or task.....	<a href="#">54</a>
Component or task operation statistics .....	<a href="#">55</a>

Exporting protection preferences .....	<a href="#">55</a>
Importing protection preferences .....	<a href="#">55</a>
Closing the application .....	<a href="#">56</a>
Return codes of the command line .....	<a href="#">56</a>

## VIEWING HELP

Use this command to view the application command line syntax:

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

To get help on the syntax of a specific command, you can use one of the following commands:

```
kav <command> -?
kav help <command>
```

## VIRUS SCAN

The text of the command to start a virus scan of a specific area has the following general format:

```
kav scan [<scan scope>] [<action>] [<file types>] [<exclusions>] [<report
parameters>] [<advanced parameters>]
```

To scan for viruses, you can also use the tasks created in the application by starting the one you need from the command line (see section "Starting / stopping a protection component or a task" on page [54](#)). The task is started with the parameters that are specified in the Kaspersky Internet Security interface.

### Parameter description

**<scan scope>** – this parameter specifies a list of objects that are to be scanned for malicious code. The parameter may include several values (separated by a blank space) from the following list:

**<files>** – list of paths to files and / or folders to be scanned. You can enter an absolute or relative path. Items in the list are separated by a blank space. Comments:

- if the name of an object or the path to it includes a blank space or special characters (such as \$, &, @), it should be put in single quotes, or the character being excluded should be separated with the backslash on its left side;
- if reference is made to a specific folder, all files and folders in this folder are scanned.

**-all** – full scan of your computer;

**-remdrives** – all removable drives;

**-fixdrives** – all local drives;

**-netdrives** – all network drives;

**-@:<filelist.lst>** – path to the file with a list of objects and folders within the scan scope. The file must be in text format and each scan object must be listed in a separate line. Only an absolute path to the file may be entered.

If no scan scope is specified, Kaspersky Internet Security starts the Custom Scan task with the preferences that are selected in the application interface.

**<action>** – this parameter determines the action to take on malicious objects that are detected during the scan. If this parameter has not been defined, the default action is the one corresponding to the value **-i8**. The following values are possible:

- i0** – take no actions on the object, only save information about the object in a report;
- i1** – disinfect infected objects, skip them if they cannot be disinfected;
- i2** – disinfect infected objects, delete them if they cannot be disinfected; do not delete containers, except for those with executable headers (sfx archives);
- i3** – disinfect infected objects, delete them if they cannot be disinfected; delete containers completely if infected files inside them cannot be deleted;
- i4** – delete infected objects; delete containers completely if infected files inside them cannot be deleted;
- i8** – prompt the user for action if an infected object is detected (used by default);
- i9** – prompt the user for action when the scan is completed.

**<file types>** – this parameter defines the file types that are subject to anti-virus scanning. By default, if this parameter is not defined, and only infected files by contents are scanned. The following values are possible:

- fe** – scan only infected files by extension;
- fi** – scan only infected files by content (by default);
- fa** – scan all files.

**<exclusions>** – this parameter defines objects that are to be excluded from scanning. You can include several parameters from the list below, separating them with a blank space:

- e:a** – do not scan archives;
- e:b** – do not scan mail databases;
- e:m** – do not scan email messages in text format;
- e:<mask>** – do not scan objects by mask;
- e:<seconds>** – skip objects that are scanned for longer than the specified time value (in seconds);
- es:<size>** – skip objects with size larger than the specified value (in megabytes).

**<report parameters>** – these parameters define the format of the report on the scan results. You can use an absolute or relative path to the file for saving the report. If the parameter is not defined, scan results are displayed and all events are shown.

- r:<report\_file>** – log only important events to the specified report file;
- ra:<report\_file>** – log all events to the specified report file.

**<advanced parameters>** – parameters that define the use of anti-virus scanning technologies and the configuration file:

- iSwift=<on|off>** – enable / disable the use of iSwift technology;
- c:<settings\_file>** – defines the path to the configuration file that contains the application preferences applied when running virus scan tasks. You can enter an absolute or relative path to the file. If the parameter is not specified, the values set in the application interface are used together with the values that are already specified in the command line.

**Example:**

Start scan of the folders ~/Documents, /Applications, and the file named my test.exe:

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

Scan the objects listed in the file object2scan.txt. Use the scan\_settings.txt configuration file. When the scan is complete, create a report to log all events:

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

A sample configuration file:

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

## UPDATING THE APPLICATION

The command for updating the application has the following syntax:

```
kav update [<update_source>] [-app=<on|off>] [<report_parameters>]  
[<advanced_parameters>]
```

### Parameter description

**<update\_source>** – an HTTP server or a network or local folder for downloading updates. If a path is not selected, the update source will be taken from the application update preferences.

**-app=<on|off>** – enable / disable application module updates.

**<report parameters>** – these parameters define the format of the report on the scan results. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown. The following values are possible:

**-r:<report\_file>** – log only important events to the specified report file;

**-ra:<report\_file>** – log all events to the specified report file.

**<advanced parameters>** – a parameter that defines the use of the configuration file.

**-c:<configuration\_file\_name>** – defines the path to the configuration file that contains the application preferences applied when updating the application. You can enter an absolute or relative path to the file. If this parameter is not defined, the values set in the application interface are used.

**Example:**

Update the application databases from the default source, logging all events in the report:

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

Update the Kaspersky Internet Security modules using the parameters of the updateapp.ini configuration file:

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

## ROLLING BACK THE LAST UPDATE

Command syntax:

```
kav rollback [<report_parameters>]
```

Administrator rights are required to run this command.

### Parameter description

**<report parameters>** – this parameter defines the format of the report on update rollback results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown.

**-r:<report\_file>** – log only important events to the specified report file;

**-ra:<report\_file>** – log all events to the specified report file.

#### Example:

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

## STARTING / STOPPING A PROTECTION COMPONENT OR TASK

The start command syntax:

```
kav start <profile|task_name> [<report_parameters>]
```

The stop command syntax:

```
kav stop <profile|task_name>
```

Computer administrator rights are required to run the stop command.

### Parameter description

**<report parameters>** – these parameters define the format of the report on the scan results. You can use an absolute and relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown. The following values are possible:

**-r:<report\_file>** – log only important events to the specified report file;

**-ra:<report\_file>** – log all events to the specified report file. You can use an absolute or relative path to the file. If the parameter is not defined, scan results are displayed and all events are shown.

**<profile|task\_name>** – one of the following values is displayed:

**file\_monitoring (fm)** – File Anti-Virus;

**web\_monitoring (wm)** – Web Anti-Virus;

**scan\_my\_computer (full)** – Full Scan task;

**scan\_objects** – Custom Scan task;

**scan\_critical\_areas (quick)** - Quick Scan task;

**updater** – update task;

**rollback** – update rollback task.

Components and tasks started from the command prompt are run with the parameters configured in the application interface.

**Example:**

To enable the File Anti-Virus component, type the following in the command line:

```
kav start fm
```

To stop the full scan task from the command line, enter the following:

```
kav stop scan_my_computer
```

## COMPONENT OR TASK OPERATION STATISTICS

The status command syntax:

```
kav status [<profile|task_name>]
```

The statistics command syntax:

```
kav statistics <profile|task_name>
```

### Parameter description

**<profile|task\_name>** – one of the values listed for the start / stop command is specified (see section "Starting / stopping a protection component or a task" on page [54](#)).

If the status command is run without specifying a value for the **<profile|task\_name>** parameter, the current status of all tasks and components of the application is displayed on the screen. For the statistics command, a value must be specified for the **<profile|task\_name>** parameter.

## EXPORTING PROTECTION PREFERENCES

Command syntax:

```
kav export <profile|task_name> <file_name>
```

### Parameter description

**<profile|task\_name>** – one of the values listed for the start / stop command is specified (see section "Starting / stopping a protection component or a task" on page [54](#)).

**<file\_name>** – path to the file to which the application preferences are exported. An absolute or relative path may be specified.

**Example:**

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

## IMPORTING PROTECTION PREFERENCES

Command syntax:

```
kav import <file_name>
```

Administrator rights are required to run this command.

### Parameter description

**<file\_name>** – path to the file from which the application preferences are imported. An absolute or relative path may be specified.

#### **Example:**

```
kav import settings.dat
```

## CLOSING THE APPLICATION

Command syntax:

```
kav exit
```

Administrator rights are required to run this command.

## RETURN CODES OF THE COMMAND LINE

The general codes may be returned by any command from the command line. The return codes include general codes as well as codes specific to a certain task.

General return codes:

- 0 – operation completed successfully;
- 1 – invalid parameter value;
- 2 – unknown error;
- 3 – task completion error;
- 4 – task canceled.

Virus scan task return codes:

- 101 – all malicious objects processed;
- 102 – malicious objects detected.



# CONTACTING TECHNICAL SUPPORT


This section describes the ways to get technical support and the terms on which it is available.

## IN THIS SECTION:

Ways to receive technical support .....	<a href="#">57</a>
Technical support by phone .....	<a href="#">57</a>
Contacting Technical Support from My Kaspersky Portal .....	<a href="#">58</a>
Using a trace file.....	<a href="#">58</a>
Creating a trace file.....	<a href="#">59</a>
Sending files with error information to Kaspersky Lab .....	<a href="#">59</a>

## WAYS TO RECEIVE TECHNICAL SUPPORT

➡ To view information about the ways in which you can receive technical support for Kaspersky Internet Security,

open the main application window (on page [20](#)) and click the  button.

If you do not find a solution to your problem in the application documentation or in one of the sources of information about the application, we recommend contacting Kaspersky Lab's Technical Support. Technical Support specialists will answer any of your questions about installing and using the application.

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

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

- Call by phone. This method allows you to consult specialists from our Russian-language or international Technical Support.
- Send a request via My Kaspersky portal <https://my.kaspersky.com/>. This option allows contacting Technical Support specialists through a request form.

Technical support is only available to users who purchased a license for the application. No technical support is available to users of trial versions.

## TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call Kaspersky Lab Technical Support representatives (<http://support.kaspersky.com/b2c>).

Before contacting Technical Support, you are advised to read the technical support rules (<http://support.kaspersky.com/support/rules>). These rules contain information about the working hours of Kaspersky Lab Technical Support and about the information that you must provide so that Kaspersky Lab Technical Support specialists can help you.

# CONTACTING TECHNICAL SUPPORT FROM MY KASPERSKY PORTAL

My Kaspersky portal is a single online resource for managing the protection of all your devices and licenses for Kaspersky Lab applications.

To access My Kaspersky portal, you have to register.

My Kaspersky portal lets you:

- send requests to Technical Support and the Virus Lab;
- exchange messages with Technical Support without using email;
- monitor the status of your requests in real time;
- view a complete history of all your requests;
- receive a copy of the key file in case it has been lost or stolen.

## Email request to Technical Support

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

In the email request form, specify the following information:

- request type;
- application name and version number;
- request text.

## Email request to Virus Lab

Some requests must be sent to the Virus Lab, not Technical Support.

You can send requests to the Virus Lab in the following cases:


- If you suspect that a file or website contains a virus, but Kaspersky Internet Security does not detect any threat. Virus Lab specialists analyze the file or web address that you send. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when Kaspersky Lab anti-virus applications are updated.
- If Kaspersky Internet Security detects a virus in a file or on a website, but you are certain that this file or website is safe.

# USING A TRACE FILE

After you report a problem to Kaspersky Lab Technical Support specialists, they may ask you to generate a report with information about the operation of Kaspersky Security and send it to Kaspersky Lab Technical Support. Kaspersky Lab Technical Support specialists may also ask you to generate a *trace file*. Trace files allow tracking the step-by-step process of command execution and finding out at which step an error occurs.

## CREATING A TRACE FILE

➡ *To create a trace file:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Reports** tab of the application preferences window, in the **Traces** section, select the **Enable trace logs** check box.
4. Restart Kaspersky Internet Security to start the tracing process.


*It is recommended to enable tracing only when instructed to do so by a Kaspersky Lab Technical Support specialist.*

Trace files can occupy a significant amount of space on your hard drive. After finishing with trace files, it is recommended that you disable creation of such files by clearing the **Enable trace logs** check box on the **Reports** tab of the application preferences window. You have to restart Kaspersky Internet Security afterwards.

## SENDING FILES WITH ERROR INFORMATION TO KASPERSKY LAB

Kaspersky Internet Security can save application status information at the time when an error occurs and automatically send it to Kaspersky Lab.

➡ *To disable automatic transmission of files with error information to Kaspersky Lab:*

1. Open the main application window (on page [20](#)).
2. Click the  button on the navigation panel in the upper part of the main application window.  
The application preferences window opens.
3. On the **Reports** tab of the application preferences window, in the **Error reporting** section, select the **Send report automatically** check box.

You can also enable automatic transmission of files with error information to Kaspersky Lab in the application startup error notification window.

# GLOSSARY

## A

### **ACTIVATING THE APPLICATION**

Conversion of the application into full-function mode. Activation is performed by the user during or after the application installation. To activate the application, the user needs an activation code or a key file.

### **ACTIVE KEY**

A key that is currently in use for application operation.

## B

### **BLOCKING THE OBJECT**

Denying access to an object from external applications. A blocked object cannot be read, executed or changed.

## D

### **DATABASES**

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

## F

### **FALSE ALARM**

Situation when Kaspersky Lab's application considers a non-infected object as infected due to its code similar to that of a virus.

## H

### **HEURISTIC ANALYZER**

A technology designed to detect threats that have not yet been added to databases of Kaspersky Lab. The heuristic analyzer allows detecting objects behaving in a way that can pose a security threat to the operating system. Objects detected using the heuristic analyzer are considered to be potentially infected. For example, an object can be considered to be potentially infected if it contains combinations of commands that are typical of malicious objects (open file, write to file).

## I

### **INFECTED OBJECT**

An object a segment of whose code fully matches a code segment of a known threat. Kaspersky Lab specialists recommend that you avoid handling such objects.

## K

### **KASPERSKY LAB UPDATE SERVERS**

HTTP servers at Kaspersky Lab from which the applications retrieve updates for the application databases and modules.

**O****OBJECT DISINFECTION**

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

**P****PHISHING**

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

**POTENTIALLY INFECTED OBJECT**

An object whose code contains a modified segment of code of a known threat, or an object resembling a threat in the way it behaves.

**PROTECTION**

The application's operating mode under which objects are scanned for the presence of malicious code in real time.

The application intercepts all attempts to open any object (read, write, or execute) and scans the object for threats. Uninfected objects are passed on; objects containing threats or probably infected objects are processed according to the task preferences (disinfected, deleted or quarantined).

**PROTECTION STATUS**

The current status of protection, summarizing the degree of a computer's security.

**Q****QUARANTINE**

Special storage designed to save backup copies of objects created before their first disinfection or deletion. The Kaspersky Lab application also quarantines potentially infected objects that have been detected. Quarantined objects are stored in encrypted form to avoid any impact on the computer.

**R****RESERVE KEY**

A key that confirms the right to use the application although it is not currently in use.

**RESTORATION**

Moving an original object from Quarantine the folder where it was originally found before being disinfected or deleted, or to a different folder specified by the user.

**U****UPDATE**

A feature of the Kaspersky Lab application that allows maintaining computer protection in up-to-date condition. While being updated, the application copies updates for application databases and modules from Kaspersky Lab servers to the computer and then installs and applies them automatically.

# 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 was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

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

**PRODUCTS.** Kaspersky Lab products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and tablet computers, and 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's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly; and the Anti-Spam database - every 5 minutes.*

**TECHNOLOGIES.** Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. This is one of the reasons why many third-party software developers have chosen to use the Kaspersky Anti-Virus engine 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), Openwave Messaging (Ireland), D-Link (Taiwan), M86 Security (USA), GFI Software (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (France), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

**ACHIEVEMENTS.** Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a reputed 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 thousand.

Kaspersky Lab's website:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Virus Lab:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (only for sending probably infected files in archives)

Kaspersky Lab's web forum:

<http://forum.kaspersky.com/index.php?showforum=117>

# INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file named legal\_notices.txt in the application installation folder.

# TRADEMARK NOTICES

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

Mac, Mac OS, OS X and Safari are registered trademarks owned by Apple Inc.

Google Chrome is a trademark owned by Google, Inc.

Firefox is a trademark owned by Mozilla Foundation.



# INDEX

## A

Activating the application .....	33
trial version .....	34
Activating the application with an activation code .....	34
Activation code .....	27
Application databases .....	43

## B

Bank online .....	44
-------------------	----

## H

Hardware and software requirements .....	13
--	----

## K

Kaspersky Lab ZAO .....	62
Key .....	27

## L

Launch	
virus scan tasks .....	41, 42
License .....	25
information .....	31
purchasing .....	32, 42
renewal .....	32, 43

## M

Main application window .....	20
My Kaspersky .....	16

## N

Notifications .....	23, 49
---------------------	--------

## P

Parental Control .....	22, 45, 46, 47
Protection .....	38, 39
Protection Center .....	38, 40

## Q

Quarantine .....	48
------------------	----

## R

Reports .....	49
Restoring an object .....	48

## S

Starting	
application .....	37
Subscription .....	32, 33

U

Update task start ..... 43

Updating the application..... 43

V

Virtual Keyboard..... 44

Virus Scan.....41, 42