

Kaspersky Internet Security for Android

KASPERSKY **lab**

Benutzerhandbuch

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Wichtiger Hinweis: Die Rechte an diesem Dokument liegen bei Kaspersky Lab und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach geltendem Recht zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Vervielfältigen, Weiterverbreiten und Übersetzen der Unterlagen ist nur nach vorheriger schriftlicher Genehmigung von Kaspersky Lab zulässig.

Das Dokument und dazu gehörende Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Kaspersky Lab behält sich das Recht vor, dieses Dokument ohne vorherige Benachrichtigung zu ändern. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse <http://www.kaspersky.de/docs>.

Für den Inhalt, die Qualität, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab ZAO die Haftung ab.

Redaktionsdatum: 22.07.2014

© 2014 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

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

INHALT

ÜBER DIESES HANDBUCH.....	5
In diesem Dokument	5
Formatierung mit besonderer Bedeutung	7
INFORMATIONSQLLENN ZUM PROGRAMM	8
Informationsquellen zur selbständigen Recherche	8
Diskussion über die Programme von Kaspersky Lab im Forum	9
Kontaktaufnahme mit der Vertriebsabteilung	9
Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation.....	9
KASPERSKY INTERNET SECURITY	10
Hard- und Softwarevoraussetzungen	11
Lieferumfang.....	11
Service für Benutzer.....	12
INSTALLATION UND DEINSTALLATION DES PROGRAMMS	13
Programm installieren.....	13
Programm deinstallieren.....	14
PROGRAMMOBERFLÄCHE.....	15
Hauptfenster von Kaspersky Internet Security	15
Indikator für den Schutzstatus in Form eines Schilds	16
Schnellstartleiste.....	17
Symbol im Infobereich der Taskleiste.....	18
Widget für das Hauptfenster des Geräts.....	19
Benachrichtigungen.....	19
LIZENZIERUNG DES PROGRAMMS	21
Über den Lizenzvertrag	21
Über die Lizenz	21
Über den Aktivierungscode.....	22
Über die Bereitstellung von Daten.....	22
PROGRAMM STARTEN UND BEENDEN	24
ERSTE-SCHRITTE-HANDBUCH	25
Vorgehensweise beim Fund eines schädlichen Objekts	25
Daten vor unerlaubtem Zugriff schützen	25
Zweck des Geheimcodes	26
Was ist ein Kaspersky Account?.....	26
Erstkonfiguration des Diebstahlschutzes.....	26
Vorgehensweise bei Verlust oder Diebstahl des Geräts	27
LÖSUNGEN FÜR TYPISCHE AUFGABEN	29
Scanner (Anti-Virus).....	29
Alles scannen	30
Speicher scannen	30
Ordner und Dateien scannen.....	30
Automatischer Scan nach Zeitplan	30
Update der Antiviren-Datenbanken und Programm-Upgrade	31

Automatisches Update nach Zeitplan.....	31
Privatsphäre.....	31
Informationen für private Kontakte ausblenden	32
Ferngesteuerter Start der Datenausblendung von einem anderen Gerät aus.....	32
Diebstahlschutz.....	33
Gerät zum Benutzerkonto im Webportal hinzufügen.....	34
SMS-Befehle aus Kaspersky Internet Security senden	34
Ferngesteuerte Überwachung der SIM-Karte	34
Ferngesteuerte Gerätesperre und Ortung	35
Ferngesteuertes Einschalten der Alarmfunktion	36
Ferngesteuerte Datenlöschung vom Gerät.....	37
Ferngesteuertes Fotografieren	38
Anruf- und SMS-Filter.....	38
Standardmäßige Filterung von Kontakten	38
Alle Kontakte sperren, außer den erlaubten	39
Nur verbotene Kontakte sperren.....	39
Web-Filter und SMS-Anti-Phishing.....	40
Echtzeituntersuchung von Webseiten	40
Echtzeituntersuchung von Links in SMS-Nachrichten.....	41
Andere Aufgaben	41
Premium-Version des Programms aktivieren	41
Lizenz kaufen	42
Lizenz verlängern	42
Informationen zur Lizenz und zur Lizenzgültigkeit anzeigen.....	43
Berichte über das Programm anzeigen	43
Geheimcode für das Programm ändern	43
Geheimcode für das Programm wiederherstellen	43
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT.....	45
Wie Sie technischen Kundendienst erhalten.....	45
Technischer Support am Telefon	45
Technischen Support erhalten über Mein Kaspersky Account.....	45
GLOSSAR.....	47
KASPERSKY LAB ZAO	49
INFORMATIONEN ÜBER DEN CODE VON DRITTHHERSTELLERN	50
MARKENINFORMATIONEN.....	51
SACHREGISTER	52

ÜBER DIESES HANDBUCH

Dies ist ein Benutzerhandbuch für Kaspersky Internet Security for Android (im Weiteren Kaspersky Internet Security).

Das Benutzerhandbuch richtet sich an Anwender von Kaspersky Internet Security, die mit der Benutzeroberfläche und den Grundfunktionen des betreffenden Betriebssystems vertraut sind, und mit dem Internet umgehen können.

Das Handbuch dient folgenden Zwecken:

- Hilfe bei der Installation, Aktivierung und Verwendung von Kaspersky Internet Security.
- Schnelle Beantwortung von Fragen, die sich auf die Arbeit mit Kaspersky Internet Security beziehen.
- Hinweise auf zusätzliche Informationsquellen zum Programm und auf Möglichkeiten des technischen Supports.

IN DIESEM ABSCHNITT

In diesem Dokument.....	5
Formatierung mit besonderer Bedeutung.....	7

IN DIESEM DOKUMENT

Dieses Handbuch enthält folgende Abschnitte:

Informationsquellen zum Programm

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Kaspersky Internet Security

Dieser Abschnitt beschreibt die Programm-Features und bietet kurze Informationen zu den Programmfunktionen und -komponenten. Hier werden der Lieferumfang und die Services beschrieben, die den registrierten Programmnutzern zur Verfügung stehen. Dieser Abschnitt informiert über die Hard- und Softwarevoraussetzungen, die ein Gerät erfüllen muss, damit das Programm installiert werden kann.

Installation und Deinstallation des Programms

Dieser Abschnitt bietet genaue Anleitungen für die Installation und Deinstallation von Kaspersky Internet Security for Android.

Programmoberfläche

Dieser Abschnitt informiert über die wichtigsten Elemente der grafischen Programmoberfläche: Hauptfenster, Indikator für den Schutzstatus in Form eines Schilds, Schnellstartleiste, Programmsymbol, Widget und Meldungsfenster.

Lizenzierung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

Programm starten und beenden

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Erste-Schritte-Handbuch

Dieser Abschnitt informiert über die ersten Schritt nach der Programminstallation.

- Anleitungen für das Vorgehen beim Fund eines schädlichen Objekts
- Hinweise für den Schutz privater Daten vor unberechtigtem Zugriff
- Anleitungen für das Vorgehen bei Verlust oder Diebstahl des Geräts

Lösungen für typische Aufgaben

Dieser Abschnitt bietet genaue Anleitungen für die wichtigsten Aufgaben, die der Benutzer mit dem Programm lösen kann.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt die Kontaktaufnahme mit dem Technischen Support.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen von Begriffen, die in diesem Dokument vorkommen.

Kaspersky Lab ZAO

Dieser Abschnitt enthält Informationen über ZAO Kaspersky Lab.

Informationen über den Code von Drittherstellern

Dieser Abschnitt enthält Informationen über den Code von Drittherstellern, der im Programm verwendet wird.

Markeninformationen

In diesem Abschnitt werden die Marken von Drittanbietern (Rechteinhabern) genannt.

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben in diesem Dokument.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Das Dokument enthält Textelemente (Warnungen, Tipps, Beispiele), die besondere Beachtung verdienen.

Zur Hervorhebung solcher Elemente werden spezielle Formatierungen verwendet. Ihre Bedeutung wird mit Beispielen in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren darüber, dass unerwünschte Aktionen möglich sind, die zu Datenverlust oder Störungen der Hardware oder des Betriebssystems führen können.
Es wird empfohlen...	Hinweise sind eingerahmt. Hinweise können nützliche Tipps, Empfehlungen und spezielle Einstellungswerte enthalten oder sich auf wichtige Sonderfälle bei der Arbeit mit dem Programm beziehen.
Beispiel: ...	Beispiele befinden sich in gelb unterlegten Blöcken und sind mit "Beispiel" überschrieben.
Das <i>Update</i> ist... Das Ereignis <i>Die Datenbanken sind veraltet</i> tritt ein.	Folgende Textelemente sind kursiv geschrieben. <ul style="list-style-type: none"> • neue Begriffe • Namen von Statusvarianten und Programmereignissen
Klicken Sie auf Aktivieren .	Die Namen von Elementen der Programmoberfläche sind fett geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).
➔ <i>Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:</i>	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
<Benutzername>	Variable stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.
Senden Sie eine SMS mit dem Text find: <Code> an Ihr Gerät.	Der Text des SMS-Befehls wird speziell hervorgehoben.

INFORMATIONSQLUELLEN ZUM PROGRAMM

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche	8
Diskussion über die Programme von Kaspersky Lab im Forum	9
Kontaktaufnahme mit der Vertriebsabteilung.....	9
Kontaktaufnahme mit der Abteilung für Lokalisierung und technische Dokumentation	9

INFORMATIONSQLUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Sie können folgende Quellen verwenden, um nach Informationen zum Programm zu suchen:

- Seite auf der Webseite von Kaspersky Lab
- Seite auf der Webseite des Technischen Supports (Wissensdatenbank)
- Elektronisches Hilfesystem
- Dokumentation

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab (s. Abschnitt "Technischer Support am Telefon" auf S. [45](#)).

Um die Informationsquellen auf der Kaspersky-Lab-Webseite zu nutzen, ist eine Internetverbindung erforderlich.

Seite auf der Webseite von Kaspersky Lab

Die Kaspersky-Lab-Webseite bietet für jedes Programm eine spezielle Seite.

Auf der Seite (<http://www.kaspersky.com/de/android-security>) finden Sie allgemeine Informationen über die Funktionen und Besonderheiten des Programms.

Auf der Seite <http://www.kaspersky.com/de> befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Die Wissensdatenbank auf der Webseite des Technischen Supports (<http://support.kaspersky.com/de/desktop>) enthält Tipps zur Arbeit mit Kaspersky-Lab-Programmen. Die Wissensdatenbank bietet Hilfeartikel, die nach Themen angeordnet sind.

Auf der Seite des Programms finden Sie in der Wissensdatenbank <http://support.kaspersky.com/de/mobile/kisandroid> nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Internet Security können die Artikel auch andere Kaspersky-Lab-Programme betreffen und Neuigkeiten über den Technischen Support enthalten.

Elektronisches Hilfesystem

Das elektronische Hilfesystem des Programms umfasst verschiedene Hilfedateien.

Die Kontexthilfe bietet Informationen über die einzelnen Programmfenster: Liste und Beschreibung der Einstellungen und Liste der entsprechenden Aufgaben.

Die vollständige Hilfe bietet ausführliche Informationen über die Verwaltung des Schutzes, die Programmeinstellungen und die zentralen Aufgaben des Benutzers.

Dokumentation

Das Benutzerhandbuch bietet eine Beschreibung der Programmoberfläche und Lösungswege für typische Aufgaben, die sich dem Anwender bei der Arbeit mit dem Programm stellen.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM FORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum (<http://forum.kaspersky.com/index.php?showforum=26>) diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf des Programms sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung zur Verfügung

- <http://www.kaspersky.de/kontakt>.
- Anfrage per E-Mail an sales@kaspersky.com.

Die Beratung kann auf Englisch oder Russisch erfolgen.

KONTAKTAUFNAHME MIT DER ABTEILUNG FÜR LOKALISIERUNG UND TECHNISCHE DOKUMENTATION

Die Abteilung für Handbücher und Hilfesysteme erreichen Sie per E-Mail über docfeedback@kaspersky.com. Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Internet Security for Android".

KASPERSKY INTERNET SECURITY

Kaspersky Internet Security bietet folgende Hauptfunktionen:

Schutz vor Viren und anderer Malware

Die Komponente Scanner (Anti-Virus) schützt Ihr Gerät vor Viren und anderer Malware.

Diese Komponente heißt in der kostenlosen Version "Scanner" und in der Premium-Version "Anti-Virus".

Mithilfe des Scanners können Sie das gesamte Gerät, die installierten Programme oder einen ausgewählten Ordner auf Viren untersuchen, eine geplante Untersuchung des Geräts anpassen, sowie die Antiviren-Datenbanken aktualisieren, die einen stets aktuellen Schutz Ihrer Daten sicherstellen.

Anti-Virus umfasst alle Funktionen des Scanners und bietet zusätzlich folgende Features:

- Echtzeitschutz für Ihr Gerät
- Untersuchung von neu installierten Programmen vor ihrem ersten Start. Dazu werden die Antiviren-Datenbanken und der Cloud-Service Kaspersky Security Network verwendet.
- Option zum automatischen Update der Antiviren-Datenbanken

Ausblenden von persönlichen Kontakten sowie der Anrufliste und der SMS-Nachrichten für diese Kontakte

Das Ausblenden von persönlichen Kontakten und der dazugehörenden Informationen erfolgt durch die Komponente Privatsphäre.

Die Komponente Privatsphäre ist nur in der Premium-Version von Kaspersky Internet Security verfügbar. Außerdem muss auf den Geräten eine SIM-Karte eingelegt sein.

Die Privatsphäre kann Ihre vertraulichen Kontakte sowie den Anrufverlauf und die SMS-Nachrichten für diese Kontakte vorübergehend verbergen. Sie können das Ausblenden von Kontakten und dazugehörenden Informationen in den Programmeinstellungen oder mithilfe eines speziellen SMS-Befehls aktivieren.

Datenschutz bei Verlust oder Diebstahl des Geräts

Die Komponente Diebstahlschutz dient dazu, Informationen vor unberechtigtem Zugriff zu schützen und das Gerät bei Verlust oder Diebstahl zu orten.

Der Diebstahlschutz bietet folgende ferngesteuerten Optionen: Alarmfunktion auf dem Gerät einschalten, Gerät sperren, Gerät orten, auf dem Gerät gespeicherte Daten löschen und unbemerkt ein Foto der Person machen, die das Gerät gerade verwendet. Mit dem Diebstahlschutz können Sie bestimmte Funktionen auf Ihrem Gerät durch spezielle SMS-Befehle oder über das Webportal <https://anti-theft.kaspersky.com> ferngesteuert starten. Wenn das Gerät eine SIM-Karte unterstützt und die SIM-Karte gewechselt wird (oder das Gerät ohne SIM eingeschaltet wird), kann der Diebstahlschutz per SMS oder E-Mail über die neue Telefonnummer informieren oder das Gerät sperren.

Sperrung von unerwünschten Anrufen und SMS

Zum Sperren von unerwünschten eingehenden Anrufen und SMS dient die Komponente Anruf- und SMS-Filter.

Die Komponente Anruf- und SMS-Filter funktioniert nur auf Geräten mit eingelegter SIM-Karte.

Schutz vor IT-Bedrohungen

Der Schutz vor IT-Bedrohungen wird durch die Komponenten Web-Filter und SMS-Anti-Phishing realisiert.

Die Komponenten Web-Filter und SMS-Anti-Phishing sind nur in der Premium-Version von Kaspersky Internet Security verfügbar.

Die Komponente SMS-Anti-Phishing funktioniert nur auf Geräten mit eingelegter SIM-Karte.

Der Web-Filter blockiert schädliche Webseiten, deren Ziel darin besteht, schädlichen Code zu verbreiten, sowie gefälschte Webseiten (Phishing-Seiten), die Ihre persönlichen Daten stehlen und sich Zugang zu Ihren Finanzkonten verschaffen können.

SMS-Anti-Phishing sperrt Links, die in einer SMS enthalten sind und zu schädlichen oder gefälschten Webseiten führen.

IN DIESEM ABSCHNITT

Hard- und Softwarevoraussetzungen.....	11
Lieferumfang.....	11
Service für Benutzer.....	12

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky Internet Security for Android zu gewährleisten, muss das Gerät folgende Voraussetzungen erfüllen:

- Smartphones und Tablets mit einer Bildschirmauflösung von 320x480 Pixel
- 65 MB freier Speicherplatz im Hauptspeicher des Geräts
- Betriebssystem Android™ 2.3.x – 4.4.x
- Prozessor-Architektur Intel® Atom™ x86, ARM5, ARM6 oder ARM7

Das Programm wird nur im Hauptspeicher des Gerätes installiert.

Um die Funktionen der Komponenten Anruf- und SMS-Filter, Privatsphäre, SIM-Kontrolle und SMS-Anti-Phishing zu nutzen, muss im Gerät eine SIM-Karte eingelegt sein.

LIEFERUMFANG

Sie können das Programm folgendermaßen kaufen:

- **In einer Box.** Verkauf über unsere Vertriebspartner.
- **Über den Online-Shop.** Verkauf über einen **Online-Shop** von Kaspersky Lab (beispielsweise <http://www.kaspersky.com/de/store>) oder unserer Vertriebspartner.
- **Über Google Play Store.** Das Programm wird aus Google Play Store auf das Gerät heruntergeladen.

Wenn Sie das Programm in einer CD-Box erworben haben, umfasst der Lieferumfang folgende Elemente:

- versiegelter Umschlag mit einem QR-Code für den Download des Programms
- kurzes Benutzerhandbuch, das einen Aktivierungscode für das Programm enthält;
- Lizenzvertrag, der die Nutzungsbedingungen für das Programm festlegt.

Der Lieferumfang kann sich je nach Region, in der das Programm vertrieben wird, unterscheiden.

Wenn Sie Kaspersky Internet Security in einem Online-Shop kaufen, kopieren Sie das Programm von der Seite des Online-Shops. Nach Eingang des Rechnungsbetrags erhalten Sie per E-Mail die zur Programmaktivierung erforderlichen Informationen einschließlich eines Aktivierungscodes.

Ausführliche Informationen zum Kauf und Lieferumfang erhalten Sie bei unserer Vertriebsabteilung unter der Adresse sales@kaspersky.com.

SERVICE FÜR BENUTZER

Wenn Sie eine Lizenz für die Nutzung des Programms kaufen, können Sie während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Update der Datenbanken und Nutzung neuer Programmversionen
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung über das Erscheinen neuer Kaspersky-Lab-Programme sowie über das Auftauchen neuer Viren und drohende Virenepidemien. Um diesen Service zu nutzen, muss auf der Webseite des Technischen Supports der Newsletter von Kaspersky Lab abonniert werden.

Die Beratung erstreckt sich nicht auf Fragen über die Funktionsweise von Betriebssystemen, der Software von Drittherstellern und sonstiger Technologien.

INSTALLATION UND DEINSTALLATION DES PROGRAMMS

Dieser Abschnitt bietet genaue Anleitungen für die Installation und Deinstallation von Kaspersky Internet Security for Android.

IN DIESEM ABSCHNITT

Programm installieren	13
Programm deinstallieren	14

PROGRAMM INSTALLIEREN

Sie können Kaspersky Internet Security aus Google Play Store oder aus einem Programmpaket auf Ihr Gerät installieren.

Mit Google Play Store können Sie Kaspersky Internet Security entweder aus dem Programm Google Play Store auf einem Gerät oder von der Webseite <https://play.google.com> auf einem Computer installieren.

Um das Programm mithilfe des Services von Google Play Store zu installieren, müssen folgende Bedingungen erfüllt sein:

- Sie benötigen ein Google-Konto.
- Das Gerät muss mit dem Google-Konto verknüpft sein.
- Auf dem Gerät muss eine Internetverbindung vorhanden sein.

Wie ein Google-Konto erstellt und mit einem Gerät verknüpft wird, und wie das Programm Google Play Store funktioniert, erfahren Sie auf der Seite des technischen Supports von Google <http://support.google.com/googleplay/>.

➡ *Um Kaspersky Internet Security aus dem Programm Google Play Store auf Ihrem Gerät zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie auf Ihrem Gerät das Programm Google Play Store.
2. Suchen Sie nach Kaspersky Internet Security. Geben Sie dazu in der Suchzeile von Google Play Store den Programmnamen ein und drücken Sie die **EINGABE**-Taste.
3. Wählen Sie in der Ergebnisliste **Kaspersky Internet Security** aus.
Eine Seite mit ausführlichen Angaben zu Kaspersky Internet Security wird geöffnet.
4. Klicken Sie auf der Seite mit den Programmdetails auf **Installieren**.
5. Hier finden Sie eine Liste mit den Rechten, die das Programm Kaspersky Internet Security benötigt. Wenn Sie einverstanden sind, dem Programm diese Rechte zu gewähren, klicken Sie auf **Akzeptieren und herunterladen**.
Kaspersky Internet Security wird heruntergeladen und installiert.
6. Wenn Sie dem Programm Kaspersky Internet Security diese Rechte nicht gewähren möchten, klicken Sie auf **Zurück**.

In diesem Fall wird die Programminstallation abgebrochen.

➤ Um Kaspersky Internet Security von der Webseite <https://play.google.com> über einen Computer zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie auf dem Computer die Webseite <https://play.google.com>.
2. Suchen Sie nach Kaspersky Internet Security. Geben Sie dazu in der Suchzeile von Google Play Store den Programmnamen ein und drücken Sie die **EINGABE**-Taste.
3. Wählen Sie in der Ergebnisliste **Kaspersky Internet Security** aus.
Eine Seite mit ausführlichen Angaben zu Kaspersky Internet Security wird geöffnet.
4. Klicken Sie auf der Seite mit den Programmdetails auf **Installieren**.
Wenn Sie nicht bei Google Play angemeldet sind, wird ein Fenster geöffnet, in dem Sie sich mit Ihrem Google-Konto anmelden können.
Wenn Sie bereits bei Google Play angemeldet waren, wird ein Fenster für die Bestellung geöffnet.
5. Wählen Sie im Bestellfenster im Dropdown-Menü **An folgendes Gerät senden** das Gerät aus, auf dem das Programm installiert werden soll. Die Liste enthält alle Geräte, die mit Ihrem Google-Konto verknüpft sind.
6. Im Bestellfenster finden Sie eine Liste mit den Rechten, die das Programm benötigt. Wenn Sie einverstanden sind, dem Programm diese Rechte zu gewähren, klicken Sie auf **Installieren**.
Wenn Ihr Gerät mit einem Wi-Fi- oder 3G/4G-Netzwerk verbunden ist, beginnt unverzüglich der Download des Programms. Wenn Ihr Gerät nicht mit dem Internet verbunden ist, wird die Anwendung automatisch auf das Gerät heruntergeladen, sobald es mit dem Internet verbunden wird.
7. Wenn Sie dem Programm die genannten Rechte nicht gewähren möchten, klicken Sie auf **Abbrechen**.
In diesem Fall wird die Programminstallation abgebrochen.

➤ Um Kaspersky Internet Security aus einem Programmpaket zu installieren, gehen Sie wie folgt vor:

1. Kopieren Sie die Distribution auf das Gerät. Führen Sie eine der folgenden Aktionen aus:
 - Wenn das Programmpaket bereits heruntergeladen und auf einem PC gespeichert wurde, verbinden Sie das Gerät mit dem Computer und kopieren Sie das Programmpaket auf das Gerät.
 - Die Programmdateien werden aus dem Online-Shop von Kaspersky Lab (<http://www.kaspersky.com/de/store>) oder aus dem Shop unserer Vertriebspartner heruntergeladen.
2. Starten Sie die Programminstallation. Öffnen Sie dazu auf dem Gerät das APK-Archiv der Distribution.

Der Installationsassistent des Programms wird gestartet. Der Assistent installiert das Programm mit den von Kaspersky Lab empfohlenen Einstellungen.

PROGRAMM DEINSTALLIEREN

➤ Um Kaspersky Mobile Security zu entfernen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Programm entfernen**
2. Geben Sie den Geheimcode für das Programm ein, falls Sie einen Code festgelegt haben (s. Abschnitt "Zweck des Geheimcodes" auf S. [26](#)).
Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie den Code wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. [43](#)).
Falls Sie keinen Geheimcode festgelegt haben, gehen Sie zum nächsten Schritt.
3. Entfernen des Programms bestätigen.

Das Entfernen des Programms beginnt. Wenn die Datenausblendung aktiviert war, wird sie automatisch deaktiviert (s. Abschnitt "Privatsphäre" auf S. [31](#)).

Kaspersky Lab warnt davor, Kaspersky Internet Security zu entfernen, da dann die Sicherheit Ihres Geräts und Ihrer persönlichen Daten bedroht ist.

PROGRAMMOBERFLÄCHE

Dieser Abschnitt informiert über die wichtigsten Elemente der grafischen Programmoberfläche: Hauptfenster, Indikator für den Schutzstatus in Form eines Schilds, Schnellstartleiste, Programmsymbol, Widget und Meldungsfenster.

IN DIESEM ABSCHNITT

Hauptfenster von Kaspersky Internet Security.....	15
Indikator für den Schutzstatus in Form eines Schilds	16
Schnellstartleiste	17
Symbol im Infobereich der Taskleiste	18
Widget für das Hauptfenster des Geräts	19
Benachrichtigungen.....	19

HAUPTFENSTER VON KASPERSKY INTERNET SECURITY

Mit den Elementen des Programmhauptfensters (s. Abb. unten) können Sie auf die Hauptfunktionen des Programms zugreifen.



Abbildung 1. Hauptfenster

Das Aussehen des Hauptfensters kann für unterschiedliche Bildschirmauflösungen geringfügig differieren.

In der Schnellstartleiste können unterschiedlich viele Schaltflächen vorhanden sein. Dies ist von den verfügbaren Funktionen abhängig.

INDIKATOR FÜR DEN SCHUTZSTATUS IN FORM EINES SCHILDS

Der Indikator für den Schutzstatus besitzt die Form eines Schilds und befindet sich in der Mitte des Hauptfensters (s. Abb. unten).



Abbildung 2. Schild in der Mitte des Hauptfensters

Die Farbe des Schilds ist vom Schutzstatus des Geräts abhängig:

- Grün – Der Schutz des Geräts entspricht dem erforderlichen Niveau. Alle Schutzkomponenten funktionieren mit den von Kaspersky Lab empfohlen Einstellungen. Die Datenbanken von Kaspersky Internet Security wurden rechtzeitig aktualisiert. Bei der Untersuchung des Geräts wurden keine schädlichen Objekte gefunden oder alle gefundenen schädlichen Objekte wurden vom Programm neutralisiert.
- Gelb – Reduziertes Schutzniveau, in Kaspersky Internet Security liegen Probleme vor. Beispiel: Das Gerät wurde seit über 14 Tagen nicht mehr untersucht oder ein neues ungeprüftes Programm wurde installiert.
- Rot – Es liegen Probleme vor, die zur Infektion des Geräts und zu Datenverlust führen können. Beispielsweise: Bestimmte Schutzkomponenten wurden angehalten oder die Antiviren-Datenbanken wurden seit über 14 Tage nicht aktualisiert.

Durch Klick auf den Schild im Programmhauptfenster können Sie den Abschnitt **Status** öffnen (s. Abb. unten). Der Abschnitt **Status** bietet ausführliche Informationen über den Schutzstatus des Geräts sowie eine Problemliste mit entsprechenden Lösungsmöglichkeiten.

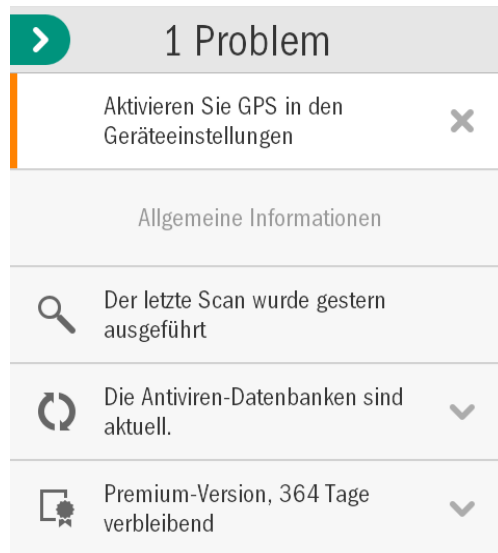


Abbildung 3. Abschnitt Status

Die Probleme, die im Schutz vorliegen, sind nach Kategorien angeordnet. Für jedes Problem werden Aktionen genannt, die Sie zur Problemlösung ausführen können.

Für Probleme, die den Schutz betreffen, werden zwei Arten unterschieden:

- *Informativ.* Gelb hervorgehoben. Informative Probleme informieren über Ereignisse, die für die Sicherheit des Geräts wichtig sind (z. B. darüber, dass die letzte Untersuchung vor über 14 Tagen erfolgte oder dass ein neues ungeprüftes Programm installiert wurde). Eine informative Benachrichtigung kann durch Streichen nach links ausgeblendet werden. Informationen über das Problem stehen weiterhin im Menü **Ausgeblendete Probleme** zur Verfügung.
- *Kritisch.* Rot hervorgehoben. Kritische Probleme informieren über Ereignisse, die höchste Wichtigkeit für die Sicherheit des Geräts besitzen (z. B. Erscheinen einer neuen Programmversion oder die Antiviren-Datenbanken wurden lange nicht mehr aktualisiert). Kritische Probleme können nicht ausgeblendet werden.

SCHNELLSTARTLEISTE

Über die Schnellstartleiste gelangen Sie zur den wichtigsten Programmfunktionen (s. Abb. unten).

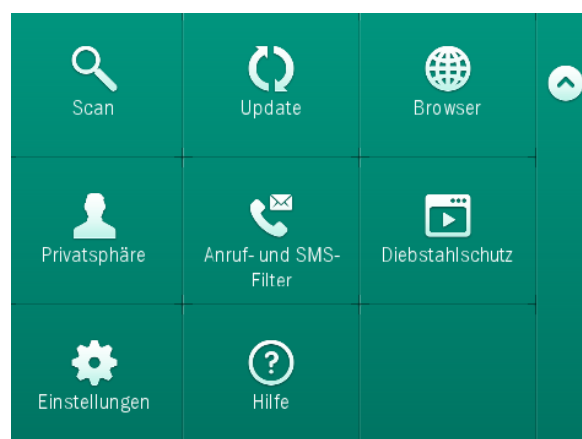











Abbildung 4. Schnellstartleiste

Die Schnellstartleiste ist standardmäßig ausgeblendet. Um die Schnellstartleiste aufzuklappen, können Sie die Leiste nach oben ziehen oder auf die Schaltfläche  klicken.

In der Schnellstartleiste können unterschiedlich viele Schaltflächen vorhanden sein. Dies ist von den verfügbaren Funktionen abhängig.

Die folgende Tabelle enthält Werte für die einzelnen Schaltflächen in der Schnellstartleiste.

Tabelle 2. Funktionen der Schaltflächen auf der Schnellstartleiste

SCHALTFLÄCHE	BEDEUTUNG
 (Scan)	Startet eine Untersuchung des gesamten Geräts, nur der installierten Programme, eines bestimmten Ordners oder einer Datei.
 (Update)	Startet eine Aktualisierung der Antiviren-Datenbanken und der Programmversion. Dadurch wird der Schutz des Geräts auf dem neuesten Stand gehalten.
 (Browser)	Öffnet den Android-Standardbrowser, in dem die Untersuchung von Webseiten auf Viren und Phishing aktiviert ist.
 (Privatsphäre)	Verbirgt die zuvor ausgewählten persönlichen Kontakte und dazugehörige Informationen vorübergehend oder zeigt diese an.
 (Anruf- und SMS-Filter)	Führt zur Auswahl eines Filtermodus für unerwünschte Anrufe und SMS.
 (Webportal)	Öffnet das Webportal, um die Diebstahlschutz-Funktionen auf dem Gerät ferngesteuert zu verwalten.
 (Einstellungen)	Öffnet das Programmkonfigurationsfenster.
 (Hilfe)	Öffnet die Hilfe für das Programm.




SYMBOL IM INFOBEREICH DER TASKLEISTE

Nachdem der Anpassungs-Assistent ausgeführt wurde, erscheint das Symbol von Kaspersky Internet Security in der Statusleiste.

Das Symbol dient als Indikator für das Programm und bietet Zugriff auf das Programmhauptfenster.

Indikator für die Programmarbeit

Das Symbol dient als Indikator für die Arbeit des Programms. In der Premium-Version zeigt das Programmsymbol den Schutzstatus Ihres Geräts an:

-  (farbiges Symbol) – Der Schutz funktioniert.
-  (schwarz-weißes Symbol) – Der Schutz ist deaktiviert.
-  (farbiges Symbol mit einem Ausrufezeichen) – Im Schutz liegen Probleme vor. Beispiele: Die Antiviren-Datenbanken sind veraltet oder ein neues ungeprüftes Programm wurde installiert.

In der kostenlosen Programmversion zeigt das Programmsymbol den Schutzstatus Ihres Geräts nicht an.

Zugriff auf das Programmhauptfenster

Über das Programmsymbol in der Taskleiste können Sie das Programmhauptfenster öffnen.

WIDGET FÜR DAS HAUPTFENSTER DES GERÄTS

Bei der Verwendung von Kaspersky Internet Security for Android steht Ihnen ein Startbildschirm-Widget zur Verfügung (s. Abb. unten).



Abbildung 5. Startbildschirm-Widget

Über das Widget können Sie zum Programmhauptfenster wechseln.

In der Premium-Version des Programms wird der Schutzstatus Ihres Geräts durch die Farbe des Startbildschirm-Widgets signalisiert. In der Premium-Version des Programms kann die Farbe des Widgets außerdem über das Verbergen von vertraulichen Kontakten und dazugehörigen Informationen informieren, falls dies in den Widget-Einstellungen erlaubt wurde.

Für das Widget gilt folgender Farbcode:

- Ein grüner Schild bedeutet, dass der Schutz aktiviert ist;
- Ein grauer Schild bedeutet, dass der Schutz deaktiviert ist.
- Grüner Hintergrund bedeutet, dass das Programm vertrauliche Kontakte und dazugehörige Informationen verbirgt;
- Grauer Hintergrund bedeutet, dass das Programm vertrauliche Kontakte und dazugehörige Informationen anzeigt.

In der kostenlosen Programmversion zeigt die Widget-Farbe keinen Schutzstatus des Geräts an.

BENACHRICHTIGUNGEN

Kaspersky Internet Security benachrichtigt Sie mithilfe von *Meldungsfenstern* und *Pop-up-Benachrichtigungen*, die in der Statuszeile angezeigt werden, über wichtige Ereignisse, die während der Programmausführung eintreten.

Meldungsfenster werden von Kaspersky Internet Security auf dem Bildschirm angezeigt, wenn im Hinblick auf ein Ereignis Varianten für das weitere Vorgehen bestehen. Beispiel: Wenn ein schädliches Objekt gefunden wurde, dessen Desinfektion nicht möglich ist, können Sie das Objekt löschen, es überspringen oder eine Hilfe öffnen, die über die mit dem Objekt möglichen Aktionen informiert (s. Abb. unten). Das Programm bietet Ihnen Aktionen zur Auswahl. Das Meldungsfenster wird erst dann geschlossen, wenn Sie eine der vorgeschlagenen Optionen auswählen.

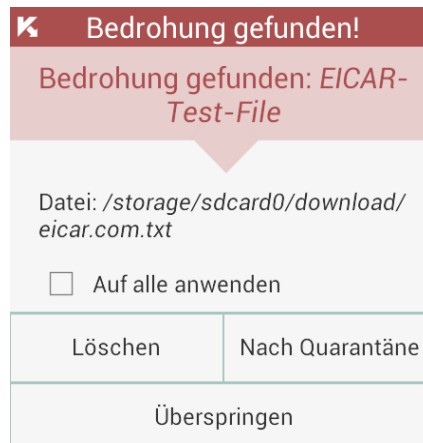


Abbildung 6. Fenster Meldungen

Die *Pop-up-Benachrichtigungen* in der Statuszeile informieren über Ereignisse, die keine Aktion seitens des Benutzers erfordern (s. Abb. unten). Die Meldungen können Sie später in der Taskleiste Ihres Geräts ansehen.

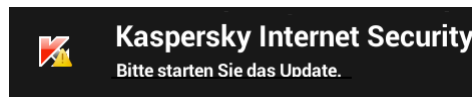


Abbildung 7. Pop-up-Meldungen

In Abhängigkeit davon, welche Relevanz ein Ereignis für die Sicherheit des Geräts besitzt, werden drei Typen von Benachrichtigungen unterschieden:

- Kritische Benachrichtigungen informieren über Ereignisse, die vorrangige Priorität für die Sicherheit des Geräts besitzen (beispielsweise Fund einer schädlichen Datei). Kritische Benachrichtigungen sind rot hervorgehoben.
- Wichtige Benachrichtigungen informieren über Ereignisse, die für die Sicherheit des Geräts potenziell wichtig sind (beispielsweise Start einer Untersuchung oder eines Updates). Wichtige Benachrichtigungen sind grün hervorgehoben.
- Informative Benachrichtigungen informieren über Ereignisse, die keine vorrangige Relevanz für die Sicherheit des Geräts besitzen. Informative Benachrichtigungen sind nicht farblich hervorgehoben.

LIZENZIERUNG DES PROGRAMMS

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag.....	21
Über die Lizenz	21
Über den Aktivierungscode	22
Über die Bereitstellung von Daten	22

ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie beginnen, mit dem Programm zu arbeiten.

Wenn Sie bei der Programminstallation dem Text des Lizenzvertrags zustimmen, gelten die Bedingungen des Lizenzvertrags als akzeptiert. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen oder das Programm nicht verwenden.

ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags gewährt wird.

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

- Verwendung des Programms auf einem oder mehreren Geräten.

Die Anzahl der Geräte, auf denen Sie das Programm nutzen dürfen, wird durch den Lizenzvertrag festgelegt.

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Nutzung von sonstigen Leistungen, die Ihnen von Kaspersky Lab oder den Vertriebspartnern während der Gültigkeitsdauer der Lizenz angeboten werden. (s. Abschnitt "Service für Benutzer" auf S. [12](#))

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer des Programms sind von der Programmversion abhängig.

Folgende Programmversionen sind vorgesehen:

- *Kostenlose Version.* Die kostenlose Version bietet eine eingeschränkte Funktionalität von Kaspersky Internet Security und ist zeitlich unbeschränkt. Die Einschränkungen der kostenlosen Version sind im Lizenzvertrag angegeben. Die kostenlose Version ist sofort nach der Programminstallation verfügbar. Von der kostenlosen Version können Sie zur Testversion oder zur Premium-Version des Programms wechseln.
- *Testversion.* Mit der Testversion können Sie innerhalb der Testdauer kostenlos alle Programmfunktionen nutzen.

Von der Testversion können Sie zur Premium-Version oder zur kostenlosen Version des Programms wechseln. Beim Ablauf der Testdauer wechselt das Programm automatisch zur kostenlosen Version.

- *Premium-Version.* Die Premium-Version bietet Zugriff auf alle Programmfunktionen. Die Premium-Version ist an den Kauf einer Lizenz für die Programmnutzung gebunden. Eine Lizenz ist für einen begrenzten Zeitraum gültig.

Bei Ablauf der Lizenz können Sie das Programm weiterhin nutzen. In diesem Fall können Sie die Lizenz verlängern oder zur kostenlosen Programmversion wechseln. Um die Lizenz zu verlängern, können Sie einen neuen Aktivierungscode eingeben, den Sie beim Kauf der Programms erhalten haben, oder online eine neue Lizenz erwerben.

Beim Ablauf der Lizenz wechselt das Programm automatisch zur kostenlosen Version.

ÜBER DEN AKTIVIERUNGSCODE

Einen *Aktivierungscode* erhalten Sie beim Kauf einer Lizenz für die Nutzung von Kaspersky Internet Security. Der Code ist für die Programmaktivierung erforderlich.

Ein Aktivierungscode besteht aus einer unikal Folge von zwanzig Ziffern und lateinischen Buchstaben im Format XXXXX-XXXXX-XXXXX-XXXXX.

Abhängig davon, auf welche Weise das Programm gekauft wird, bestehen folgende Varianten für die Lieferung des Aktivierungscodes:

- Wenn Sie Kaspersky Internet Security in einer CD-Box gekauft haben, ist der Aktivierungscode in der Dokumentation oder auf der Verpackung angegeben, in der sich die Installations-CD befindet.
- Wenn Sie Kaspersky Internet Security in einem Online-Shop gekauft haben, erhalten Sie den Aktivierungscode per E-Mail an die Adresse, die Sie bei der Bestellung angegeben haben.

Die Laufzeit einer Lizenz wird ab dem Datum der Programmaktivierung gerechnet. Wenn Sie eine Lizenz gekauft haben, mit der Kaspersky Internet auf mehreren Geräten genutzt werden kann, so beginnt die Laufzeit der Lizenz, wenn der Aktivierungscode zum ersten Mal verwendet wird.

Wenn ein Aktivierungscode nach der Programmaktivierung verloren geht oder versehentlich gelöscht wurde, wenden Sie sich zur Wiederherstellung an den Technischen Support von Kaspersky Lab.

ÜBER DIE BEREITSTELLUNG VON DATEN

Um den Schutz zu optimieren, verwendet Kaspersky Internet Security für folgende Komponenten den Cloud-Service Kaspersky Security Network (s. Abschnitt "Kaspersky Security Network (KSN)" auf S. [47](#)):

- **Scan.** Das Programm führt eine zusätzliche Untersuchung der zu installierenden Programme vor deren erstem Start durch. Die Untersuchung bezieht sich auf neue Bedrohungen, über die es in den Antiviren-Datenbanken noch keine Informationen gibt.
- **Web-Filter.** Das Programm führt eine zusätzliche Untersuchung von Webseiten durch, bevor sie geöffnet werden.
- **SMS-Anti-Phishing.** Das Programm sperrt Links, die in einer SMS enthalten sind und zu schädlichen oder gefälschte Webseiten (Phishing-Seiten) führen.

Sie können in der Lizenzvereinbarung nachlesen, welche Daten bei der Benutzung des Cloud-Dienstes während der Ausführung von Kaspersky Internet Security auf den mobilen Geräten der Benutzer an Kaspersky Lab übertragen werden. Wenn Sie die Lizenzvereinbarung akzeptieren, stimmen Sie damit auch zu, dass automatisch folgende Informationen an Kaspersky Lab übertragen werden:

- über ein verwendetes WLAN
- über auf dem Gerät installierte Hard- und Software
- über die Kontrollsummen der verarbeiteten Dateien (MD5 und SHA-256)
- über die Typen der gefundenen Bedrohungen, die Verarbeitungsergebnisse und die installierten Antiviren-Datenbanken
- über die Webadressen, deren Reputation ermittelt wurde, einschließlich Daten über die Verbindungsprotokoll-ID und die Nummer des verwendeten Ports
- über die Aktivierung und über die eingesetzte Version von Kaspersky Internet Security
- über die unikale Geräte-ID
- über die Ergebnisse der heuristischen Analyse
- über die unikale Benutzer-ID
- über die Verbindungs-ID für das Webportal und über den Verbindungsstatus
- über die installierten Programme

Zusätzlich können zum Zweck einer Untersuchung an Kaspersky Lab Dateien und Dateibestandteile gesendet werden, die von Angreifern benutzt werden können, um das Gerät oder die Benutzerdaten zu beschädigen.

Keine der erhaltenen Informationen enthalten persönlichen Daten oder sonstige vertrauliche Informationen des Benutzers.

Die erhaltenen Informationen werden von Kaspersky Lab gemäß den gesetzlich vorgeschriebenen Anforderungen geschützt. Kaspersky Lab verwendet diese Informationen nur in Form einer allgemeinen Statistik. Die Daten der allgemeinen Statistik werden automatisch aus den gesammelten Quellinformationen ermittelt und enthalten keinerlei persönliche oder sonstige vertrauliche Informationen. Die gesammelten Quellinformationen werden in verschlüsselter Form gespeichert und regelmäßig gelöscht (2 Mal jährlich). Die Daten der allgemeinen Statistik werden unbegrenzt gespeichert.

PROGRAMM STARTEN UND BEENDEN

Kaspersky Internet Security wird in der Grundeinstellung automatisch beim Hochfahren des Betriebssystems gestartet und schützt Ihr Gerät während der gesamten Sitzung.

Sie können das Programm beenden, indem Sie Kaspersky Internet Security löschen oder alle Programmkomponenten deaktivieren.

Kaspersky Lab warnt davor, alle Komponenten von Kaspersky Internet Security zu deaktivieren, da dann die Sicherheit Ihres Geräts und Ihrer persönlichen Daten bedroht ist.

ERSTE-SCHRITTE-HANDBUCH

Dieser Abschnitt informiert über die ersten Schritt nach der Programminstallation.

- Anleitungen für das Vorgehen beim Fund eines schädlichen Objekts
- Hinweise für den Schutz privater Daten vor unberechtigtem Zugriff
- Anleitungen für das Vorgehen bei Verlust oder Diebstahl des Geräts

IN DIESEM ABSCHNITT

Vorgehensweise beim Fund eines schädlichen Objekts	25
Daten vor unerlaubtem Zugriff schützen	25
Vorgehensweise bei Verlust oder Diebstahl des Geräts	27

VORGEHENSWEISE BEIM FUND EINES SCHÄDLICHEN OBJEKTS

Wird beim Start einer Anwendung (z. B. eines Spiels) ein Sicherheitsrisiko für Ihr Gerät erkannt, so bietet Kaspersky Internet Security Varianten für das Vorgehen mit der Anwendung an. Folgende Aktionen stehen zur Auswahl:

- **Nach Quarantäne** – Das Programm verschiebt die Anwendung in die Quarantäne.
- **Löschen** – Das Programm löscht die Anwendung.
- **Überspringen** – Das Programm führt keine Aktion mit der Anwendung aus.

Die Kaspersky-Lab-Experten empfehlen, gefundene Bedrohungen zu löschen.

Wird bei einer Untersuchung von Dateien ein schädliches Objekt erkannt, so verschiebt Kaspersky Internet Security das Objekt standardmäßig in die Quarantäne und informiert Sie über die Neutralisierung des Objekts.

Informationen über gefundene schädliche Objekte finden Sie in den Abschnitten **Status** und **Berichte**.

DATEN VOR UNERLAUBTEM ZUGRIFF SCHÜTZEN

Kaspersky Internet Security schützt persönliche Daten vor unerlaubtem Zugriff. Dazu dienen folgende Schutzverfahren:

- Festlegen eines Geheimcodes, mit dem ein unberechtigter Zugriff auf die Einstellungen der Komponenten Diebstahlschutz und Privatsphäre verhindert wird.
- Einstellungen für den Diebstahlschutz anpassen

Der Diebstahlschutz wird mithilfe von SMS-Befehlen und Befehlen aus dem Webportal <https://anti-theft.kaspersky.com> verwaltet. Um die Verwaltung der Diebstahlschutz-Funktionen über das Portal zu ermöglichen, muss im Webportal ein Benutzerkonto erstellt werden.

Der Schutz Ihrer Daten vor unerlaubtem Zugriff setzt voraus: Registrierung im Webportal für den Diebstahlschutz, Festlegen eines Geheimcodes für den Zugriff auf die Programmeinstellungen, und entsprechende Einstellungen auf dem Gerät.

IN DIESEM ABSCHNITT

Zweck des Geheimcodes.....	26
Was ist ein Kaspersky Account?	26
Erstkonfiguration des Diebstahlschutzes	26

ZWECK DES GEHEIMCODES

Der *Geheimcode* für das Programm wird in folgenden Fällen verwendet:

- für den Zugriff auf die Einstellungen der Komponenten Diebstahlschutz und Privatsphäre
- beim Senden eines SMS-Befehls von einem anderen mobilen Gerät aus, um die Alarmfunktion ferngesteuert einzuschalten, das Gerät zu sperren, das Gerät zu orten, Daten vom Gerät zu löschen oder vertrauliche Kontakte und dazugehörige Informationen auszublenden.

Bei der Erstkonfiguration des Diebstahlschutzes (s. Abschnitt "Erstkonfiguration des Diebstahlschutzes" auf S. [26](#)) oder beim ersten Start der Privatsphäre wird Ihnen vorgeschlagen, einen Geheimcode für das Programm festzulegen. Der aktuelle Geheimcode des Programms kann später geändert werden.

Der Geheimcode des Programms besteht aus Ziffern. Der Geheimcode muss mindestens vier Ziffern lang sein.

Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie den Code wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. [43](#)).

WAS IST EIN KASPERSKY ACCOUNT?

Sie benötigen ein Benutzerkonto, um folgende Funktionen über das Webportal <https://anti-theft.kaspersky.com> fernzusteuern: Alarmfunktion auf dem Gerät einschalten, Gerät sperren, Gerät orten, Daten vom Gerät löschen oder unbemerkt die Person fotografieren, die Ihr Gerät gerade verwendet. Außerdem können Sie über das Webportal den Geheimcode für Kaspersky Internet Security wiederherstellen, falls Sie ihn vergessen haben.

Kaspersky Account ist ein universelles Benutzerkonto, mit dem Sie sich bei allen Diensten von Kaspersky Lab anmelden können. Wenn Sie sich bei Diensten wie Mein Kaspersky Account registriert haben oder ein Benutzerkonto für das Webportal <https://anti-theft.kaspersky.com> besitzen, so verfügen Sie bereits über einen Kaspersky Account.

Das Benutzerkonto können Sie bei der Erstkonfiguration des Diebstahlschutzes (s. Abschnitt "Erstkonfiguration des Diebstahlschutzes" auf S. [26](#)) angeben. Als Benutzername dient Ihre E-Mail-Adresse. Falls Sie das Kennwort für die Anmeldung am Webportal vergessen haben, können Sie es wiederherstellen.

ERSTKONFIGURATION DES DIEBSTAHLSCHUTZES

Nach der Programminstallation sind die Diebstahlschutz-Funktionen standardmäßig deaktiviert: Die Funktionen lassen sich nicht ferngesteuert über das Webportal oder mit SMS-Befehlen starten. Um die Diebstahlschutz-Funktionen zu aktivieren, ist eine Erstkonfiguration des Diebstahlschutzes notwendig.

Nach der Erstkonfiguration werden alle Diebstahlschutz-Funktionen mit den von Kaspersky Lab empfohlenen Einstellungen aktiviert.

Der Schnellstartassistent für den Diebstahlschutz wird einmal ausgeführt. Der Diebstahlschutz kann später in den Programmeinstellungen angepasst werden.

➤ *Um die Erstkonfiguration des Diebstahlschutzes vorzunehmen, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Diebstahlschutz**.
Starten Sie den Assistenten für die Erstkonfiguration des Diebstahlschutzes.
2. Folgen Sie den Anweisungen des Assistenten.

➤ *Um die Einstellungen für den Diebstahlschutz nach der Erstkonfiguration zu ändern,*

klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Diebstahlschutz**.

VORGEHENSWEISE BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Bei Diebstahl oder Verlust des Geräts können Sie ferngesteuert die Kontakte und die dazugehörigen Informationen verbergen und die Diebstahlschutz-Funktionen starten: Alarmfunktion einschalten, Gerät sperren, auf dem Gerät gespeicherte Daten löschen, Gerät orten oder unbemerkt die Person fotografieren, die das Gerät gerade verwendet.

Sie können die Diebstahlschutz-Funktionen über das Webportal <https://anti-theft.kaspersky.com> oder mithilfe spezieller SMS-Befehle von einem beliebigen Gerät aus ferngesteuert starten.

Sie können Kontakte und dazugehörige Informationen nur mithilfe eines speziellen SMS-Befehls ferngesteuert verbergen.

Das Verbergen von Kontakten und dazugehörigen Informationen ist nur möglich, wenn auf Ihrem Gerät die Premium-Version von Kaspersky Mobile Security aktiviert ist.

Sie können einen Befehl senden, um die Person zu fotografieren, die Ihr Gerät gerade verwendet. Dieser Befehl ist nur über das Webportal <https://anti-theft.kaspersky.com> möglich. Dieser Befehl kann nicht per SMS gesendet werden.

Für das Senden einer SMS fallen auf dem Gerät, von dem der SMS-Befehl gesendet wird, die tarifgemäßen Gebühren an.

Der ferngesteuerte Start der Diebstahlschutz-Funktionen und der Datenausblendung ist unter folgenden Bedingungen möglich:

- Kaspersky Internet Security ist als Geräteadministrator festgelegt.
- Das Gerät ist zum Empfang von Mobilfunksignalen bereit.
- Auf dem Gerät ist der Start der Diebstahlschutz-Funktionen und der Datenausblendung erlaubt.

➤ *Um die Diebstahlschutz-Funktionen ferngesteuert über das Webportal zu starten, gehen Sie wie folgt vor:*

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.
3. Wählen Sie das Gerät, für das Sie die Funktionen von Diebstahlschutz ferngesteuert starten möchten.
4. Wählen Sie in den Abschnitten im oberen Fensterbereich des Webportals die Aktionen, die auf dem Gerät ausgeführt werden sollen.

➡ Um mithilfe von SMS-Befehlen ferngesteuert Informationen über Kontakte auszublenden und die Diebstahlschutz-Funktionen zu starten, führen Sie eine der folgenden Aktionen aus:

- Wenn Kaspersky Internet Security for Android auf dem Zweitgerät installiert ist, erstellen Sie dort in Kaspersky Internet Security for Android mithilfe der SMS-Befehlsfunktion einen Befehl und senden Sie diesen an Ihr Gerät (s. Abschnitt "Senden von SMS-Befehlen aus Kaspersky Internet Security for Android" auf S. [34](#)).

Verwenden Sie beim Erstellen des SMS-Befehls den Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.

- Senden Sie eine SMS mit folgendem Text an Ihr Gerät:
 - hide: <Code> – zum Verbergen von vertraulichen Kontakten und dazugehörigen Informationen.
 - alarm: <Code> – zum Einschalten der Alarmfunktion und der Gerätesperre (wobei <Code> für den Geheimcode steht, der auf Ihrem Gerät für Kaspersky Internet Security gilt).
 - find: <Code> – zur Gerätesperre und Ortung.
 - wipe: <Code> – zum Löschen von persönlichen Daten und Daten auf der Speicherkarte.
 - fullreset: <Code> – zum Löschen aller Daten vom Gerät und zum Zurücksetzen auf die Werkseinstellungen.

Nachdem alle Daten gelöscht wurden und das Gerät auf die Werkseinstellungen zurückgesetzt wurde, kann das Gerät keine weiteren ferngesteuerten Befehle empfangen und ausführen.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt bietet genaue Anleitungen für die wichtigsten Aufgaben, die der Benutzer mit dem Programm lösen kann.

IN DIESEM ABSCHNITT

Scanner (Anti-Virus)	29
Privatsphäre	31
Diebstahlschutz	33
Anruf- und SMS-Filter	38
Web-Filter und SMS-Anti-Phishing	40
Andere Aufgaben.....	41

SCANNER (ANTI-VIRUS)

Diese Komponente heißt in der kostenlosen Version "Scanner" und in der Premium-Version "Anti-Virus".

Scanner (Anti-Virus) dient zur Untersuchung des Geräts sowie zur Erkennung und Neutralisierung von Bedrohungen auf Ihrem Gerät. Mit Kaspersky Internet Security kann der Inhalt des Geräts vollständig oder teilweise untersucht werden, d. h. die Untersuchung lässt sich auf den Inhalt des internen Gerätespeichers oder eines bestimmten Ordners (auch eines Ordners auf einer Speicherkarte) beschränken.

Die Suche nach schädlichen Objekten erfolgt auf Basis von Antiviren-Datenbanken des Programms, die eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger schädlicher Objekte enthalten. Es wird empfohlen, die Antiviren-Datenbanken des Programms regelmäßig zu aktualisieren.

Kaspersky Internet Security lädt die Updates der Antiviren-Datenbanken des Programms von Kaspersky-Lab-Updateservern herunter. Dabei handelt es sich um spezielle Internetseiten, auf denen Updates der Datenbanken für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Um die Antiviren-Datenbanken des Programms zu aktualisieren, muss auf dem Gerät eine Internetverbindung eingerichtet sein. Beim Update der Antiviren-Datenbanken fallen für den Datenverkehr Gebühren gemäß Ihres Mobilfunktarifes an.

IN DIESEM ABSCHNITT

Alles scannen	30
Speicher scannen	30
Ordner und Dateien scannen	30
Automatischer Scan nach Zeitplan	30
Update der Antiviren-Datenbanken und Programm-Upgrade.....	31
Automatisches Update nach Zeitplan	31

ALLES SCANNEN

Mithilfe einer vollständigen Untersuchung des gesamten Geräts auf Viren und schädliche Programme schützen Sie Ihre Daten und Finanzen, und können Bedrohungen auf Ihrem Gerät (in installierten Programmen und in Installationspaketen) immer rechtzeitig erkennen und beseitigen.

Die meisten Schadprogramme bedrohen insbesondere die persönlichen Benutzerdaten auf einem Gerät: Sie sammeln persönliche Daten des Gerätebesitzers und alle verfügbaren Informationen über das Gerät (wie beispielsweise GPS-Koordinaten und E-Mails) und senden diese an die Angreifer.

Es empfiehlt sich, nach der Installation des Programms das gesamte Dateisystem des Geräts mindestens einmal auf Viren zu untersuchen, um die Sicherheit Ihrer persönlichen Daten sicherzustellen.

➔ *Um das gesamte Dateisystem auf Viren und andere Schadprogramme zu prüfen:*

klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Scan > Alles scannen**.

SPEICHER SCANNEN

Mithilfe der schnellen Untersuchung können Sie nur die installierten Programme scannen.

Wenn Sie eine kostenlose Version nutzen, wird empfohlen, die schnelle Untersuchung nach der Installation neuer Programme zu starten.

➔ *Um eine schnelle Untersuchung zu starten,*

klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Scan > Speicher scannen**.

ORDNER UND DATEIEN SCANNEN

Sie können einen Ordner oder eine Datei im integrierten Gerätespeicher oder auf einer Speicherkarte scannen.

➔ *Gehen Sie folgendermaßen vor, um einen Ordner oder eine Datei zu untersuchen:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Scan > Ordner scannen**.
2. Wählen Sie einen Ordner oder eine Datei für die Untersuchung aus.

AUTOMATISCHER SCAN NACH ZEITPLAN

Sie können den automatischen Start einer vollständigen Untersuchung des Geräts anpassen und einen Zeitplan für den Untersuchungsstart erstellen: Intervall sowie Tag und Uhrzeit für den Start auswählen. Das Programm untersucht automatisch das gesamte Dateisystem gemäß dem erstellten Zeitplan.

Damit die vollständige Untersuchung automatisch gestartet werden kann, muss das Gerät zum Startzeitpunkt in Betrieb sein.

➔ *Gehen Sie folgendermaßen vor, um den automatischen Start der Untersuchung nach Zeitplan anzupassen:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Anti-Virus > Scan-Einstellungen**.
2. Passen Sie ein Intervall für den Start der Untersuchung an. Wählen Sie dazu einen Wert für **Zeitplan**.
3. Legen Sie Tag und Uhrzeit für den Untersuchungsstart fest. Wählen Sie Werte für **Starttag** und **Startzeit** aus.

Die Untersuchung wird nach Zeitplan gestartet.

UPDATE DER ANTIVIREN-DATENBANKEN UND PROGRAMM-UPGRADE

Kaspersky Internet Security verwendet bei der Suche nach schädlichen Programmen die Antiviren-Datenbanken. Die Antiviren-Datenbanken des Programms enthalten eine Beschreibung aller schädlichen Programme, die Kaspersky Lab momentan bekannt sind, entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger schädlicher Objekte. Es wird empfohlen, die Antiviren-Datenbanken des Programms regelmäßig zu aktualisieren.

Neben der Aktualisierung der Antiviren-Datenbanken ermöglicht Kaspersky Internet Security auch ein Upgrade des Programms. Upgrades der Programmversion beheben Schwachstellen von Kaspersky Internet Security, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Um die Antiviren-Datenbanken des Programms zu aktualisieren, muss auf dem Gerät eine Internetverbindung eingerichtet sein.

Haben Sie Kaspersky Internet Security von Google Play heruntergeladen, aktualisiert das Programm nur die Antiviren-Datenbanken. Die Programmversion wird über Google Play aktualisiert.

➔ Um die Antiviren-Datenbanken und die Programmversion zu aktualisieren,

klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Update**.

AUTOMATISCHES UPDATE NACH ZEITPLAN

Sie können den Start des automatischen Updates für die Antiviren-Datenbanken und die Programmversion (im Weiteren "Update") anpassen. Dazu können Sie einen Update-Zeitplan erstellen: Wählen Sie, falls erforderlich, ein Intervall sowie den Tag und die Uhrzeit des Starts aus. Das Programm aktualisiert die Antiviren-Datenbanken und Programmversionen nach dem erstellten Zeitplan.

Das automatische Update ist nur in der Premium-Version von Kaspersky Internet Security verfügbar.

Für die Durchführung des Updates wird eine Internetverbindung benötigt.

Damit das Update zu einer festgelegten Zeit automatisch gestartet werden kann, muss das Gerät zum Startzeitpunkt in Betrieb sein.

➔ Gehen Sie folgendermaßen vor, um einen Startzeitplan für das automatische Update anzupassen:

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Anti-Virus > Update**.
2. Passen Sie ein Intervall für den Start des Updates an. Legen Sie dazu einen Wert für **Zeitplan** fest.
3. Bestimmen Sie einen Tag und eine Uhrzeit für den Start des Updates. Geben Sie dazu Werte für die Parameter **Starttag** und **Startzeit** an.

Das Update wird nach Zeitplan gestartet.

PRIVATSPHÄRE

Mithilfe der Komponente Privatsphäre können Sie Ihre privaten Kontakte sowie den Anrufverlauf und die SMS-Nachrichten für diese Kontakte ausblenden.

Die Komponente Privatsphäre ist nur in der Premium-Version von Kaspersky Internet Security verfügbar. Außerdem muss auf den Geräten eine SIM-Karte eingelegt sein.

Die Privatsphäre bietet folgende Funktionen:

- Erstellen einer Liste für private Kontakte. Die Liste enthält vertrauliche Nummern.
- Ausblenden von Informationen über Kontakte im Telefonbuch, in gelesenen eingehenden SMS-Nachrichten, in weitergeleiteten SMS und in SMS-Entwürfen, sowie von Einträgen über Kontakte in der Anrufliste.
- Sperren von Signalen über den Eingang von SMS-Nachrichten und eingehenden Anrufen von vertraulichen Nummern (Der Anrufer hört in diesem Fall ein "Besetzt"-Zeichen).

Um die Anrufe und SMS-Nachrichten anzuzeigen, die eingegangen sind, während das Verbergen sensibler Daten aktiviert war, muss die Datenausblendung deaktiviert werden. Wenn Sie die Datenausblendung erneut aktivieren, werden die vertraulichen Informationen wieder verborgen.

Sie können die Datenausblendung vom Programm aus oder ferngesteuert mit einem SMS-Befehl aktivieren, der von einem anderen mobilen Gerät aus geschickt wird.

Sie können entweder eine Standard-SMS mit einem speziellen Text schicken oder eine SMS aus Kaspersky Internet Security schicken, falls das Programm auf dem anderen Gerät installiert ist.

Sie können auf Ihrem Gerät den ferngesteuerten Start der Datenausblendung erlauben oder verbieten. Wenn der ferngesteuerte Start der Datenausblendung verboten ist, kann diese Funktion nicht ferngesteuert durch einen SMS-Befehl gestartet werden.

Die Datenausblendung kann nur in dem Programm deaktiviert werden, das auf Ihrem Gerät installiert ist.

Der Zugriff auf die Einstellungen für den Diebstahlschutz ist durch einen Geheimcode geschützt (s. Abschnitt "Zweck des Geheimcodes" auf S. 26). Der Geheimcode wird bei der Erstkonfiguration des Diebstahlschutzes (s. Abschnitt "Erstkonfiguration des Diebstahlschutzes" auf S. 26) festgelegt oder wenn die Privatsphäre zum ersten Mal geöffnet wird.

IN DIESEM ABSCHNITT

Informationen für private Kontakte ausblenden32

Ferngesteuerter Start der Datenausblendung von einem anderen Gerät aus32

INFORMATIONEN FÜR PRIVATE KONTAKTE AUSBLENDEN

➔ *Gehen Sie folgendermaßen vor, um Kontakte und dazugehörige Informationen zu verbergen:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Privatsphäre**.
2. Klicken Sie auf **Verborgene Kontakte**.
3. Geben Sie den Geheimcode für das Programm ein.

Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie den Code wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. 43).

4. Klicken Sie auf **Hinzufügen**, um eine Liste mit zu verbergenden Kontakten zu erstellen.

Die Liste enthält Kontakte, für die Informationen verborgen werden sollen. Falls bereits eine Kontaktliste erstellt wurde, überspringen Sie diesen Schritt.

5. Setzen Sie den Schalter **Privatsphäre** auf **aktiviert**.

FERNGESTEUERTER START DER DATENAUSBLENDUNG VON EINEM ANDEREN GERÄT AUS

Falls erforderlich, können Sie die Kontakte und dazugehörige Informationen auf einem Gerät ferngesteuert verbergen. Dazu müssen Sie von einem anderen Gerät aus einen speziellen SMS-Befehl schicken.

Der ferngesteuerte Start der Datenausblendung unter folgenden Bedingungen möglich:

- Auf dem Gerät, an das der SMS-Befehl gerichtet ist, ist eine Premium-Version des Programms aktiviert.
- Das Gerät ist zum Empfang von Mobilfunksignalen bereit.
- Auf dem Gerät ist der ferngesteuerte Start der Funktion für die Datenausblendung erlaubt.

➔ *Um die Daten auf Ihrem Gerät ferngesteuert auszublenden, führen Sie eine der folgenden Aktionen aus:*

- Erstellen Sie auf dem anderen Gerät in Kaspersky Internet Security mithilfe der SMS-Befehlsfunktion einen Befehl und senden Sie ihn an Ihr Gerät (wenn das Programm auf dem anderen Gerät installiert ist).
- Erstellen Sie auf dem anderen Gerät eine SMS mit dem speziellen Text `hide:<Code>` und senden Sie die SMS an Ihr Gerät. Dabei steht `<Code>` für den Geheimcode von Kaspersky Internet Security auf Ihrem Gerät.

Sie werden durch eine Antwort-SMS über die Befehlsausführung informiert.

Für das Senden eines SMS-Befehls an Ihr Gerät fallen Gebühren gemäß des Mobilfunktarifes an, der auf dem anderen mobilen Gerät gilt.

DIEBSTAHLSCHUTZ

Der Diebstahlschutz schützt Ihre Informationen auf dem Gerät vor unberechtigtem Zugriff und hilft Ihnen, das Gerät bei Verlust oder Diebstahl wiederzufinden.

Mithilfe des Webportals oder der speziellen SMS-Befehle können Sie ferngesteuert folgende Aktionen ausführen:

- Gerät sperren und orten
- Alarmfunktion auf dem Gerät einschalten
- Daten vom Gerät löschen
- Person fotografieren, die das Gerät verwendet

Wenn die SIM-Karte auf dem Gerät ausgetauscht oder das Gerät ohne SIM-Karte eingeschaltet wird, können Sie das Gerät ferngesteuert sperren und die neue Telefonnummer ermitteln. Anschließend können Sie andere Diebstahlschutz-Funktionen auf dem vermissten Gerät starten.

IN DIESEM ABSCHNITT

Gerät zum Benutzerkonto im Webportal hinzufügen.....	34
SMS-Befehle aus Kaspersky Internet Security senden.....	34
Ferngesteuerte Überwachung der SIM-Karte.....	34
Ferngesteuerte Gerätesperre und Ortung.....	35
Ferngesteuertes Einschalten der Alarmfunktion.....	36
Ferngesteuerte Datenlöschung vom Gerät.....	37
Ferngesteuertes Fotografieren.....	38

GERÄT ZUM BENUTZERKONTO IM WEBPORTAL HINZUFÜGEN

Über Ihr Benutzerkonto für den Kaspersky Account im Webportal <https://anti-theft.kaspersky.com> können Sie gleichzeitig mehrere Geräte verwalten.

Um ein Gerät zu Ihrem Benutzerkonto hinzuzufügen, müssen Sie bei der Erstkonfiguration von Kaspersky Internet Security auf dem neuen Gerät die Daten Ihres Benutzerkontos eingeben.

Das neue Gerät wird automatisch mit Ihrem Benutzerkonto verknüpft und ist künftig im Webportal verfügbar.

SMS-BEFEHLE AUS KASPERSKY INTERNET SECURITY SENDEN

Bei Diebstahl oder Verlust Ihres Geräts können Sie ferngesteuert die Diebstahlschutz-Funktionen starten oder vertrauliche Informationen auf dem Gerät verbergen. Dazu müssen entweder über das Webportal <https://anti-theft.kaspersky.com> oder per SMS spezielle Befehle an Ihr Gerät geschickt werden.

Sie können von einem anderen mobilen Gerät aus eine Standard-SMS mit einem speziellen Text an Ihr Gerät schicken (s. Abschnitt "Vorgehensweise bei Verlust oder Diebstahl des Geräts" auf S. 27). Wenn Kaspersky Internet Security auf dem anderen Gerät installiert ist, können Sie von dort aus einen SMS-Befehl schicken. Zum Senden des SMS-Befehls muss der Geheimcode des Programms Kaspersky Internet Security bekannt sein, das auf Ihrem Gerät installiert ist.

Für das Senden eines SMS-Befehls an Ihr Gerät fallen Gebühren gemäß des Mobilfunktarifes an, der auf dem anderen mobilen Gerät gilt.

► *Um von einem Gerät aus, auf dem Kaspersky Internet Security installiert ist, ferngesteuert die Diebstahlschutz-Funktionen zu starten und Daten auszublenden, gehen Sie wie folgt vor:*

1. Öffnen Sie auf dem anderen Gerät das Programm Kaspersky Internet Security.
2. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Diebstahlschutz**.
3. Geben Sie den Geheimcode für das Programm ein.

Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie den Code wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. 43).

4. Klicken Sie auf **SMS-Befehle senden**.
5. Klicken Sie auf **SMS-Befehl jetzt senden**, erstellen Sie einen Befehl und senden Sie ihn an Ihr Gerät. Verwenden Sie beim Erstellen des SMS-Befehls den Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.

Sie werden durch eine Antwort-SMS über die Befehlsausführung informiert.

FERNGESTEUERTE ÜBERWACHUNG DER SIM-KARTE

Wenn die SIM-Karte auf dem Gerät ausgetauscht oder das Gerät ohne SIM-Karte eingeschaltet wird, können Sie das Gerät ferngesteuert sperren und die neue Telefonnummer ermitteln. Anschließend können Sie andere Diebstahlschutz-Funktionen auf dem vermissten Gerät starten.

Sie können sich per SMS oder E-Mail über die neue Telefonnummer informieren lassen. Wenn die Funktion aktiviert ist, wird das verlorene Gerät automatisch gesperrt, falls es ohne SIM-Karte eingeschaltet wird. Wenn eine andere SIM-Karte in das Gerät eingelegt wird, schickt das Programm automatisch eine SMS und eine Nachricht mit der neuen Telefonnummer an die von Ihnen angegebene Telefonnummer und E-Mail-Adresse.

Zum Senden einer E-Mail-Nachricht schickt das Programm eine SMS an eine spezielle Nummer des Mobilfunkanbieters MTS (Russland). Der Mobilfunkanbieter MTS (Russland) schickt die neue Telefonnummer an Ihre E-Mail-Adresse. Die Kosten für das Senden einer SMS an die Servicenummer werden vom Handykonto abgebucht, das der momentan eingelegten SIM-Karte entspricht.

➤ Um die SIM-Kontrolle zu aktivieren, sind folgende Vorkehrungen erforderlich:

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Diebstahlschutz**.
2. Geben Sie den Geheimcode für das Programm ein.
3. Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie den Code wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. 43).
4. Gehen Sie zu **SIM-Kontrolle**.
5. Aktivieren Sie das Kontrollkästchen **SIM-Kontrolle**.
6. Füllen Sie im Abschnitt **Methoden für den Empfang der neuen Telefonnummer und der Geräteposition** die Felder **Telefonnummer** und **E-Mail-Adresse** aus, damit Sie per SMS oder E-Mail über die neue Telefonnummer informiert werden, wenn die SIM-Karte gewechselt wird.
7. Aktivieren Sie im Abschnitt **Gerätesperre** das Kontrollkästchen **Beim Wechsel der SIM-Karte sperren**, damit das Gerät gesperrt wird, falls die SIM-Karte ausgetauscht oder das Gerät ohne SIM eingeschaltet wird.
8. Geben Sie, falls erforderlich, im Feld **Text beim Blockieren** einen Text an, der auf dem Display des gesperrten Geräts erscheinen soll.

FERNGESTEUERTE GERÄTESPERRE UND ORTUNG

Bei Verlust oder Diebstahl Ihres Geräts können Sie über das Webportal <https://anti-theft.kaspersky.com> oder mithilfe des SMS-Befehls find: <Code> das Gerät sperren und orten (<Code> ist der Geheimcode für Kaspersky Internet Security auf Ihrem Gerät).

Für das Senden eines SMS-Befehls an Ihr Gerät fallen Gebühren gemäß des Mobilfunktarifes an, der auf dem anderen mobilen Gerät gilt.

Die ferngesteuerte Sperrung und Ortung des Geräts sind unter folgenden Bedingungen möglich:

- Kaspersky Internet Security ist als Geräteadministrator festgelegt.
- Das Gerät ist zum Empfang von Mobilfunksignalen bereit.
- Der Start dieser Funktion ist auf dem Gerät erlaubt.

Kaspersky Lab empfiehlt außerdem, die GPS-Nutzung in den Geräteeinstellungen zu erlauben, damit das Gerät vom Programm mithilfe von GPS geortet werden kann.

➤ Um Ihr Gerät über das Webportal zu sperren und zu orten, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.
3. Wählen Sie das Gerät aus, das Sie sperren und orten möchten.
4. Klicken Sie auf **Gerätesperre und Ortung**.
5. Bei Bedarf können Sie im Abschnitt **Gerätesperre und Ortung** einen Text eingeben, der auf dem Monitor des gesperrten Geräts angezeigt werden soll. Geben Sie zusätzlich eine E-Mail-Adresse an, an die eine Nachricht mit den Positionskordinaten des Geräts gesendet werden soll.
6. Klicken Sie auf **Sperren und orten**.

Wenn Kaspersky Internet Security Ihr Gerät findet, werden die Gerätekoordinaten im Portal angezeigt und Sie erhalten eine entsprechende E-Mail.

Im Webportal können Sie nur den letzten ermittelten Standort Ihres Geräts auf der Karte anzeigen lassen. Früher ermittelte GPS-Koordinaten werden aus dem Webportal gelöscht. Sie können diese Daten aber in den entsprechenden E-Mail-Nachrichten finden.

➤ *Um Ihr Gerät durch einen SMS-Befehl zu sperren und zu orten, gehen Sie wie folgt vor:*

- Wenn Kaspersky Internet Security for Android auf dem Zweitgerät installiert ist, erstellen Sie dort in Kaspersky Internet Security for Android mithilfe der SMS-Befehlsfunktion einen Befehl und senden Sie diesen an Ihr Gerät (s. Abschnitt "Senden von SMS-Befehlen aus Kaspersky Internet Security for Android" auf S. 34). Verwenden Sie beim Erstellen des SMS-Befehls den Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.
- Senden Sie eine SMS mit folgendem Text an Ihr Gerät find: <Code> (<Code> ist der Geheimcode für Kaspersky Internet Security auf Ihrem Gerät).

Wenn Kaspersky Internet Security Ihr Gerät findet, werden Sie mit einer Antwort-SMS und per E-Mail an die angegebene Adresse über die Gerätekoordinaten informiert.

FERNGESTEUERTES EINSCHALTEN DER ALARMFUNKTION

Bei Verlust oder Diebstahl Ihres Geräts können Sie ferngesteuert die Alarmfunktion auf dem Gerät einschalten (auch wenn der Ton auf dem Gerät deaktiviert ist) und das Gerät sperren. Diese Funktionen werden über das Webportal <https://anti-theft.kaspersky.com> oder mit dem SMS-Befehl alarm: <Code> gesteuert (<Code> ist der Geheimcode für Kaspersky Internet Security auf Ihrem Gerät).

Für das Senden eines SMS-Befehls an Ihr Gerät fallen Gebühren gemäß des Mobilfunktarifes an, der auf dem anderen mobilen Gerät gilt.

Das ferngesteuerte Einschalten der Alarmfunktion ist möglich, wenn das Gerät zum Empfang von Mobilfunksignalen bereit ist und diese Funktion auf dem Gerät erlaubt ist.

➤ *Um über das Webportal die Alarmfunktion auf dem Gerät einzuschalten und das Gerät zu sperren, gehen Sie wie folgt vor:*

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.
3. Wählen Sie das Gerät aus, auf dem Sie die Alarmfunktion einschalten möchten und das gesperrt werden soll.
4. Klicken Sie auf **Alarmfunktion**.
5. Bei Bedarf können Sie im Abschnitt **Alarmfunktion** einen Text eingeben, der auf dem Monitor des gesperrten Geräts angezeigt werden soll.
6. Klicken Sie auf **Alarmfunktion aktivieren**.

➤ *Um mithilfe eines SMS-Befehls die Alarmfunktion auf dem Gerät einzuschalten und das Gerät zu sperren, führen Sie eine der folgenden Aktionen aus:*

- Wenn Kaspersky Internet Security for Android auf dem Zweitgerät installiert ist, erstellen Sie dort in Kaspersky Internet Security for Android mithilfe der SMS-Befehlsfunktion einen Befehl und senden Sie diesen an Ihr Gerät (s. Abschnitt "Senden von SMS-Befehlen aus Kaspersky Internet Security for Android" auf S. 34). Verwenden Sie beim Erstellen des SMS-Befehls den Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.
- Senden Sie eine SMS mit folgendem Text an Ihr Gerät alarm: <Code> (<Code> ist der Geheimcode für Kaspersky Internet Security auf Ihrem Gerät).

Sie werden durch eine Antwort-SMS über die Befehlsausführung informiert.

FERNGESTEUERTE DATENLÖSCHUNG VOM GERÄT

Bei Diebstahl oder Verlust Ihres Geräts können Sie mithilfe des Webportals <https://anti-theft.kaspersky.com> oder mit SMS-Befehlen ferngesteuert Daten vom Gerät löschen.

Sie können folgende Informationen löschen:

- persönliche Daten (z. B. Kontakte, Chatverlauf und Daten des Google™-Benutzerkontos) und Daten auf der Speicherkarte
- alle Daten, einschließlich der Daten auf der Speicherkarte (Werkseinstellungen des Geräts wiederherstellen)

Für das Senden eines SMS-Befehls an Ihr Gerät fallen Gebühren gemäß des Mobilfunktarifes an, der auf dem anderen mobilen Gerät gilt.

Die ferngesteuerte Datenlöschung ist unter folgenden Bedingungen möglich:

- Kaspersky Internet Security ist als Geräteadministrator festgelegt.
- Das Gerät ist zum Empfang von Mobilfunksignalen bereit.
- Der Start dieser Funktion ist auf dem Gerät erlaubt.

➡ Um über das Webportal ferngesteuert Daten vom Gerät zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.
3. Wählen Sie das Gerät aus, von dem Daten gelöscht werden sollen.
4. Klicken Sie auf **Datenlöschung**.
5. Wählen Sie im Abschnitt **Datenlöschung** die Daten, die Sie vom Gerät löschen möchten.
 - Um persönlichen Daten zu löschen (z. B. Google-Benutzerkontodaten, Kontakte und Chatverlauf) und die Speicherkarte neu zu formatieren, wählen Sie **Nur persönliche Informationen**.
 - Um alle Daten einschließlich der Daten auf der Speicherkarte zu löschen und das Gerät auf Werkseinstellungen zurückzusetzen, wählen Sie **Alle Daten**.

Nach der Löschung aller Daten vom Gerät wird auch das Programm Kaspersky Internet Security entfernt. Das Gerät kann dann keine ferngesteuerten Befehle mehr ausführen.

6. Klicken Sie auf **Löschen**.

➡ Gehen Sie folgendermaßen vor, um durch SMS-Befehle Daten von Ihrem Gerät ferngesteuert zu löschen:

- Wenn Kaspersky Internet Security for Android auf dem Zweitgerät installiert ist, erstellen Sie dort in Kaspersky Internet Security for Android mithilfe der SMS-Befehlsfunktion einen Befehl und senden Sie diesen an Ihr Gerät (s. Abschnitt "Senden von SMS-Befehlen aus Kaspersky Internet Security for Android" auf S. 34). Sie können entweder nur die persönlichen Daten oder alle Daten zum Löschen auswählen. Verwenden Sie beim Erstellen des SMS-Befehls den Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.
- Senden Sie eine SMS mit folgendem Text an Ihr Gerät:
 - wipe: <Code> – zum Löschen von persönlichen Daten und Daten auf der Speicherkarte.
 - fullreset: <Code> – zum Löschen aller Daten vom Gerät mit Zurücksetzen der Werkeinstellungen.
<Code> – Geheimcode, der auf Ihrem Gerät für Kaspersky Internet Security gilt.

Sie werden durch eine Antwort-SMS über die Befehlsausführung informiert.

FERNGESTEUERTES FOTOGRAFIEREN

Bei Diebstahl oder Verlust des Geräts können Sie mithilfe des Webportals <https://anti-theft.kaspersky.com> ferngesteuert die Person fotografieren, die Ihr Gerät gerade verwendet, und das Gerät sperren .

Das ferngesteuerte Fotografieren ist nur möglich, wenn Ihr Gerät eine Frontkamera besitzt. Die Funktion kann nur über das Webportal aktiviert werden. Das Aktivieren durch einen SMS-Befehl wird nicht unterstützt.

Der ferngesteuerte Start der Diebstahlschutz-Funktionen ist unter folgenden Bedingungen möglich:

- Kaspersky Internet Security ist als Geräteadministrator festgelegt.
- Das Gerät ist zum Empfang von Mobilfunksignalen bereit.
- Der ferngesteuerte Start dieser Funktion ist auf dem Gerät erlaubt.

➔ Gehen Sie folgendermaßen vor, um ein Fahndungsfoto der Person zu schießen, die im Moment Ihr Gerät verwendet:

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.
3. Wählen Sie das Gerät aus, mit dem Sie fotografieren möchten und das gesperrt werden soll.
4. Klicken Sie auf **Fahndungsfoto**.
5. Bei Bedarf können Sie im Abschnitt **Fahndungsfoto** einen Text eingeben, der auf dem Monitor des gesperrten Geräts angezeigt werden soll.
6. Klicken Sie auf **Fotografieren**.

Wenn Kaspersky Internet Security den Befehl ausführt, stehen die Bilder im Webportal zur Verfügung. Nachdem Sie Fotos empfangen haben, können Sie den Befehl wiederholen.

ANRUF- UND SMS-FILTER

Der Anruf- und SMS-Filter ist nur auf Geräten mit eingelegter SIM-Karte verfügbar.

Mit dem Anruf- und SMS-Filter können Sie unerwünschte eingehende Anrufe und SMS sperren. Das Programm filtert Anrufe und SMS gemäß dem ausgewählten Filtermodus. Dazu dienen Listen mit erlaubten und verbotenen Kontakten.

IN DIESEM ABSCHNITT

Standardmäßige Filterung von Kontakten	38
Alle Kontakte sperren, außer den erlaubten	39
Nur verbotene Kontakte sperren.....	39

STANDARDMÄßIGE FILTERUNG VON KONTAKTEN

Wenn Sie Anrufe und SMS von erlaubten Kontakten erhalten und Anrufe und SMS von verbotenen Kontakten sperren möchten, verwenden Sie den standardmäßigen Filtermodus.

Wenn Sie einen Anruf oder eine SMS von einem Kontakt erhalten, der nicht auf der Erlaubnis- oder Verbotsliste steht, bietet Ihnen das Programm an, eine Aktion für den Anruf oder die SMS von diesem Kontakt auszuwählen. Für künftige Anrufe und SMS von diesem Kontakt richtet sich das Kontakt nach der ausgewählten Aktion.

➤ *Um den standardmäßigen Filtermodus zu aktivieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Modus für Anruf- und SMS-Filter > Standard**.
2. Erstellen Sie eine Liste für verbotene Kontakte. Klicken Sie dazu im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Verbotene Kontakte**.
3. Erstellen Sie eine Liste für erlaubte Kontakte. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Erlaubte Kontakte**.
4. Aktivieren Sie bei Bedarf die zusätzlichen Filtereinstellungen. Klicken Sie dazu im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Anruf- und SMS-Filter**.

Um den Empfang von Anrufen und SMS von allen Kontakten aus dem Telefonbuch des Geräts zu erlauben, aktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

Um eingehende SMS von Nummern zu verbieten, die Buchstaben enthalten, aktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.

ALLE KONTAKTE SPERREN, AUßER DEN ERLAUBTEN

Wenn Sie Anrufe und SMS von allen Kontakten außer den erlaubten Kontakten sperren möchten, verwenden Sie den Filtermodus für erlaubte Kontakte.

➤ *Um den Filtermodus für erlaubte Kontakte zu aktivieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Modus für Anruf- und SMS-Filter > Erlaubte Kontakte**.
2. Erstellen Sie eine Liste für erlaubte Kontakte. Klicken Sie dazu im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Erlaubte Kontakte**.
3. Erlauben Sie falls erforderlich den Empfang von Anrufen und SMS von Kontakten aus dem Telefonbuch des Geräts.
 - a. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Anruf- und SMS-Filter**.
 - b. Aktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

NUR VERBOTENE KONTAKTE SPERREN

Wenn Sie nur Anrufe und SMS von verbotenen Kontakten sperren möchten, verwenden Sie den Filtermodus für verbotene Kontakte.

➤ *Um den Filtermodus für verbotene Kontakte zu aktivieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security for Android in der Schnellstartleiste auf **Anruf- und SMS-Filter > Modus für Anruf- und SMS-Filter > Verbotene Kontakte**.
2. Erstellen Sie eine Liste für verbotene Kontakte. Klicken Sie dazu im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Anruf- und SMS-Filter > Verbotene Kontakte**.

3. Aktivieren Sie falls erforderlich das automatische Sperren von SMS, die von Nicht-Ziffern-Nummern stammen:
 - a. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Anruf- und SMS-Filter**.
 - b. Aktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**.

WEB-FILTER UND SMS-ANTI-PHISHING

Dank des Web-Filters und SMS-Anti-Phishing können Sie überprüfte Webseiten aufrufen und Ihre persönlichen Daten gefahrlos im Netz nutzen.

Web-Filter und SMS-Anti-Phishing sind nur in der Premium-Version von Kaspersky Internet Security verfügbar.

SMS-Anti-Phishing funktioniert nur auf Geräten mit eingelegter SIM-Karte.

Der Web-Filter blockiert schädliche Webseiten, deren Ziel darin besteht, schädlichen Code zu verbreiten, sowie gefälschte Webseiten (Phishing-Seiten), die Ihre persönlichen Daten stehlen und sich Zugang zu Ihren Finanzkonten verschaffen können.

SMS-Anti-Phishing sperrt in SMS-Nachrichten Links, die auf schädliche und gefälschte Webseiten verweisen.

Der Web-Filter untersucht Webseiten, bevor sie geöffnet werden. Auch SMS-Anti-Phishing überprüft die Links in einer SMS bevor sie geöffnet werden. Für die Untersuchung wird von Web-Filter und SMS-Anti-Phishing der Cloud-Dienst Kaspersky Security Network genutzt (ein spezieller Online-Service von Kaspersky Lab, der Informationen über die Zuverlässigkeit von Dateien, Programmen und Internetressourcen bereitstellt).

IN DIESEM ABSCHNITT

Echtzeituntersuchung von Webseiten.....	40
Echtzeituntersuchung von Links in SMS-Nachrichten.....	41

ECHTZEITUNTERSUCHUNG VON WEBSEITEN

Web-Filter untersucht Webseiten nur im Android-Standardbrowser. Andere Browser werden derzeit nicht unterstützt. Wenn Sie den Web-Filter permanent im Internet verwenden möchten, legen Sie den Android-Standardbrowser als Standardbrowser fest.

➔ Um eine kontinuierliche Untersuchung von Webseiten zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Web-Filter**.
2. Aktivieren Sie das Kontrollkästchen **Web-Filter**.
3. Klicken Sie auf **Browser ändern** (Die Schaltfläche wird angezeigt, wenn der Web-Filter aktiviert ist und der Android-Standardbrowser nicht als Standardbrowser festgelegt ist).

Der Assistent zur Auswahl eines Standardbrowsers wird gestartet.

4. Folgen Sie den Anweisungen des Assistenten.

Der Assistent legt den Android-Standardbrowser als Standardbrowser fest.

ECHTZEITUNTERSUCHUNG VON LINKS IN SMS-NACHRICHTEN

SMS-Anti-Phishing funktioniert nur auf Geräten mit eingelegter SIM-Karte.

- Um die Untersuchung von Links in SMS-Nachrichten zu aktivieren, gehen Sie wie folgt vor:
1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Web-Filter**.
 2. Aktivieren Sie das Kontrollkästchen **SMS-Anti-Phishing**.

ANDERE AUFGABEN

Sie können zusätzlich folgende Aktionen ausführen:

- Premium-Version des Programms aktivieren
- Lizenz kaufen oder verlängern
- Informationen über die aktuelle Lizenz anzeigen
- Berichte über das Programm anzeigen (beispielsweise Berichte über eine ausgeführte Untersuchung, über gefundene Bedrohungen, über blockierte SMS, Anrufe oder Webseiten)
- Geheimcode für das Programm ändern
- Geheimcode für das Programm wiederherstellen.

IN DIESEM ABSCHNITT

Premium-Version des Programms aktivieren	41
Lizenz kaufen	42
Lizenz verlängern	42
Informationen zur Lizenz und zur Lizenzgültigkeit anzeigen	43
Berichte über das Programm anzeigen	43
Geheimcode für das Programm ändern	43
Geheimcode für das Programm wiederherstellen	43

PREMIUM-VERSION DES PROGRAMMS AKTIVIEREN

Um alle Programmfunktionen zu nutzen, müssen Sie die Premium-Version von Kaspersky Internet Security aktivieren.

Durch die *Aktivierung* wird der volle Funktionsumfang des Programms erreicht. Zur Aktivierung müssen Sie den Aktivierungscode eingeben, den Sie beim Kauf einer Lizenz erhalten haben, oder Sie müssen im Online-Shop eine Lizenz kaufen (s. Abschnitt "Lizenz kaufen" auf S. [42](#)).

Sie können die Premium-Version des Programms beim ersten Start oder zu einem späteren Zeitpunkt aktivieren.

Für die Programmaktivierung wird eine aktive Internetverbindung benötigt.

➤ *Um die Premium-Version des Programms mit einem Aktivierungscode zu aktivieren, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Lizenzverwaltung > Premium-Version aktivieren**.
2. Gehen Sie auf **Aktivierungscode eingeben**.
3. Geben Sie im folgenden Fenster den Aktivierungscode ein und klicken Sie auf **Aktivieren**.

Das Programm sendet eine Aktivierungsanfrage an den Aktivierungsserver von Kaspersky Lab. Bei erfolgreicher Durchführung der Aktivierungsanfrage benachrichtigt Sie das Programm darüber und zeigt Ihnen die aktuellen Lizenzinformationen an.

LIZENZ KAUFEN

Wenn Sie sich zur Nutzung der Premium-Version von Kaspersky Internet Security entschieden haben, können Sie über den Online-Shop von Kaspersky Lab oder bei unseren Vertriebspartnern eine Lizenz für die Programmnutzung kaufen.

Wenn Sie eine Lizenz über den Online-Shop kaufen, erhalten Sie einen Aktivierungscode. Mit diesem Code müssen Sie die Premium-Version des Programms aktivieren (s. Abschnitt "Premium-Version des Programms aktivieren" auf S. [41](#)).

Beim Kauf einer Lizenz über den Dienst Google Play Store, wird das Programm automatisch aktiviert.

➤ *Um im Online-Shop eine Lizenz zu erwerben, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Lizenzverwaltung > Premium-Version aktivieren**.

Die Schaltfläche für die Verlängerung der Lizenz heißt **Verlängern**.

2. Wählen Sie **Lizenz kaufen**.

Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine neue Lizenz erwerben.

LIZENZ VERLÄNGERN

Kaspersky Internet Security überprüft bei jedem Programmstart, ob eine Lizenz für die Nutzung der Premium-Version von Kaspersky Internet Security vorliegt.

Wenn Sie die Premium-Version des Programms nutzen, können Sie unter Lizenzinformationen (s. Abschnitt "Informationen zur Lizenz und zur Lizenzgültigkeit anzeigen" auf S. [43](#)) nachsehen, wie viele Tage bis zum Ablauf der Lizenz verbleiben.

Wenn bis zum Ablauf der Lizenz weniger als 14 Tage verbleiben, können Sie diese verlängern. Sie können entweder im Online-Shop eine Lizenz kaufen (s. Abschnitt "Lizenz kaufen" auf S. [42](#)) oder den Aktivierungscode verwenden (s. Abschnitt "Über den Aktivierungscode" auf S. [22](#)), den Sie beim Kauf einer Lizenz erhalten haben.

Beim Ablauf der Testlizenz wechselt das Programm automatisch zur kostenlosen Version.

➤ *Um die Lizenz mit einem Aktivierungscode zu verlängern, gehen Sie wie folgt vor:*

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Lizenzverwaltung > Verlängern**.
2. Gehen Sie auf **Aktivierungscode eingeben**.
3. Geben Sie den vorher beim Kauf der Lizenz erhaltenen Aktivierungscode ein.

INFORMATIONEN ZUR LIZENZ UND ZUR LIZENZGÜLTIGKEIT ANZEIGEN

Sie können den Schlüssel, die Gültigkeitsdauer der Lizenz und weitere Lizenzinformationen anzeigen lassen.

Informationen zur Lizenz können eingesehen werden, wenn Sie eine Testversion oder die Premium-Version des Programms nutzen.

➤ Gehen Sie folgendermaßen vor, um die Lizenzlaufzeit zu prüfen und Informationen über die Lizenz anzusehen:

Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Lizenzverwaltung > Details zur Lizenz**.

BERICHTE ÜBER DAS PROGRAMM ANZEIGEN

Die Ereignisse, die in Scanner (Anti-Virus), im Web-Filter und im Anruf- und SMS-Filter auftreten, werden in Berichten protokolliert.

Die Berichte sind nach dem Erstellungszeitpunkt angeordnet. Sie können die Berichte für eine bestimmte Programmkomponente anzeigen. Es werden maximal 50 Berichtseinträge gespeichert. Wenn die Anzahl der Einträge in einem Bericht über 50 steigt, werden ältere Einträge gelöscht und durch neue ersetzt.

➤ Um Programmberichte anzuzeigen,

klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Berichte**.

GEHEIMCODE FÜR DAS PROGRAMM ÄNDERN

Bei der Erstkonfiguration des Diebstahlschutzes (s. Abschnitt Erstkonfiguration des Diebstahlschutzes auf S. 26) oder beim ersten Start der Privatsphäre schlägt Ihnen das Programm vor, einen Geheimcode festzulegen. Sie können den Geheimcode jederzeit ändern.

➤ Um den Geheimcode für das Programm zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Erweiterte Einstellungen > Geheimcode ändern**.
2. Tragen Sie den aktuellen Geheimcode für das Programm im Feld **Aktuellen Geheimcode eingeben** ein und klicken Sie auf **Weiter**.
3. Tragen Sie im Feld **Legen Sie einen Geheimcode fest** einen neuen Geheimcode für das Programm ein und klicken Sie auf **Weiter**.
4. Wiederholen Sie den neuen Code im Feld **Bitte Code wiederholen** und klicken Sie auf **OK**.

GEHEIMCODE FÜR DAS PROGRAMM WIEDERHERSTELLEN

➤ Gehen Sie folgendermaßen vor, um den Programm-Geheimcode auf sichere Weise wiederherzustellen:

1. Öffnen Sie auf einem beliebigen Gerät das Webportal <https://anti-theft.kaspersky.com>.
2. Melden Sie sich am Webportal an. Verwenden Sie dazu das Benutzerkonto für den Kaspersky Account, das Sie bei der Erstkonfiguration des Programms verwendet haben.

3. Wählen Sie das Gerät aus, für das Sie den Geheimcode wiederherstellen möchten.
4. Klicken Sie auf **Geheimcode-Wiederherstellung**.
Der Wiederherstellungscodewird im Webportal angezeigt.
5. Starten Sie Kaspersky Internet Security auf dem Gerät.
6. Klicken Sie im Hauptfenster von Kaspersky Internet Security in der Schnellstartleiste auf **Einstellungen > Diebstahlschutz**.
7. Wenn der Geheimcode abgefragt wird, klicken Sie auf **Menü > Geheimcode-Wiederherstellung**.
8. Geben Sie den Wiederherstellungscodewein, der im Webportal angezeigt wird.
Auf dem Gerätedisplay wird Ihr Geheimcode angezeigt.
9. Geben Sie den Geheimcode im Feld **Geben Sie den wiederhergestellten Geheimcode ein** ein.
Das Programm eröffnet ein Fenster mit den Einstellungen des Diebstahlschutzes.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können und nennt die Voraussetzungen, die dafür erfüllt sein müssen.

IN DIESEM ABSCHNITT

Wie Sie technischen Kundendienst erhalten	45
Technischer Support am Telefon.....	45
Technischen Support erhalten über Mein Kaspersky Account	45

WIE SIE TECHNISCHEN KUNDENDIENST ERHALTEN

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm (s. Abschnitt "Informationsquellen zum Programm" auf S. 8) keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support von Kaspersky Lab zu wenden. Die Support-Mitarbeiter beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Beachten Sie die Support-Richtlinien (<http://support.kaspersky.com/de/support/rules>), bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonisch. Sie können sich am telefonisch von den Spezialisten des lokalen oder internationalen Technischen Supports beraten lassen.
- Aus Mein Kaspersky Account auf der Support-Webseite eine Anfrage senden. Sie können sich über ein Webformular an die Support-Experten wenden.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine Lizenz für die Programmnutzung gekauft haben. Die Benutzer von Testversionen haben keinen Anspruch auf technischen Kundendienst.

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie den lokalen oder internationalen Technischen Support anrufen (<http://support.kaspersky.com/de/support/international>).

Beachten Sie die Support-Richtlinien (<http://support.kaspersky.de/support/rules>), bevor Sie sich an den Technischen Support wenden. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

TECHNISCHEN SUPPORT ERHALTEN ÜBER MEIN KASPERSKY ACCOUNT

Mein Kaspersky Account ist Ihr persönlicher Bereich (<https://my.kaspersky.ru>) auf der Seite des Technischen Supports.

Sie müssen sich auf der Login-Seite anmelden (<https://my.kaspersky.com/ru/registration>). Geben Sie Ihre E-Mail-Adresse und das Kennwort für den Zugriff auf Ihren Kaspersky Account an.

In Mein Kaspersky Account können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- mit dem Technischen Support kommunizieren, ohne E-Mails zu verwenden.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- vollständigen Verlauf Ihrer Anfragen an den Technischen Support ansehen.
- Kopie einer Schlüsseldatei erhalten, falls die Schlüsseldatei verloren gegangen ist oder gelöscht wurde.

E-Mail-Anfrage an den Technischen Support

Anfragen an den Technischen Support können per E-Mail auf Deutsch, Englisch, Französisch, Spanisch oder Russisch gestellt werden.

Füllen Sie folgende Felder des elektronischen Formulars aus:

- Typ der Anfrage.
- Name und Versionsnummer des Programms;
- Anfragetext.
- Kundennummer und Kennwort.
- E-Mail-Adresse.

Die Support-Spezialisten richten ihre Antwort an My Kaspersky Account und an die E-Mail-Adresse, die in der Anfrage angegeben wurde.

Elektronische Anfrage an das Virenlabor

Beachten Sie, dass für die Bearbeitung bestimmter Anfragen nicht der Technische Support, sondern das Virenlabor verantwortlich ist.

In folgenden Fällen können Sie Anfragen an das Virenlabor richten:

- Wenn Sie den Verdacht haben, dass eine Datei oder eine Webressource infiziert ist, obwohl Kaspersky Internet Security keine Bedrohungen erkennt. Die Experten des Virenlabors analysieren die eingeschickte Datei oder Webadresse. Wird ein bisher unbekannter Virus gefunden, so werden Informationen zur entsprechenden Datenbank hinzugefügt und diese Datenbank wird in das nächste Update für die Kaspersky-Lab-Antiviren-Programme aufgenommen.
- Wenn Kaspersky Internet Security eine Datei oder eine Webressource als infiziert einstuft, obwohl Sie sicher sind, dass die Datei oder die Webressource keine Bedrohung darstellt.

Anfragen an das Virenlabor können Sie auf der Seite (<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>) stellen. Dazu ist keine Anmeldung bei Mein Kaspersky Account notwendig. In diesem Fall ist die Angabe eines Aktivierungscodes notwendig.

GLOSSAR

A

AKTIVIERUNGSCODE

Code, den Sie beim Kauf einer Lizenz für die Nutzung von Kaspersky Internet Security for Android erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Ein Aktivierungscode besteht aus einer Folge von zwanzig Ziffern und lateinischen Buchstaben im Format XXXXX-XXXXX-XXXXX-XXXXX.

ANTIVIREN-DATENBANKEN

Datenbanken, die Informationen über die Computer-Bedrohungen enthalten, die Kaspersky Lab beim Erscheinen der Datenbanken bekannt sind. Mithilfe der Einträge in den Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert. Die Datenbanken werden von Kaspersky-Lab-Experten angelegt und jede Stunde aktualisiert.

ARCHIV

Eine oder mehrere Dateien, die in komprimierter Form in eine Datei gepackt wurden. Für die Archivierung und zum Entpacken von Daten ist ein spezielles Kompressionsprogramm erforderlich.

D

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Antiviren-Datenbanken von den Kaspersky-Lab-Updateservern auf das Gerät kopiert und automatisch vom Programm übernommen.

DESINFEKTION VON OBJEKTEN

Verarbeitungsmethode für infizierte Objekte, bei der Daten vollständig oder teilweise wiederhergestellt werden. Nicht alle infizierten Objekte können desinfiziert werden.

G

GEHEIMCODE FÜR DAS PROGRAMM

Der Geheimcode für das Programm wird in folgenden Fällen verwendet:

- für den Zugriff auf die Einstellungen der Komponenten Diebstahlschutz und Privatsphäre
- beim Senden eines SMS-Befehls von einem anderen mobilen Gerät aus, um die Alarmfunktion ferngesteuert einzuschalten, das Gerät zu sperren, das Gerät zu orten, Daten vom Gerät zu löschen oder vertrauliche Kontakte und dazugehörige Informationen auszublenden.

I

INFIZIERTES OBJEKT

Objekt, das einen Codeabschnitt enthält, der mit dem Codeabschnitt eines bekannten Programms, das eine Bedrohung darstellt, übereinstimmt. Die Kaspersky-Lab-Experten warnen davor, mit solchen Objekten zu arbeiten.

K

KASPERSKY SECURITY NETWORK (KSN)

Infrastruktur aus Online-Diensten und Services, die Zugriff auf eine aktuelle Wissensdatenbank von Kaspersky Lab bietet. Die Datenbank bezieht sich auf die Reputation von Dateien, Webressourcen und Programmen. Die Verwendung von Daten aus dem Kaspersky Security Network ermöglicht eine schnellere Reaktion des Kaspersky-Lab-Programms auf unbekannte Bedrohungen, steigert die Effektivität bestimmter Schutzkomponenten und reduziert die Wahrscheinlichkeit von Fehlalarmen.

U

LISTE FÜR ERLAUBTE KONTAKTE

Zur Liste für erlaubte Kontakte können Sie jene Kontakte hinzufügen, von denen Sie eingehende Ereignisse erhalten möchten.

Die Einträge dieser Liste enthalten folgende Informationen:

- *Telefonnummer*, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS zustellen soll.
- *Typ der Ereignisse*, die der Anruf- und SMS-Filter von dieser Nummer zustellen soll. Es sind folgende Ereignistypen vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- *Schlüsselphrase*, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter blockiert.

LISTE FÜR VERBOTENE KONTAKTE

Zur Liste für verbotene Kontakte können Sie jene Kontakte hinzufügen, von denen Sie keine eingehenden Ereignisse erhalten möchten.

Die Einträge dieser Liste enthalten folgende Informationen:

- *Telefonnummer*, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS blockieren soll.
- *Typ der Ereignisse*, die der Anruf- und SMS-Filter von dieser Nummer blockieren soll. Es sind folgende Ereignistypen vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- *Schlüsselphrase*, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter zugestellt.

LIZENZLAUFZEIT

Gültigkeitsdauer der Lizenz – Zeitraum, für den Sie die Programmfunktionen und Zusatzleistungen nutzen dürfen. Der Umfang der Programmfunktionen und Zusatzleistungen ist vom Lizenztyp abhängig.

N

NICHT-ZIFFERN-NUMMERN

Eine Nicht-Ziffern-Nummer (auch Buchstabenwahl-, Wortwahlrufnummer oder Vanity-Rufnummer) ist eine Telefonnummer, die teilweise oder vollständig aus Buchstaben besteht.

O

OBJEKT LÖSCHEN

Verarbeitungsmethode für ein Objekt. Dabei wird das Objekt unwiderruflich von dem Ort gelöscht, an dem es vom Programm gefunden wurde. Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

P

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Die Aktivierung wird während oder nach der Programminstallation vom Benutzer ausgeführt. Zur Programmaktivierung muss der Benutzer den Aktivierungscode eingeben, den er beim Kauf einer Lizenz erhalten hat, oder er muss im Online-Shop eine Lizenz kaufen.

KASPERSKY LAB ZAO

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Programme für Desktops, Laptops, Tablet-PCs, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert, die Anti-Spam-Datenbanken im 5-Minuten-Takt.*

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Critical Path (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Frankreich), NETGEAR (USA), Parallels (Russland), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:

<http://www.kaspersky.de>

Viren-Enzyklopädie:

<http://www.securelist.com/de/>

Antiviren-Labor

newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>

(für Fragen an die Virenanalysten)

Webforum von Kaspersky Lab:

<http://forum.kaspersky.com>

INFORMATIONEN ÜBER DEN CODE VON DRITTHHERSTELLERN

Informationen über den Code von Drittherstellern finden Sie im Block **Programm-Infos** in den Programmeinstellungen.

MARKENINFORMATIONEN

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

Android und Google sind Marken von Google, Inc.

Intel, Atom sind Marken sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Intel Corporation.

ARM ist eine Marke oder eine eingetragene Marke von ARM Ltd. oder ihrer Tochterunternehmen.

SACHREGISTER

A

Alarmfunktion 36

B

Berichte..... 43

C

Code
 Geheimcode für das Programm ändern..... 43
 Wiederherstellen des Geheimcodes..... 43

D

Diebstahlschutz 27, 34, 35, 36, 37, 38
 Alarmfunktion 36
 Datenlöschung 27, 37
 Fahndungsfoto 38
 Gerätesperre und Ortung..... 27, 35
 SIM-Watch..... 34

G

Geheimcode für das Programm..... 43

K

Kaspersky Account..... 26
Kaspersky Lab ZAO..... 49

L

Lizenz
 Informationen 43
 Lizenzvertrag 21, 41, 42, 43
 online verlängern..... 42
 Programm aktivieren 41
 verlängern..... 42
Lizenz verlängern 42
Lizenzvertrag..... 21

O

Ortung sind 27, 35

P

Privatsphäre..... 32
 Remote-Start 32
Programm aktivieren..... 41
 Aktivierungscode..... 41
 Lizenz 21
 Lizenz online kaufen..... 42
Programmbenachrichtigungen 19
Programmhauptfenster 15
Programmsymbol in der Statuszeile 18

S

Scan auf Befehl	30
SMS-Befehle senden	27, 32, 34
Start	
Gerät manuell untersuchen.....	30
Gerät nach Zeitplan untersuchen	30
manuell aktualisieren.....	31
Programm.....	24
Startbildschirm-Widget.....	19

U

Update	31
manuell starten	31
Scan nach Zeitplan.....	31

Z

Zeitplan	
Scan auf Befehl.....	30
Update.....	31