

**MANUALE D'USO**

**KASPERSKY  
INTERNET  
SECURITY 2009  
SPECIAL EDITION  
FOR ULTRA-  
PORTABLES**

---

Gentile utente di Kaspersky Internet Security 2009!

Grazie per aver scelto il nostro prodotto. Speriamo che la presente documentazione possa essere di aiuto e sia in grado di offrire risposte riguardanti il presente prodotto software.

Attenzione! Il presente documento è proprietà di Kaspersky Lab e tutti i diritti su di esso sono riservati in base alla legge sul copyright della Federazione Russa ed ai trattati internazionali. La riproduzione e la distribuzione illegali di questo documento o di sue parti possono risultare in responsabilità civile, amministrativa o penale in base alle legge della Federazione Russa. Qualsiasi tipo di riproduzione e distribuzione di qualsiasi materiale, compresa la loro traduzione, è consentita esclusivamente con permesso scritto di Kaspersky Lab. Questo documento e le immagini grafiche ad esso correlate possono essere utilizzate esclusivamente per scopi informativi, non-commerciali o personali.

Questo documento può essere modificato senza preavviso. Per la versione più recente di questo documento, vedere il sito Web di Kaspersky Lab all'indirizzo <http://www.kaspersky.com/it/docs>. Kaspersky Lab non si assume alcuna responsabilità per quanto riguarda il contenuto, la qualità, la rilevanza o l'accuratezza dei materiali utilizzati in questo documento i cui diritti appartengono a terzi, o per possibili danni associati all'utilizzo di tali documenti.

Questo documento include marchi commerciali registrati e non registrati. Tali marchi appartengono ai rispettivi proprietari.

© Kaspersky Lab, 1997-2009

+7 (495) 645-7939,  
Tel., fax: +7 (495) 797-8700,  
+7 (495) 956-7000

[www.kaspersky.com/it](http://www.kaspersky.com/it)  
<http://kb.kaspersky.it>

Data revisione: 08.04.2009

---

# SOMMARIO

INSTALLAZIONE DI KASPERSKY INTERNET SECURITY .....	6
Ottenimento delle informazioni sull'applicazione.....	6
Fonti d'informazione per una ricerca autonoma .....	7
Contattare l'ufficio vendite .....	7
Contattare il servizio di assistenza tecnica.....	7
Discutere le applicazioni Kaspersky Lab sul Forum Web.....	9
Concetto di protezione dell'applicazione .....	9
Procedure guidate e strumenti .....	10
Funzioni di assistenza .....	11
Analisi euristica .....	12
Requisiti di sistema hardware e software.....	13
MINACCE ALLA SICUREZZA DEL COMPUTER.....	14
Applicazioni pericolose .....	14
Programmi nocivi.....	15
Virus e worm.....	15
Trojan .....	18
Utilità nocive .....	24
Programmi potenzialmente indesiderati .....	27
Adware .....	28
Pornware .....	28
Altri programmi riskware .....	29
Metodo di rilevamento degli oggetti infetti, sospetti e potenzialmente pericolosi da parte dell'applicazione.....	32
Minacce su Internet.....	33
Spam o posta in arrivo non richiesta .....	33
Phishing .....	33
Attacchi di pirateria informatica .....	34
Visualizzazione banner .....	34
INSTALLAZIONE DELL'APPLICAZIONE SUL COMPUTER.....	36
Passaggio 1. Ricerca di una versione più recente dell'applicazione .....	37
Passaggio 2. Verificare la conformità del sistema ai requisiti d'installazione	38

Passaggio 3. Finestra di benvenuto della procedura guidata .....	38
Passaggio 4. Visualizzazione dell'accordo di licenza .....	39
Passaggio 5. Selezione del tipo d'installazione.....	39
Passaggio 6. Selezione della cartella d'installazione .....	40
Passaggio 7. Selezione dei componenti dell'applicazione da installare .....	40
Passaggio 8. Ricerca di altri software antivirus.....	41
Passaggio 9. Preparazione finale per l'installazione .....	42
Passaggio 10. Completamento dell'installazione .....	42
<b>INTERFACCIA DELL'APPLICAZIONE .....</b>	<b>43</b>
Icona dell'area di notifica.....	43
Menu di scelta rapida.....	44
Finestra principale dell'applicazione.....	46
Notifiche .....	49
Finestra di configurazione delle impostazioni dell'applicazione .....	49
<b>GUIDA INTRODUTTIVA.....</b>	<b>51</b>
Selezione del tipo di rete.....	52
Aggiornamento dell'applicazione .....	53
Analisi della protezione .....	53
Scansione antivirus del computer .....	54
Gestione della licenza.....	54
Sottoscrizione al rinnovo automatico della licenza.....	56
Partecipazione a Kaspersky Security Network .....	58
Gestione della sicurezza .....	59
Sospensione della protezione .....	61
<b>CONVALIDA DELLE IMPOSTAZIONI DELL'APPLICAZIONE .....</b>	<b>62</b>
"Virus" di prova EICAR e sue varianti .....	62
Prova della protezione del traffico HTTP .....	66
Prova della protezione del traffico SMTP .....	66
Convalida delle impostazioni di Anti-virus file .....	67
Convalida delle impostazioni dell'attività di scansione antivirus.....	68
Convalida delle impostazioni di Anti-Spam .....	68

---

DICHIARAZIONE SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK .....	70
KASPERSKY LAB .....	76
Altri prodotti Kaspersky Lab .....	77
Recapiti .....	86
CRYPTOEX LLC .....	88
MOZILLA FOUNDATION .....	89
CONTRATTO DI LICENZA.....	90

---

# **INSTALLAZIONE DI KASPERSKY INTERNET SECURITY**

Kaspersky Internet Security può essere installato in una delle due modalità seguenti:

- modalità interattiva, attraverso l'Installazione guidata, che richiede la partecipazione dell'utente durante l'installazione;
- modalità non interattiva, in cui l'installazione dell'applicazione viene eseguita dal prompt dei comandi, che non richiede alcuna partecipazione da parte dell'utente.

Prima di installare Kaspersky Internet Security, è consigliabile chiudere tutte le applicazioni attive.

## **IN QUESTA SEZIONE:**

---

Ottenimento delle informazioni sull'applicazione .....	6
Concetto di protezione dell'applicazione.....	9
Requisiti di sistema hardware e software .....	13

## **OTTENIMENTO DELLE INFORMAZIONI SULL'APPLICAZIONE**

Se ci sono domande sull'acquisto, l'installazione o l'utilizzo dell'applicazione, è facile ottenere una risposta.

Kaspersky Lab offre molte fonti d'informazione ed è possibile selezionare la fonte ritenuta più pratica, in funzione dell'urgenza e dell'importanza della domanda.

## **FONTI D'INFORMAZIONE PER UNA RICERCA AUTONOMA**

È possibile utilizzare la Guida in linea.

La Guida in linea contiene informazioni sulla gestione della protezione del computer: consente di visualizzare lo stato di protezione, esaminare diverse aree del computer ed eseguire altre attività.

Per aprire la Guida, cliccare sul collegamento **Guida** nella finestra principale dell'applicazione o scegliere **<F1>**.

## **CONTATTARE L'UFFICIO VENDITE**

In caso di domande riguardanti la selezione o l'acquisto dell'applicazione o l'estensione del periodo di utilizzo, è possibile telefonare agli specialisti dell'ufficio vendite nella Sede centrale di Mosca, al numero:

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

Il servizio è disponibile in russo o in inglese.

Inviare le proprie domande all'Ufficio Vendite all'indirizzo di posta elettronica [sales@kaspersky.com](mailto:sales@kaspersky.com).

## **CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA**

Se l'applicazione è già stata acquistata, è possibile ottenere informazioni su di essa dal servizio di assistenza tecnica, telefonicamente o tramite Internet.

Gli specialisti dell'assistenza tecnica risponderanno alle vostre domande sull'installazione e l'utilizzo dell'applicazione e, se il computer in uso è stato infettato, vi aiuteranno ad eliminare le conseguenze delle attività del software nocivo.

Prima di contattare il Servizio di assistenza tecnica, leggere le regole per l'assistenza (<http://support.kaspersky.com/it/support/rules>).

## Richiesta al servizio di assistenza tecnica via posta elettronica (solo per utenti registrati)

Per porre domande agli specialisti del Servizio di assistenza tecnica, compilare un modulo Web Helpdesk (<http://support.kaspersky.ru/helpdesk.html?LANG=it>).

La domanda può essere inviata in russo, inglese, tedesco, francese o spagnolo.

Per inviare un messaggio di posta elettronica con la propria domanda, è necessario indicare il **numero cliente** ottenuto durante la registrazione presso il sito del servizio di assistenza tecnica, unitamente alla **password**.

### Nota

Se non si è ancora utenti registrati delle applicazioni di Kaspersky Lab, è possibile compilare un modulo di registrazione (<https://support.kaspersky.com/it/PersonalCabinet/Registration/Form/>). Durante la registrazione sarà necessario fornire il codice di attivazione o un nome di file chiave.

Si riceverà una risposta da uno specialista del servizio di assistenza tecnica nella **Pagina personale** (<https://support.kaspersky.com/it/PersonalCabinet>) ed all'indirizzo specificato nella richiesta.

Descrivere più dettagliatamente possibile il problema affrontato nel modulo di richiesta Web. Compilare i seguenti campi obbligatori:

- **Tipo di richiesta.** Le domande più frequenti degli utenti sono raggruppate in argomenti speciali, ad esempio "Installazione del prodotto/problema di rimozione" o "Scansione antivirus/problema di rimozione". Se non si trova l'argomento appropriato, selezionare "Domanda di carattere generale".
- **Nome e numero di versione dell'applicazione.**
- **Testo richiesta.** Descrivere il problema affrontato il più dettagliatamente possibile.
- **Numero cliente e password.** Inserire il numero cliente e la password ricevuti durante la registrazione nel sito Web del Servizio di assistenza tecnica.
- **Indirizzo di posta elettronica.** Gli specialisti dell'assistenza tecnica utilizzeranno questo indirizzo di posta elettronica per inviare la risposta alla vostra domanda.

## Assistenza tecnica telefonica

In caso di problemi che richiedano un'assistenza immediata, è possibile chiamare il servizio di assistenza tecnica ubicato nella vostra città. Non si dimentichino le informazioni necessarie

(<http://support.kaspersky.com/support/details>) rivolgendosi al servizio di assistenza tecnica

([http://support.kaspersky.com/support/support\\_local](http://support.kaspersky.com/support/support_local)) o internazionale (<http://support.kaspersky.com/support/international>). Ciò aiuterà i nostri specialisti ad elaborare le vostre richieste al più presto.

## DISCUTERE LE APPLICAZIONI KASPERSKY LAB SUL FORUM WEB

Se la domanda non richiede una risposta urgente, è possibile discuterla con gli specialisti di Kaspersky Lab ed altri utenti delle applicazioni antivirus di Kaspersky Lab sul Forum Web di Kaspersky Lab <http://forum.kaspersky.com>.

In questo forum è possibile visualizzare gli argomenti pubblicati in precedenza, lasciare commenti, creare nuovi argomenti e utilizzare il motore di ricerca.

## CONCETTO DI PROTEZIONE DELL'APPLICAZIONE

Kaspersky Internet Security garantisce la protezione del computer dalle minacce note e sconosciute, dagli attacchi degli hacker e degli intrusi, dalla posta spam e da altri dati indesiderati. Ciascun tipo di minaccia viene elaborato da un componente individuale dell'applicazione. Ciò fa dell'impostazione un processo flessibile, offrendo facili opzioni di configurazione per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o aziende nella loro globalità.

Kaspersky Internet Security include:

- Il monitoraggio delle attività delle applicazioni nel sistema, che impedisce l'esecuzione di azioni pericolose da parte delle applicazioni.
- Componenti di protezione dai software nocivi, che offrono la protezione in tempo per tutti i trasferimenti di dati ed i percorsi di ingresso al vostro computer.

- Componenti di protezione per lavorare su internet che garantiscono la protezione del computer contro gli attacchi di rete e degli intrusi attualmente noti.
- Componenti di filtraggio dei dati indesiderati che aiutano a risparmiare tempo, traffico Web e denaro.
- Attività di scansione antivirus, che consentono di esaminare singoli file, cartelle, unità alla ricerca di virus o di eseguire una scansione completa del computer. Le attività di scansione possono essere configurate per rilevare le vulnerabilità nelle applicazioni installate sul computer.
- Aggiornamento, che controlla lo stato dei moduli interni dell'applicazione utilizzati per la scansione delle minacce, gli attacchi dei pirati informatici e il rilevamento del messaggi spam.
- Procedure guidate e strumenti che facilitano l'esecuzione delle attività durante il funzionamento di Kaspersky Internet Security.
- Funzioni di supporto, che forniscono supporto informativo per lavorare con il programma ed espandere le sue capacità.

## **PROCEDURE GUIDATE E STRUMENTI**

Garantire la protezione del computer è un'attività assai difficile che richiede la conoscenza delle caratteristiche del sistema operativo e dei metodi utilizzati per sfruttarne le vulnerabilità. D'altro canto, una grande quantità e varietà d'informazioni sulla sicurezza dei sistemi complica l'analisi e l'elaborazione.

Per facilitare l'esecuzione di alcune attività specifiche di protezione del computer, Kaspersky Internet Security include diverse procedure guidate e strumenti:

- La procedura guidata Security Analyzer diagnostica i problemi del computer ricercando le vulnerabilità nel sistema operativo e nei programmi installati nel computer.
- La Configurazione guidata del browser analizza le impostazioni del browser Microsoft Internet Explorer e le valuta innanzitutto dal punto di vista della sicurezza.
- Il ripristino guidato del sistema dopo un'infezione consente di eliminare le tracce di presenza di oggetti nocivi dal sistema.
- La Pulitura guidata dei dati riservati ricerca ed elimina le tracce delle attività dell'utente nel sistema e nelle impostazioni del sistema operativo, che consentono di raccogliere informazioni sulle attività dell'utente.

- L'analisi dei pacchetti di rete intercetta i pacchetti di rete e ne visualizza i dettagli.
- Il Monitor rete visualizza dettagli relativi all'attività di rete del computer.
- La tastiera virtuale consente di prevenire l'intercettazione dei dati immessi tramite tastiera.

## FUNZIONI DI ASSISTENZA

L'applicazione comprende diverse funzioni di assistenza. Queste funzioni sono concepite per mantenere aggiornata l'applicazione, espanderne le capacità e assistere l'utente.

### Kaspersky Security Network

**Kaspersky Security Network** – sistema che prevede il trasferimento automatico dei rapporti sulle minacce potenziali e rilevate al database centrale. Questo database garantisce una reazione ancora più veloce alle minacce più comuni e notifiche ancora più tempestive agli utenti in caso di pandemie.

### Licenza

Quando si acquista Kaspersky Internet Security, si stipula un accordo di licenza con Kaspersky Lab che regola l'utilizzo dell'applicazione come anche l'accesso agli aggiornamenti al database dell'applicazione ed al Supporto tecnico per un periodo di tempo specificato. I termini di utilizzo e le altre informazioni necessarie per la piena funzionalità dell'applicazione sono fornite in un file chiave di licenza.

Utilizzando la funzione **Licenza** è possibile ottenere dettagli sulla licenza che si sta utilizzando o rinnovare la licenza corrente.

### Assistenza

Tutti gli utenti registrati di Kaspersky Internet possono avvalersi del servizio di supporto tecnico. Per sapere esattamente dove ottenere il supporto tecnico, usare la funzione **Assistenza**.

Seguendo i collegamenti corrispondenti, è possibile raggiungere il forum degli utenti di prodotti Kaspersky Lab ed inviare un rapporto di errore all'assistenza tecnica o feedback sull'applicazione tramite uno speciale modulo online.

È possibile inoltre accedere al Supporto tecnico online ed ai servizi di Assistenza personalizza; il nostro personale sarà sempre lieto di fornire l'assistenza telefonica per Kaspersky Internet Security.

## ANALISI EURISTICA

Alcuni componenti di protezione in tempo reale sono basati sull'euristica, come Anti-virus file, Anti-virus posta, Anti-virus web e le scansioni antivirus.

Ovviamente, la scansione tramite il metodo delle firme con un database creato in precedenza contenente una descrizione delle minacce conosciute e dei metodi per trattarle offrirà una risposta definita in relazione alla nocività o meno di un oggetto esaminato ed alla sua classe di programmi pericolosi di appartenenza. Il metodo euristico, invece, mira a rilevare il comportamento tipico di funzionamento anziché la firma del codice nocivo, per prendere una decisione relativamente affidabile per quanto riguarda un file.

Il vantaggio dell'analisi euristica è che non è necessario aggiornare il database prima della scansione. Grazie a ciò, le nuove minacce vengono rilevate prima che gli analisti antivirus le abbiano scoperte.

Tuttavia, ci sono metodi per aggirare l'analisi euristica. Una di queste misure difensive è di sospendere l'attività del codice nocivo non appena rilevato dalla scansione euristica.

### Nota

Utilizzare una combinazione tra i diversi metodi di scansione garantisce una maggiore sicurezza.

In caso di potenziale minaccia, l'analizzatore euristico emula l'esecuzione dell'oggetto nell'ambiente virtuale protetto dell'applicazione. Se invece viene rilevata attività sospetta all'esecuzione dell'oggetto, esso verrà considerato nocivo e non potrà essere eseguito sull'host, oppure verrà visualizzato un messaggio richiedente ulteriori istruzioni da parte dell'utente:

- metti in quarantena la nuova minaccia per esaminarla e trattarla successivamente con i database aggiornati;
- elimina l'oggetto;
- ignora (se si è certi che l'oggetto non possa essere nocivo).

Per utilizzare i metodi euristici, selezionare **Analisi euristica**. A tal fine, portare il cursore in una delle seguenti posizioni: Basso, Medio, o Dettagliato. Il livello di profondità della scansione garantisce l'equilibrio tra la completezza, e quindi la qualità, della scansione per nuove minacce ed il carico sulle risorse del sistema operativo, nonché in termini di durata della scansione. Maggiore è il livello euristico selezionato, più risorse di sistema saranno richieste dalla scansione e maggiore sarà la durata.

Attenzione!

Le nuove minacce rilevate tramite l'analisi euristica vengono rapidamente analizzate da Kaspersky Lab, ed i metodi per disinfettarle vengono aggiunte agli aggiornamenti orari del database.

Se il database viene aggiornato regolarmente, viene mantenuto il livello di protezione ottimale per il computer.

## **REQUISITI DI SISTEMA HARDWARE E SOFTWARE**

Pr garantire il normale funzionamento dell'applicazione, il computer deve soddisfare i seguenti requisiti minimi:

*Requisiti generali:*

- 75 MB di spazio disponibile sul disco fisso.
- Un mouse.
- Microsoft Internet Explorer 5.5 o superiore (per l'aggiornamento dei database dell'applicazione e dei moduli software via Internet).
- Microsoft Windows Installer 2.0.

*Microsoft Windows XP Home Edition (SP2 o superiore), Microsoft Windows XP Professional (SP2 o superiore):*

- Processore Intel Atom, Intel Celeron-M o VIA C7-M.
- 256 MB di RAM liberi.

---

# MINACCE ALLA SICUREZZA DEL COMPUTER

Una minaccia considerevole alla sicurezza del computer è costituita dalle applicazioni pericolose. Inoltre, tale minaccia è potenziata dalla spam, del phishing, dagli attacchi degli hacker e dai banner pubblicitari nell'adware. Tali minacce sono legate all'utilizzo di Internet.

## IN QUESTA SEZIONE:

---

Applicazioni pericolose .....	14
Minacce su Internet .....	33

## APPLICAZIONI PERICOLOSE

L'applicazione di Kaspersky Lab è in grado di rilevare centinaia di migliaia di programmi pericolosi che possono risiedere sul computer in uso. Alcuni di questi programmi costituiscono una grande minaccia per il computer, altri sono pericolosi solo in certe condizioni. Quando l'applicazione rileva un'applicazione nociva, la classifica e assegna ad essa un livello di pericolosità (elevato o medio).

Gli analisti virali distinguono due categorie principali: *programmi nocivi* e *programmi potenzialmente indesiderati*.

I programmi nocivi (vedere pagina 15) (Malware) vengono creati allo scopo di creare danno ad un computer ed al suo utente, ad esempio trafugando, bloccando, modificando od eliminando informazioni o scombussolando il funzionamento di un computer o di una rete di computer.

I programmi potenzialmente indesiderati (vedere pagina 27), (PUP) non hanno l'esclusivo scopo di creare danno, a differenza dei programmi nocivi.

La Virus Encyclopedia (<http://www.viruslist.com/en/viruses/encyclopedia>) contiene una descrizione dettagliata di questi programmi.

## PROGRAMMI NOCIVI

I **programmi nocivi** vengono creati specificatamente per danneggiare i computer ed i loro utenti: trafugare, bloccare, modificare o cancellare informazioni, scombussolare il funzionamento di computer o di reti di computer.

I programmi malware si suddividono in tre sottocategorie: *virus e worm*, *programmi Trojan* e *utilità nocive*.

I virus e worm (vedere pagina 15) (Viruses\_and\_Worms) sono in grado di creare copie di sé stessi, a loro volta in grado di replicarsi. Alcuni di questi vengono eseguiti senza alcuna partecipazione o consapevolezza dell'utente, altri richiedono azioni da parte dell'utente per essere lanciati. Questi programmi eseguono le loro azioni nocive quando vengono eseguiti.

I programmi Trojan (vedere pagina 18) (Trojan\_programs) non creano copie di sé stessi, a differenza dei worm e dei virus. Essi penetrano in un computer, ad esempio, tramite la posta elettronica o un Web browser quando l'utente visita un sito Web "infetto". Per essere lanciati richiedono un'azione da parte dell'utente, ed iniziano ad eseguire le loro azioni nocive all'esecuzione.

Le Utilità nocive (vedere pagina 24) (Malicious\_tools) vengono create appositamente per creare danno. Tuttavia, a differenza di altri programmi nocivi, non eseguono azioni dannose immediatamente al lancio, e possono essere conservati ed eseguiti senza problemi sul computer dell'utente. Tali programmi hanno funzioni che possono essere utilizzate per creare virus, worm e programmi Trojan, organizzare attacchi di rete sui server remoti, l'hackeraggio di computer ed altre azioni pericolose.

## VIRUS E WORM

**Sottocategoria:** virus e worm (Viruses\_and\_Worms)

**Livello di gravità:** elevato

I virus e worm classici eseguono sul computer azioni non consentite dall'utente; possono creare copie di sé stessi che a loro volta sono in grado di replicarsi.

### Virus classico

Una volta penetrato nel sistema, un virus classico infetta un file, si attiva al suo interno, esegue la sua azione nociva ed aggiunge copie di sé stesso ad altri file.

I virus classici si riproducono solo sulle risorse locali di un determinato computer, non sono in grado di penetrare autonomamente altri computer. Possono penetrare altri computer solo se una loro copia viene aggiunta ad un file ubicato

in una cartella condivisa, su un CD, oppure se l'utente inoltra un messaggio di posta elettronica con un allegato infetto.

Il codice di un virus classico è in grado di penetrare diverse aree di un computer, del sistema operativo o di un'applicazione. A seconda dell'ambiente, si può distinguere tra virus per *file*, *boot*, *script* e *virus macro*.

I virus possono infettare i file in diversi modi. I virus di *sovrascrittura* scrivono il loro codice a sostituzione di quello del file che infettano, quindi ne distruggono i contenuti. Il file infetto non funziona più e non può essere disinfettato. I *virus parassiti* modificano i file lasciandoli parzialmente o completamente funzionanti. I *virus compagni* non modificano i file ma si autoreplicano. Quando si apre un file di questo tipo, verrà eseguito il suo duplicato, che è un virus. Esistono inoltre *virus collegamento*, virus (OBJ) che *infettano i moduli degli oggetti*, virus che *infettano le librerie del compilatore (LIB)*, virus che *infettano il testo originale dei programmi*, ecc.

## Worm

Una volta penetrato nel sistema, il codice di un worm di rete, analogamente al codice di un virus classico, si attiva e esegue le sue azioni perniciose. Il worm di rete è così chiamato a causa della sua abilità a trasmettersi da un computer ad un altro – senza che l'utente se ne renda conto – inviando copie di sé stesso attraverso vari canali d'informazione.

Il principale metodo di proliferazione è l'attributo più importante che differenzia i vari tipi di worm. La seguente tabella elenca i tipi di worm in base al metodo di proliferazione.

Tabella 1. Worm in base al metodo di proliferazione

TIPO	NOME	DESCRIZIONE
<b>Worm IM</b>	Worm IM	<p>Questi worm si propagano attraverso i client IM (instant messaging) come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager o Skype.</p> <p>Solitamente questi worm utilizzano la rubrica dei contatti per inviare messaggi contenenti un collegamento ad un file infetto ubicato su un sito Web. Quando l'utente scarica ed apre il file, il worm si attiva.</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Worm di posta elettronica</b>	Worm di posta elettronica	<p>I worm di posta elettronica infettano i computer tramite la posta.</p> <p>Un messaggio infetto contiene un file allegato contenente una copia del worm oppure un collegamento a tale file caricato su un sito Web che, per esempio, può essere stato "hackerato" o appartenere ad un hacker. Quando si apre tale allegato, il worm si attiva; anche quando si fa clic sul collegamento, si scarica un file e lo si apre, il worm si attiva e comincia ad eseguire la sua azione nociva. Dopodiché, continuerà a riprodursi attraverso le sue copie, trovando altri indirizzi di posta elettronica ai quali inviare messaggi infetti.</p>
<b>Worm IRC</b>	Worm IM	<p>I worm di questo tipo penetrano i computer attraverso le Internet Relay Chat – sistemi di servizio utilizzati per comunicare con altre persone in tempo reale via internet.</p> <p>Questo tipo di worm pubblica sulla chat Internet un file contenente una sua copia o un collegamento a tale file. Quando l'utente scarica ed apre il file, il worm si attiva.</p>
<b>Worm di rete</b>	Worm di rete (worm residenti nelle reti di computer)	<p>Tali worm sono distribuiti tramite le reti di computer.</p> <p>A differenza di altri tipi di worm, questi worm vengono propagati con la partecipazione dell'utente. Essi cercano nella rete locale i computer che utilizzano programmi con vulnerabilità. Per fare ciò invia uno speciale pacchetto di rete (exploit) contenente il suo codice o parte di esso. Se esiste un computer vulnerabile nella rete, esso riceverà tale pacchetto. Quando il worm ha penetrato interamente il computer, si attiva.</p>

TIPO	NOME	DESCRIZIONE
<b>Worm P2P</b>	Worm di file sharing	<p>I worm di file sharing si propagano attraverso le reti peer-to-peer di file sharing, come Kazaa, Grokster, EDonkey, FastTrack o Gnutella.</p> <p>Per poter penetrare in una rete di file sharing, solitamente il worm si replica nella cartella di condivisione, solitamente ubicata sul computer dell'utente. La rete di file sharing visualizza informazioni su questo fatto e l'utente può "trovare" il file infetto nella rete, come qualsiasi altro file, scaricarlo ed aprirlo.</p> <p>I worm più complessi imitano i protocolli di rete di una rete specifica di file sharing: offrono risposte positive alle ricerche e propongono copie di sé stessi da scaricare.</p>
<b>Worm</b>	Altri worm	<p>Altri tipi di worm di rete includono:</p> <ul style="list-style-type: none"> <li>• Worm che distribuiscono copie di sé stessi tramite le risorse di rete. Tramite la funzionalità del sistema operativo, esplorano le cartelle di rete disponibili, si connettono ai computer nella rete globale e cercano di aprirne le unità per ottenere l'accesso completo. A differenza dei worm per computer della rete, l'utente deve aprire un file contenente una copia del worm per attivarlo.</li> <li>• Worm che non utilizzano nessuno dei metodi di propagazione descritti in questa tabella (ad esempio i worm che si propagano tramite telefoni cellulari).</li> </ul>

## TROJAN

**Sottocategoria:** Trojan (Trojan\_programs)

**Livello di gravità:** elevato

A differenza dei worm e dei virus, i Trojan non replicano sé stessi. Essi penetrano in un computer, ad esempio, tramite la posta elettronica o un Web browser quando l'utente visita un sito Web "infetto". I programmi Trojan vengono

lanciati dall'utente ed iniziano ad eseguire la loro azione perniciosa durante il funzionamento.

Il comportamento dei diversi programmi Trojan nel computer infetto può variare. La funzione principale di un Trojan è bloccare, modificare e cancellare i dati, scombusolare il funzionamento dei computer o delle reti di computer. D'altro canto, i Trojan possono ricevere ed inviare file, eseguirli, visualizzare messaggi, accedere a pagine Web, scaricare ed installare programmi e riavviare il computer infetto.

Gli intrusi utilizzano spesso delle "collezioni" composte da vari programmi Trojan.

I tipi di programmi Trojan ed il loro comportamento vengono descritti nella tabella sotto.

*Tabella 2. Tipi di programmi Trojan in base al comportamento sul computer infetto*

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Trojan-ArcBomb</b>	Programmi Trojan – bombe archivio	Archivi; quando vengono decompressi raggiungono una dimensione tale da diventare un problema per il funzionamento del computer. Quando si cerca di decomprimere questo archivio, il computer può iniziare a rallentare o "congelarsi", ed il disco può riempirsi di dati "vuoti". Le "bombe archivio" sono particolarmente pericolose per i file server ed i server di posta. Tale "bomba archivio" può arrestare un server, se questo utilizza un sistema automatico di elaborazione delle informazioni in arrivo.
<b>Backdoor</b>	Programmi Trojan di amministrazione remota	Questi programmi sono considerati i programmi di tipo Trojan più pericolosi; dal punto di vista funzionale ricordano i programmi di amministrazione remota commerciali. Essi si installano senza che l'utente ne sia consapevole, e consentono all'intruso di gestire il computer in remoto.

TIPO	NOME	DESCRIZIONE
<b>Trojan</b>	Trojan	<p>I Trojan comprendono i seguenti programmi nocivi:</p> <ul style="list-style-type: none"><li>• <b>programmi Trojan classici</b>; essi eseguono solo le funzioni principali dei programmi Trojan: blocco, modifica o cancellazione di dati, scambussolamento del funzionamento dei computer o della rete di computer; non hanno alcuna caratteristica funzionale degli altri tipi di programmi Trojan descritti in questa tabella;</li><li>• <b>programmi Trojan “multi-purpose”</b>; hanno funzioni aggiuntive caratteristiche di diversi tipi di programmi Trojan.</li></ul>
<b>Trojan con riscatto</b>	Programmi Trojan che richiedono un riscatto	<p>Essi "prendono in ostaggio" le informazioni sul computer dell'utente, modificandole o bloccandole, oppure scambussolando il funzionamento del computer in modo che l'utente non sia più in grado di utilizzare i dati. L'intruso richiede quindi all'utente un riscatto in cambio della promessa di inviare il programma che ripristini l'utilizzabilità del computer.</p>
<b>Trojan-Clicker</b>	Trojan-Clicker	<p>Questi programmi accedono a pagine Web dal computer dell'utente: inviano un comando al browser Web o sostituiscono gli indirizzi Web conservati nei file di sistema.</p> <p>Utilizzando questi programmi, l'intruso organizza attacchi di rete ed aumenta il traffico verso tali siti per aumentare la frequenza di visualizzazione dei banner pubblicitari.</p>

TIPO	NOME	DESCRIZIONE
<b>Trojan-Downloader</b>	Programmi Trojan-Downloader	Essi accedono alla pagina Web dell'intruso, scaricano da questa altri programmi nocivi e li installano sul computer dell'utente; il nome del programma nocivo scaricabile può essere memorizzato in essi o ricevuto dal sito al quale si collegano.
<b>Trojan-Dropper</b>	Programmi Trojan-Dropper	<p>Questi programmi salvano programmi contenenti altri programmi Trojan sul disco del computer, quindi li installano.</p> <p>Gli intrusi possono utilizzare i Trojan-Dropper per:</p> <ul style="list-style-type: none"> <li>• installare un programma nocivo senza che l'utente lo sappia: i Trojan-Dropper non visualizzano alcun messaggio, oppure visualizzano messaggi falsi; ad esempio, notificando un errore nell'archivio o l'utilizzo di una versione errata del sistema operativo;</li> <li>• proteggere un altro programma nocivo dall'essere rilevato: non tutti i programmi antivirus sono in grado di rilevare un programma nocivo ubicato all'interno di un Trojan-Dropper.</li> </ul>
<b>Trojan-Notifier</b>	Trojan-Notifier	<p>Essi notificano l'intruso quando il computer infetto è connesso; quindi, trasferiscono informazioni su questo computer all'intruso, tra cui: l'indirizzo IP, il numero di una porta aperta o uno degli indirizzi di posta elettronica. Quindi comunicano con l'intruso via posta elettronica, tramite FTP, accedendo alla sua pagina Web o attraverso altri metodi.</p> <p>I Trojan-Notifier vengono spesso utilizzati in gruppi che comprendono diversi programmi Trojan. Essi comunicano all'intruso che ci sono altri programmi Trojan installati con successo nel computer dell'utente.</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Trojan-Proxy</b>	Trojan-Proxy	Essi consentono all'intruso di accedere anonimamente alle pagine Web utilizzando il computer dell'utente, e vengono spesso utilizzati per inviare posta spam.
<b>Trojan-PSW</b>	Trojan che trafugano le password	<p>Trojan che trafugano le password (Password Stealing Ware); essi rubano gli account dell'utente, ad esempio le informazioni di registrazione software. Recuperano le informazioni riservate nei file di sistema e nel registro e le inviano al loro sviluppatore via posta elettronica, tramite FTP, accedendo al sito Web dell'intruso o attraverso altri metodi.</p> <p>Alcuni di questi programmi Trojan ricadono in tipologie specifiche descritte in questa tabella. Si tratta di programmi Trojan che trafugano informazioni bancarie (Trojans-Bankers), programmi Trojan che trafugano i dati personali degli utenti di programmi client IM (Trojans-IMs) e programmi Trojan che trafugano dati dagli utenti di giochi in rete (Trojans-GameThieves).</p>
<b>Trojan-Spie</b>	Programmi Trojan-Spia	Questi programmi vengono utilizzati per spiare l'utente: essi raccolgono informazioni sulle azioni dell'utente sul computer, ad esempio, intercettano i dati inseriti dall'utente tramite la tastiera, scattano istantanee dello schermo e raccolgono elenchi di applicazioni attive. Una volta ricevute tali informazioni, le trasferiscono all'intruso via posta elettronica, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Trojan-DDoS</b>	Programmi Trojan – attacchi di rete	Inviano numerose richieste dal computer dell'utente al server remoto. Il server esaurirà quindi le risorse per elaborare le richieste ricevute e smetterà di funzionare (Denial-of-Service – DoS). Questi programmi vengono spesso utilizzati per infettare più computer da utilizzare come base per attaccare il server.
<b>Trojan-IMs</b>	Programmi Trojan che carpiscono i dati personali degli utenti di client IM	Questi worm trafugano i numeri e le password degli utenti di client IM (programmi di instant messaging) come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager o Skype. Quindi trasferiscono tali informazioni all'intruso via posta elettronica, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
<b>Rootkit</b>	Rootkit	Questi programmi nascondono altri programmi nocivi e la loro attività, prolungando quindi l'esistenza di tali programmi nel sistema; essi nascondono i file ed i processi nella memoria di un computer infetto o le chiavi di registro gestite dai programmi nocivi, nonché lo scambio di dati tra le applicazioni installate sul computer dell'utente e gli altri computer della rete.
<b>Trojan-SMS</b>	Programmi Trojan – messaggi SMS	Questi programmi infettano i telefoni cellulari ed inviano da questi messaggi SMS a certi numeri, a carico dell'utente del telefono infetto.
<b>Trojan-GameThieves</b>	Programmi Trojan che rubano i dati personali degli utenti di giochi di rete	Questi programmi carpiscono le informazioni degli account degli utenti dei giochi di rete; tali informazioni vengono quindi trasferite all'intruso via posta elettronica, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Trojan-Banker</b>	Programmi Trojan che trafugano le informazioni sui conti bancari	Questi programmi carpiscono le informazioni sui conti bancari o le informazioni sui conti elettronici o digitali; tali dati vengono trasferiti all'intruso via posta elettronica, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
<b>Trojan-Mailfinder</b>	Programmi Trojan che raccolgono indirizzi di posta elettronica	Questi programmi raccolgono gli indirizzi di posta elettronica sul computer e li trasferiscono all'intruso via posta elettronica, tramite FTP, accedendo al suo sito Web o attraverso altri metodi. L'intruso può utilizzare gli indirizzi raccolti per inviare spam.

## UTILITÀ NOCIVE

**Sottocategoria:** utilità nocive (Malicious\_tools)

**Livello di gravità:** medio

Queste utilità sono progettate specificatamente per causare danno. Tuttavia, a differenza di altri programmi nocivi, non eseguono azioni dannose immediatamente al lancio, e possono essere conservati ed eseguiti senza problemi sul computer dell'utente. Tali programmi hanno funzioni che possono essere utilizzate per creare virus, worm e programmi Trojan, organizzare attacchi di rete sui server remoti, l'hackeraggio di computer ed altre azioni pericolose.

Ci sono diversi tipi di utilità nocive con funzioni diverse: I vari tipi sono descritti nella seguente tabella.

*Tabella 3. Utilità nocive per funzione*

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Constructor</b>	Constructor	I constructor vengono utilizzati per creare nuovi virus, worm e programmi Trojan. Alcuni constructor hanno un'interfaccia standard di Windows che consente di selezionare il tipo di programma nocivo da creare, il metodo utilizzato dal programma per resistere al debugging ed altre proprietà.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Dos</b>	Attacchi di rete	<p>Invia numerose richieste dal computer dell'utente al server remoto. Il server esaurirà quindi le risorse per elaborare le richieste ricevute e smetterà di funzionare (Denial-of-Service – DoS).</p>
<b>Exploit</b>	Exploit	<p>Gli Exploit sono un insieme di dati o un codice di programma. Eseguono azioni nocive sul computer, utilizzando le vulnerabilità dell'applicazione che li elabora. Ad esempio, gli exploit possono scrivere o leggere i file o accedere alle pagine Web infette.</p> <p>I diversi exploit utilizzano le vulnerabilità di diverse applicazioni o servizi di rete. Un exploit viene trasferito tramite la rete a diversi computer, sotto forma di pacchetto di rete che cerca i computer con servizi di rete vulnerabili. Gli exploit contenuti in un file DOC utilizzano le vulnerabilità degli editor di testo. Può iniziare ad eseguire le funzioni programmate dall'intruso quando l'utente apre un file infetto. Un exploit contenuto in un messaggio di posta elettronica ricerca le vulnerabilità nei programmi client di posta; può iniziare ad eseguire le sue azioni nocive non appena l'utente apre un messaggio infetto nel programma stesso.</p> <p>Gli exploit vengono utilizzati per distribuire i worm di rete (Net-Worm). Exploit -Nuker sono pacchetti di rete che rendono i computer non operativi.</p>
<b>FileCryptor</b>	File Cryptor	<p>I file cryptor decriptano altri programmi nocivi per nasconderli dalle applicazioni antivirus.</p>

TIPO	NOME	DESCRIZIONE
<b>Flooder</b>	Programmi utilizzati per il flooding delle reti	<p>Invisano un gran numero di messaggi tramite i canali di rete. Questi canali comprendono, per esempio, i programmi utilizzati per il flooding delle Internet Relay chat.</p> <p>Tuttavia, questo tipo di software nocivo non include i programmi che eseguono il flooding del traffico di posta elettronica e dei canali IM e SMS. Tali programmi vengono classificati secondo i tipi individuali descritti nella seguente tabella (Email-Flooder, IM-Flooder e SMS-Flooder).</p>
<b>HackTool</b>	Strumenti di hacking	<p>Gli strumenti di hacking vengono utilizzati per hackerare i computer sui quali sono installati, oppure per organizzare attacchi su altri computer (ad esempio, per aggiungere altri utenti di sistema senza autorizzazione, o per cancellare i log di sistema per nascondere qualsiasi traccia della loro presenza). Includono alcuni sniffer che eseguono funzioni nocive, come ad esempio intercettare le password. Gli sniffer sono programmi che consentono di visualizzare il traffico di rete.</p>
<b>not-virus:Hoax</b>	Programmi burla	<p>Questi programmi spaventano l'utente con messaggi correlati a virus: possono "rilevare" un virus in un file pulito o visualizzare un messaggio relativo alla formattazione del disco che non avrà luogo.</p>
<b>Spoofers</b>	Spoofers	<p>Questi programmi inviano messaggi e richieste di rete con l'indirizzo di un mittente fittizio. Ad esempio, gli intrusi utilizzano gli spoofers per falsificare la loro identità di mittente.</p>
<b>VirTool</b>	Si tratta di strumenti utilizzati per creare varianti di programmi nocivi	<p>Consentono di modificare altri programmi nocivi per nascondarli alle applicazioni antivirus.</p>

TIPO	NOME	DESCRIZIONE
<b>Email-Flooder</b>	Programmi per il flooding degli indirizzi di posta elettronica	Questi programmi inviano moltissimi messaggi agli indirizzi di posta elettronica (flooding). Data la grande quantità di messaggi in arrivo, gli utenti non sono in grado di visualizzare i messaggi in arrivo non spam.
<b>IM-Flooder</b>	Programmi utilizzati per il flooding dei programmi IM	Questi programmi inviano moltissimi messaggi agli utenti di client IM (programmi di instant messaging) come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager o Skype. Data la grande quantità di messaggi in arrivo, gli utenti non sono in grado di visualizzare i messaggi in arrivo non spam.
<b>SMS-Flooder</b>	Programmi utilizzati per il flooding con messaggi di testo SMS	Questi programmi inviano numerosi messaggi SMS ai telefoni cellulari.

## PROGRAMMI POTENZIALMENTE INDESIDERATI

I **programmi potenzialmente indesiderati**, a differenza dei programmi nocivi, non hanno l'esclusivo scopo di creare danno. Possono tuttavia essere utilizzati per violare la sicurezza del computer.

Essi comprendono adware, pornware ed altri *programmi potenzialmente indesiderati*.

I programmi adware (vedere pagina 28) visualizzano informazioni pubblicitarie per l'utente.

I programmi pornware (vedere pagina 28) visualizzano informazioni pornografiche per l'utente.

Altri programmi pericolosi (vedere pagina 29) – spesso si tratta di programmi utili usati dai molti utenti di computer. Tuttavia, se un intruso ottiene l'accesso a questi programmi o li installa nel computer dell'utente, può utilizzarne le funzionalità per violare la sicurezza.

I programmi potenzialmente indesiderati vengono installati tramite uno dei seguenti metodi:

- Vengono installati dall'utente, individualmente o unitamente ad altri programmi (ad esempio, se gli sviluppatori software includono programmi adware nei programmi freeware o shareware).
- Vengono anche installati dagli intrusi che, ad esempio inseriscono tali programmi in pacchetti con altri programmi nocivi, utilizzano le "vulnerabilità" del browser Web o Trojan downloader e dropper, quando l'utente visita un sito Web "infetto".

## **ADWARE**

**Sottocategoria:** Adware

**Livello di gravità:** medio

I programmi adware visualizzano informazioni pubblicitarie per l'utente. Visualizzano banner pubblicitari nell'interfaccia di altri programmi e ridirigono le query di ricerca verso siti pubblicitari. Alcuni programmi adware raccolgono informazioni di marketing sull'utente e le ridirigono ai loro sviluppatori, quali ad esempio quali siti visita, o le ricerche che effettua (a differenza dei Trojan spy, questi programmi trasferiscono queste informazioni con il permesso dell'utente).

## **PORNWARE**

**Sottocategoria:** Pornware

**Livello di gravità:** medio

Solitamente, gli utenti installano volontariamente questi programmi per ricercare offerte pornografiche o scaricarle.

Anche gli intrusi possono installare questi programmi sul computer dell'utente, per visualizzare pubblicità di siti e servizi pornografici commerciali per l'utente, senza la sua autorizzazione. Per essere installati, utilizzano le vulnerabilità del sistema operativo o del browser Web, i Trojan downloader o i Trojan dropper.

Ci sono tre tipi di software di tipo pornografico, la cui distinzione dipende dalle loro funzioni. Questi tipi sono descritti nella seguente tabella.

Tabella 4. Tipi di programmi pornware in base al loro funzionamento

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Porn-Dialer</b>	Dialer automatici	Questi programmi chiamano automaticamente i servizi telefonici di tipo pornografico (i numeri telefonici sono memorizzati); a differenza dei Trojan dialer, l'utente viene avvertito della loro azione.
<b>Porn-Downloader</b>	Programmi per lo scaricamento di file da Internet	Questi programmi scaricano sul computer dell'utente informazioni pornografiche; a differenza dei Trojan dialer, l'utente viene avvertito della loro azione.
<b>Porn-Tool</b>	Strumenti	Vengono utilizzati per ricercare e visualizzare pornografia; questo tipo include speciali barre degli strumenti per il browser e speciali video player.

## ALTRI PROGRAMMI RISKWARE

**Sottocategoria:** altri programmi pericolosi

**Livello di gravità:** medio

Gran parte di questi programmi sono programmi utili usati da molti utenti. Essi comprendono client IRC, dialer, programmi di downloading, monitor dell'attività di sistema del computer, utilità per lavorare con le password, server Internet per servizi FTP, HTTP o Telnet.

Tuttavia, se un intruso ottiene l'accesso a questi programmi o li installa nel computer dell'utente, può utilizzare alcune delle loro funzionalità per violarne la sicurezza.

Altri programmi pericolosi vengono classificati in base al loro funzionamento. I vari tipi sono descritti nella seguente tabella.

Tabella 5. Altri tipi di programmi pericolosi distinti in base alle funzioni

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Client-IRC</b>	Programmi client di chat Internet	Gli utenti installano questi programmi per comunicare attraverso le Internet Relay Chat. Gli intrusi li usano per diffondere programmi nocivi.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Dialer</b>	Programmi di composizione automatica	Questi programmi sono in grado di stabilire connessioni telefoniche "nascoste" tramite il modem.
<b>Downloader</b>	Downloader	Questi programmi possono scaricare segretamente file da siti Web.
<b>Monitor</b>	Monitor	Questi programmi consentono l'attività di monitoraggio dei computer sui quali sono installati (monitoraggio delle prestazioni delle applicazioni, di come scambiano dati con le applicazioni su altri computer, ecc.).
<b>PSWTool</b>	Strumenti di recupero password	Questi programmi vengono utilizzati per visualizzare e recuperare le password dimenticate. Gli intrusi hanno esattamente lo stesso obiettivo quando li installano sui computer degli utenti.
<b>RemoteAdmin</b>	Programmi di amministrazione remota	<p>Questi programmi vengono spesso utilizzati dagli amministratori di sistema; garantiscono l'accesso all'interfaccia del computer remoto per monitorarlo e gestirlo. Gli intrusi hanno esattamente lo stesso obiettivo quando li installano sui computer degli utenti per monitorarli e gestirli.</p> <p>I programmi pericolosi di amministrazione remota sono diversi dai programmi Trojan di amministrazione remota detti Backdoor. I programmi Trojan dispongono di funzioni che consentono loro di infiltrarsi autonomamente nei sistemi ed installarsi; i programmi pericolosi non hanno questa funzionalità.</p>
<b>Server-FTP</b>	Server FTP	Questi programmi fungono da server FTP. Gli intrusi li installano sui computer degli utenti per ottenere l'accesso remoto tramite il protocollo FTP.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>Server proxy</b>	Server proxy	Questi programmi fungono da server proxy. Gli intrusi li installano sui computer degli utenti per inviare spam a nome dell'utente.
<b>Server-Telnet</b>	Server Telnet	Questi programmi fungono da server Telnet. Gli intrusi li installano sui computer degli utenti per ottenere l'accesso remoto tramite il protocollo Telnet.
<b>Server-Web</b>	Server Web	Questi programmi fungono da server Web. Gli intrusi li installano sui computer degli utenti per ottenere l'accesso remoto tramite il protocollo HTTP.
<b>RiskTool</b>	Strumenti del computer locale	Questi strumenti offrono agli utenti funzionalità aggiuntive e vengono utilizzati solo dal computer dell'utente (consentono di nascondere i file o le finestre delle applicazioni attive, chiudendo i processi attivi).
<b>NetTool</b>	Strumenti di rete	Questi strumenti offrono all'utente del computer sui quali sono installati funzionalità aggiuntive per la gestione di altri computer della rete (riavviarli, trovare le porte aperte, eseguire i programmi installati su questi computer).
<b>Client-P2P</b>	Programmi client Peer-to-Peer	Questi programmi utilizzano le reti peer-to-peer. Gli intrusi possono utilizzarli per diffondere programmi nocivi.
<b>Client-SMTP</b>	Client SMTP	Questi programmi inviano messaggi di posta elettronica in modalità nascosta. Gli intrusi li installano sui computer degli utenti per inviare spam a nome dell'utente.
<b>Barra degli strumenti Web</b>	Barre degli strumenti Web	Questi programmi aggiungono le loro barre di ricerca alle barre degli strumenti di altre applicazioni.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIZIONE</b>
<b>FraudTool</b>	Programmi fraudolenti	Questi programmi si camuffano da altri programmi reali. Ad esempio, ci sono programmi antivirus fraudolenti; visualizzano messaggi sul rilevamento di programmi nocivi, ma non trovano né disinfettano alcunché.

## **METODO DI RILEVAMENTO DEGLI OGGETTI INFETTI, SOSPETTI E POTENZIALMENTE PERICOLOSI DA PARTE DELL'APPLICAZIONE**

L'applicazione di Kaspersky Lab rileva i programmi nocivi negli oggetti applicando due metodi: *reattivo* (tramite i database) e *proattivo* (tramite l'analisi euristica).

I database sono file contenenti voci che vengono utilizzate per identificare la presenza di centinaia di migliaia di minacce conosciute negli oggetti rilevabili. Queste voci contengono informazioni riguardanti le sezioni di controllo del codice del programma nocivo e gli algoritmi utilizzati per disinfettare gli oggetti in cui sono contenuti questi programmi. Gli analisti antivirus di Kaspersky Lab rilevano quotidianamente centinaia di nuovi programmi pericolosi, creano voci che li identificano e li includono negli aggiornamenti del database.

Se l'applicazione di Kaspersky Lab rileva in un oggetto rilevabile una sezione del codice che coincide, sulla base delle informazioni nel database, con le sezioni di controllo del codice di un programma nocivo, considererà tale oggetto infetto, mentre se coincide solo parzialmente (secondo alcune condizioni) lo considererà *sospetto*.

Utilizzando il metodo proattivo, l'applicazione è in grado di identificare i programmi nocivi più recenti non ancora presenti nel database.

L'applicazione di Kaspersky Lab rileva gli oggetti contenenti nuovi programmi nocivi in base al loro comportamento. Non corrisponderebbe al vero affermare che il codice di tale oggetto coincide parzialmente o interamente con quello di un programma nocivo noto, ma contiene alcune sequenze di comandi che sono caratteristiche di programmi nocivi, come l'apertura di un file o la scrittura in un file, o l'intercettazione dei vettori di interrupt. Ad esempio, l'applicazione determina che un file sembra essere infetto con un virus di boot sconosciuto.

Gli oggetti identificati tramite il metodo proattivo vengono considerati *potenzialmente pericolosi*.

# MINACCE SU INTERNET

L'applicazione di Kaspersky Lab utilizza speciali tecnologie per prevenire le seguenti minacce alla sicurezza del computer:

- posta in arrivo indesiderata o spam (vedere la sezione "Posta indesiderata in arrivo o spam" a pagina 33);
- phishing (a pagina 33);
- attacchi degli hacker (a pagina 34);
- visualizzazione banner (a pagina 34).

## SPAM O POSTA IN ARRIVO NON RICHIESTA

L'applicazione di Kaspersky Lab protegge gli utenti dalla posta spam. La Spam è la posta in arrivo non richiesta, spesso di carattere pubblicitario. La spam è un carico aggiuntivo sui canali ed i server di posta del provider. Il destinatario paga per il traffico creato dalla spam, e la posta non spam viaggia più lentamente. Ecco perchè in molti paesi la posta spam è illegale.

L'applicazione di Kaspersky Lab esamina i messaggi in arrivo in Microsoft Office Outlook, Microsoft Outlook Express e The Bat! e, se identifica messaggi spam, esegue le azioni selezionati, come ad esempio spostare tali messaggi in una cartella speciale o eliminarli.

L'applicazione di Kaspersky Lab rileva la posta spam con grande precisione. Applica diverse tecnologie di filtraggio anti-spam: rileva la posta spam in base all'indirizzo del mittente, come anche tramite parole e frasi presenti nell'oggetto del messaggio; rileva la spam grafica ed utilizza un algoritmo di autoapprendimento per rilevare la spam in base al testo del messaggio.

I database di Anti-Spam contengono le liste "nere" e "bianche" degli indirizzi dei mittenti, l'elenco di parole e frasi legate alle diverse categorie di spam, come quella pubblicitaria, quella relativa alla medicina ed alla salute, il gioco d'azzardo, ecc.

## PHISHING

Il *phishing* è un tipo di attività fraudolenta su Internet che implica il "pescare" (in inglese fishing) i numeri di carte di credito, pin e altre informazioni personali dagli utenti per trafugare il loro denaro.

Il phishing è spesso mirato agli utenti dei servizi di Internet banking. Gli intrusi creano una copia esatta della banca presa di mira ed inviano quindi messaggi ai suoi clienti, a nome della banca. Li informano che, a causa di modifiche o guasti nel software di banking on-line, gli account degli utenti sono andati perduti e che l'utente deve confermare o modificare le proprie informazioni sul sito della banca. L'utente fa clic sul collegamento creato dai malfattori ed inserisce i propri dati personali.

Il database anti-phishing contiene l'elenco dei siti Web noti per essere utilizzati per attacchi di phishing.

L'applicazione Kaspersky Lab analizza i messaggi in arrivo in Microsoft Office Outlook e Microsoft Outlook Express, e se rileva un collegamento ad un URL incluso nei database, contrassegna il messaggio come spam. Se l'utente apre il messaggio e cerca di seguire il collegamento, l'applicazione blocca il sito Web.

## **ATTACCHI DI PIRATERIA INFORMATICA**

Un *attacco di rete* è un'intrusione in un computer remoto per ottenerne il controllo e metterlo fuori uso, oppure per accedere ad informazioni riservate.

Gli attacchi di rete sono sia azioni di intrusi (ad esempio, la scansione delle porte o il tentativo di "hackerare" le password) o di programmi nocivi che eseguono comandi a nome dell'utente e trasferiscono informazioni al proprio "master" o eseguono altre funzioni legate agli attacchi di rete. Comprendono alcuni programmi Trojan, gli attacchi DoS, gli script nocivi ed alcuni tipi di worm di rete.

Gli attacchi di rete si diffondono nella rete locale ed in quella globale tramite le vulnerabilità nei sistemi operativi e nelle applicazioni. Possono essere trasferiti come pacchetti di dati IP individuali durante le connessioni di rete.

L'applicazione di Kaspersky Lab arresta il traffico di rete senza interrompere le connessioni di rete. Si avvale per questo di speciali database di Firewall. Questi database contengono le voci che identificano i pacchetti di dati IP caratteristici di diversi programmi di hacking. L'applicazione analizza le connessioni di rete e blocca in esse i pacchetti IP che ritiene pericolosi.

## **VISUALIZZAZIONE BANNER**

I *banner* sono pubblicità collegate al sito Web dell'inserzionista e sono spesso visualizzati sotto forma di immagini. La visualizzazione dei banner sul sito Web non costituisce alcuna minaccia per la sicurezza del computer, ma è comunque un'interferenza col normale funzionamento del computer. I banner che lampeggiano sullo schermo peggiorano le condizioni lavorative e diminuiscono

l'efficienza. L'utente viene distratto da informazioni irrilevanti. Seguire i collegamenti dei banner aumenta il traffico Internet.

Molte organizzazioni vietano la visualizzazione dei banner nelle interface come parte della propria politica di sicurezza dati.

L'applicazione di Kaspersky Lab blocca i banner in base all'URL del sito Web al quale è collegato il banner. Utilizza database Anti-Banner aggiornabili che contengono l'elenco degli URL delle reti di banner russi ed esteri. L'applicazione esamina i collegamenti del sito Web da caricare, li confronta agli indirizzi nei database e se trova una corrispondenza nel database, elimina il collegamento a questo indirizzo dal sito e continua a caricare la pagina.

---

# INSTALLAZIONE DELL'APPLICAZIONE SUL COMPUTER

L'applicazione viene installata sul computer in modalità interattiva tramite l'installazione guidata dell'applicazione.

Attenzione!

Si consiglia di chiudere tutte le applicazioni in esecuzione prima di procedere con l'installazione.

Per installare l'applicazione sul computer, eseguire il programma di distribuzione (il file con estensione \*.exe).

Al termine, l'installazione guidata cercherà il pacchetto d'installazione dell'applicazione (file con estensione \*.msi), e, se si trova questo file, la procedura guidata cercherà una versione più recente sui server Internet di Kaspersky Lab. Se non si trova il pacchetto d'installazione, verrà proposto di scaricarlo. Una volta scaricato il file, partirà l'installazione dell'applicazione. Se si cancella il download dell'applicazione, il processo d'installazione parte in modalità normale.

Il programma d'installazione viene implementato come procedura guidata. Ciascuna finestra contiene un insieme di pulsanti che controllano il processo d'installazione. Di seguito è fornita una breve descrizione del loro scopo:

- **Avanti** – accetta l'azione e procede al passaggio successivo del processo d'installazione.
- **Indietro** – torna al passaggio precedente del processo d'installazione.
- **Annulla** – annulla l'installazione del prodotto.
- **Fine** – completa la procedura di installazione del programma.

Ciascun passaggio del pacchetto installazione viene discusso in dettaglio di seguito.

**IN QUESTA SEZIONE:**

---

Passaggio 1. Ricerca di una versione più recente dell'applicazione.....	37
Passaggio 2. Verificare la conformità del sistema ai requisiti d'installazione.....	38
Passaggio 3. Finestra di benvenuto della procedura guidata .....	38
Passaggio 4. Visualizzazione dell'accordo di licenza .....	39
Passaggio 5. Selezione del tipo d'installazione .....	39
Passaggio 6. Selezione della cartella d'installazione.....	40
Passaggio 7. Selezione dei componenti dell'applicazione da installare .....	40
Passaggio 8. Ricerca di altri software antivirus .....	41
Passaggio 9. Preparazione finale per l'installazione.....	42
Passaggio 10. Completamento dell'installazione.....	42

## **PASSAGGIO 1. RICERCA DI UNA VERSIONE PIÙ RECENTE DELL'APPLICAZIONE**

Prima di installare l'applicazione sul computer, la procedura guidata accede ai server di aggiornamento di Kaspersky Lab per verificare l'eventuale disponibilità di una versione più recente dell'applicazione da installare.

Se tale nuova versione non è stata rilevata sui server di aggiornamento di Kaspersky Lab, l'installazione guidata verrà avviata per installare la versione corrente.

Se viene rilevata una versione più recente sui server, ne verrà proposto il download. Se si annulla il download, l'installazione guidata verrà avviata per installare la versione corrente. Se si decide di installare una versione più recente, i file d'installazione verranno scaricati sul computer e l'installazione guidata verrà automaticamente avviata per installare la versione più recente. Per ulteriori dettagli sull'installazione di una versione più recente, fare riferimento alla documentazione della versione corrispondente dell'applicazione.

## **PASSAGGIO 2. VERIFICARE LA CONFORMITÀ DEL SISTEMA AI REQUISITI D'INSTALLAZIONE**

Prima di installare l'applicazione sul computer, la procedura guidata verifica la conformità del sistema operativo e dei service pack installati ai requisiti di installazione del software (vedere la sezione "Requisiti hardware e software di sistema" a pagina 13). Verificherà inoltre che i programmi richiesti siano installati sul computer e che si disponga dei diritti richiesti per installare software.

Se uno qualsiasi dei requisiti non è soddisfatto, verrà visualizzata la relativa notifica sullo schermo. Si consiglia di installare gli aggiornamenti richiesti utilizzando il servizio **Windows Update**, nonché i programmi richiesti prima di installare l'applicazione Kaspersky Lab.

## **PASSAGGIO 3. FINESTRA DI BENVENUTO DELLA PROCEDURA GUIDATA**

Se il sistema è completamente conforme ai requisiti (vedere la sezione "Requisiti di sistema hardware e software" a pagina 13), nessuna nuova versione dell'applicazione è stata trovata sui server di aggiornamento di Kaspersky Lab, oppure l'installazione della versione più recente è stata annullata, l'installazione guidata verrà avviata per installare la versione corrente dell'applicazione. La prima finestra di dialogo dell'installazione guidata contenente informazioni sull'avvio dell'installazione dell'applicazione sul computer verrà quindi visualizzata sullo schermo.

Per procedere con l'installazione, premere il pulsante **Avanti**. Per annullare l'installazione, scegliere il pulsante **Annulla**.

## PASSAGGIO 4. VISUALIZZAZIONE DELL'ACCORDO DI LICENZA

La finestra successiva della procedura guidata contiene l'accordo di licenza tra l'utente e Kaspersky Lab. Leggerlo attentamente e, se si accettano i termini e le condizioni dell'accordo, selezionare **Accetto i termini del contratto di licenza** e scegliere il pulsante **Avanti**. L'installazione continua.

Per annullare l'installazione, scegliere il pulsante **Annulla**.

## PASSAGGIO 5. SELEZIONE DEL TIPO D'INSTALLAZIONE

Durante questa fase verrà proposto di selezionare il tipo d'installazione ritenuto più adatto:

- **Installazione Express.** Selezionando questa opzione, l'intera applicazione verrà installata sul computer con le impostazioni di protezione raccomandate dagli esperti di Kaspersky Lab. Una volta terminata l'installazione, partirà la configurazione guidata dell'applicazione.
- **Installazione personalizzata.** In questo caso, sarà possibile selezionare i componenti dell'applicazione che si desidera installare sul computer, specificare la cartella nella quale verrà installata l'applicazione (vedere la sezione "Passaggio 6. Selezione della cartella d'installazione" a pagina 40), per attivare l'applicazione e configurarla con una speciale procedura guidata.

Se si seleziona la prima opzione, la procedura guidata d'installazione passa direttamente al Passaggio 8 (vedere la sezione "Passaggio 8. Ricerca di altri software antivirus" a pagina 41). In caso contrario, ciascun passaggio dell'installazione richiederà una conferma o l'intervento dell'utente.

## PASSAGGIO 6. SELEZIONE DELLA CARTELLA D'INSTALLAZIONE

Nota

Questo passaggio della procedura guidata d'installazione verrà eseguito solo se si è selezionata l'opzione di installazione personalizzata (vedere la sezione "Passaggio 5. Selezione del tipo d'installazione" a pagina 39).

Durante questo passaggio verrà proposto di identificare una cartella sul computer nel quale verrà installata l'applicazione. Il percorso predefinito è:

- <Unità> \ Programmi \ Kaspersky Lab \ Kaspersky Internet Security 2009 Special Edition for Ultra-Portables – per sistemi a 32 bit.

È possibile specificare una cartella diversa scegliendo il pulsante **Sfoggia** e selezionando una cartella nella finestra di dialogo standard di selezione della cartella oppure inserendo il percorso ad essa nel campo d'immissione fornito.

Attenzione!

Si tenga presente che, se si digita manualmente il percorso completo alla cartella di installazione, esso non deve superare i 200 caratteri né contenere caratteri speciali.

Per procedere con l'installazione, premere il pulsante **Avanti**.

## PASSAGGIO 7. SELEZIONE DEI COMPONENTI DELL'APPLICAZIONE DA INSTALLARE

Nota.

Questo passaggio dell'installazione guidata verrà eseguito solo se si è selezionata l'opzione di installazione personalizzata (vedere la sezione "Passaggio 5. Selezione del tipo d'installazione" a pagina 39).

In caso di installazione personalizzata, è necessario selezionare i componenti dell'applicazione da installare sul computer. Per impostazione predefinita, tutti i

componenti dell'applicazione sono selezionati per l'installazione: componenti di protezione, scansione e aggiornamento.

Per decidere quali componenti non si desidera installare, utilizzare le informazioni riepilogative sui componenti. Per fare ciò, selezionare il componente dall'elenco e leggere le informazioni su di esso nel campo sottostante. Le informazioni comprendono una breve descrizione del componente e lo spazio libero su disco richiesto per installarlo.

Per annullare l'installazione di qualsiasi componente, aprire il menu di scelta rapida facendo clic sull'icona accanto al nome del componente e selezionare la voce **L'intera funzionalità non sarà disponibile**. Si noti che se si annulla l'installazione di qualsiasi componente, non si sarà protetti da diversi programmi pericolosi.

Per selezionare un componente da installare, aprire il menu di scelta rapida facendo clic sull'icona accanto al nome del componente e selezionare la voce **La funzionalità specificata sarà installata sull'unità disco rigido locale**.

Dopo aver terminato la selezione dei componenti da installare, scegliere il pulsante **Avanti**. Per tornare all'elenco di componenti da installare per impostazione predefinita, scegliere il pulsante **Reimposta**.

## **PASSAGGIO 8. RICERCA DI ALTRI SOFTWARE ANTIVIRUS**

Durante questo passaggio la procedura guidata cerca altri programmi antivirus, compresi quelli di Kaspersky Lab, che potrebbero essere in conflitto con l'applicazione che si sta installando.

Se vengono rilevati tali programmi sul computer, l'elenco di tali programmi viene visualizzato sullo schermo. Verrà proposto di eliminarli prima di procedere con l'installazione.

È possibile scegliere se rimuoverli automaticamente o manualmente tramite i comandi ubicati sotto l'elenco di programmi antivirus rilevati.

Per procedere con l'installazione, premere il pulsante **Avanti**.

## PASSAGGIO 9. PREPARAZIONE FINALE PER L'INSTALLAZIONE

Durante questa fase verrà proposto di eseguire la preparazione finale per l'installazione sul computer.

Durante l'installazione iniziale personalizzata (vedere la sezione "Passaggio 5. Selezione del tipo d'installazione" a pagina 39) si consiglia di non deselezionare la casella **Abilità Auto-Difesa prima dell'installazione** durante l'installazione iniziale. Se il modulo di protezione è abilitato, se si verifica un errore durante l'installazione la correttezza della procedura di ritorno dell'installazione sarà garantita. Quando si tenta nuovamente l'installazione, si consiglia di deselezionare questa casella.

### Nota

In caso di installazione remota dell'applicazione tramite **Remote Desktop**, si consiglia di deselezionare la casella **Abilità Auto-Difesa prima dell'installazione**. Se la casella è selezionata, la procedura d'installazione potrebbe essere eseguita scorrettamente o non essere eseguita affatto.

Per procedere con l'installazione, premere il pulsante **Avanti**. I file d'installazione iniziano ad essere copiati sul computer.

### Attenzione!

Durante il processo d'installazione, la connessione di rete attuale viene chiusa se il pacchetto dell'applicazione comprende componenti per l'intercettazione del traffico di rete. La maggior parte delle connessioni terminate saranno ripristinate dopo un breve intervallo di tempo.

## PASSAGGIO 10. COMPLETAMENTO DELL'INSTALLAZIONE

La finestra **Installazione completa** contiene informazioni sul completamento della procedura di installazione dell'applicazione sul computer.

Se è necessario riavviare il computer per completare l'installazione correttamente, verrà visualizzata una notifica corrispondente sullo schermo. Dopo il riavvio del sistema, verrà avviata automaticamente la configurazione guidata.

Se non è necessario riavviare l'applicazione per completare l'installazione, scegliere il pulsante **Avanti** per avviare la configurazione guidata.

---

# INTERFACCIA DELL'APPLICAZIONE

L'applicazione presenta un'interfaccia semplice e di facile uso. Questo capitolo ne descrive le caratteristiche principali in dettaglio.

Oltre all'interfaccia principale del programma, esistono plugin per Microsoft Office Outlook (scansione anti-virus e elaborazione spam), Microsoft Outlook Express (Windows Mail), The Bat! (scansione anti-virus ed elaborazione spam), Microsoft Internet Explorer e Microsoft Windows Explorer. I plug-in espandono le funzionalità delle suddette applicazioni, consentendo di gestire e configurare i componenti Anti-Virus Posta e Anti-Spam dall'interfaccia.

## IN QUESTA SEZIONE:



---

Icona dell'area di notifica .....	43
Menu di scelta rapida .....	44
Finestra principale dell'applicazione .....	46
Notifiche .....	49
Finestra di configurazione delle impostazioni dell'applicazione .....	49

## ICONA DELL'AREA DI NOTIFICA

Subito dopo aver installato l'applicazione, la relativa icona viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

Questa icona funge da indicatore del funzionamento dell'applicazione. Riflette lo stato della protezione e visualizza numerose funzioni di base eseguite dal programma.

Se l'icona è attiva  (colorata), significa che la protezione completa o alcune delle sue componenti sono in esecuzione. Se l'icona non è attiva  (bianco e nero), tutti i componenti di protezione sono disattivati.

L'icona dell'applicazione cambia in funzione dell'operazione eseguita:



– scansione della posta elettronica.



– aggiornamento dei database dell'applicazione e dei moduli del programma.



– il computer deve essere riavviato per applicare gli aggiornamenti.




– si è verificato un errore in qualche componente di Kaspersky Internet Security.

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina 44) e finestra principale dell'applicazione (vedere la sezione "Finestra principale dell'applicazione" a pagina 46).

Per aprire il menu di scelta rapida, cliccare con il tasto destro del mouse sull'icona dell'applicazione.

Per aprire la finestra principale dell'applicazione, fare doppio clic sull'icona dell'applicazione. La finestra principale si apre sempre sulla sezione **Protezione**.

Se sono disponibili notizie da Kaspersky Lab, verrà visualizzata l'icona notizie nell'area di notifica della barra delle applicazioni . Fare doppio clic sull'icona per visualizzare le notizie nella relativa finestra.

## MENU DI SCELTA RAPIDA

Il menu di scelta rapida consente di eseguire le attività di protezione di base.

Il menu dell'applicazione contiene le seguenti voci:

- **Aggiorna** – avvia l'aggiornamento dei database e dei moduli dell'applicazione ed installa gli aggiornamenti sul computer.
- **Scansione completa del computer** – avvia una scansione completa del computer per individuare eventuali oggetti pericolosi. Durante l'operazione vengono esaminati gli oggetti di tutte le unità, inclusi i supporti rimovibili.
- **Scansione virus** – seleziona gli oggetti e avvia la relativa scansione antivirus. Per impostazione predefinita l'elenco contiene diversi oggetti, tra i quali la cartella **Documenti** e le caselle di posta. Questo elenco può essere completato selezionando gli oggetti da esaminare per avviare una scansione antivirus.

- **Monitor rete** – visualizza l'elenco delle connessioni di rete stabilite, le porte aperte e il traffico.
- **Tastiera virtuale** – passa alla tastiera virtual.
- **Kaspersky Internet Security** – apertura della finestra principale dell'applicazione (vedere la sezione "Finestra principale dell'applicazione" a pagina 46).
- **Impostazioni** – visualizza e configura le impostazioni dell'applicazione.
- **Attiva** – attiva il programma. Per ottenere lo status di utente registrato, è necessario attivare il programma. Questa voce di menu è disponibile solo se il programma non è attivato.
- **Informazioni su** – visualizza una finestra con le informazioni sull'applicazione.
- **Sospendi protezione / Riprendi protezione** – disabilita temporaneamente o abilita i componenti di protezione in tempo reale. Questa voce di menu non ha effetto sulle attività di scansione antivirus o di aggiornamento del prodotto.
- **Blocca traffico di rete** – blocca temporaneamente tutte le connessioni di rete del computer. Se si desidera che il computer possa interagire nuovamente con la rete, selezionare nuovamente questa voce dal menu.
- **Esci** – chiude l'applicazione (quando viene selezionata questa opzione, l'applicazione viene scaricata dalla RAM del computer).



Figura 1. Menu di scelta rapida

Se un'attività di scansione antivirus è in corso mentre si apre il menu di scelta rapida, quest'ultimo ne visualizza il nome e lo stato di avanzamento (percentuale completata). Selezionando l'attività, è possibile portarsi sulla finestra principale contenente un rapporto sui risultati correnti della sua esecuzione.

## FINESTRA PRINCIPALE DELL'APPLICAZIONE

La finestra principale dell'applicazione può essere divisa in tre parti:

- La parte superiore della finestra indica l'attuale stato di protezione del computer.



*Figura 2. Stato attuale della protezione del computer*

Ci sono tre possibili stati di protezione, ciascuno dei quali è visualizzato con un certo colore analogamente ad un semaforo. Il verde indica che la protezione del computer è di livello adeguato, il giallo ed il rosso evidenziano la presenza di diverse minacce alla sicurezza nella configurazione delle impostazioni o nel funzionamento dell'applicazione. Oltre ai programmi nocivi, le minacce comprendono il mancato aggiornamento dei database dell'applicazione obsoleti, la disabilitazione di alcuni componenti di protezione, le impostazioni dell'applicazione sul minimo, ecc.

Le minacce alla sicurezza devono essere eliminate non appena compaiono. Per ottenere informazioni dettagliate su di esse e per eliminarle con rapidità, utilizzare il collegamento **Correggi** (vedere la figura sopra).

- La parte sinistra della finestra – la barra di navigazione – consente di passare rapidamente all'utilizzo di qualsiasi funzione dell'applicazione, all'esecuzione di un'attività di scansione antivirus, di aggiornamento, ecc.



Figura 3. Parte sinistra della finestra principale

- La parte destra della finestra contiene informazioni sulla funzione dell'applicazione selezionata nella parte sinistra ed è utilizzata per configurare le impostazioni di tali funzioni ed offrire strumenti per eseguire le attività di scansione antivirus, scaricare gli aggiornamenti, ecc.



Figura 4. Parte informativa della finestra principale

È inoltre possibile utilizzare i pulsanti:

- **Impostazioni** – per passare alle impostazioni dell'applicazione.
- **Guida** – per passare alla Guida in linea dell'applicazione.
- **Rilevato** – per passare all'elenco di oggetti nocivi rilevati grazie al funzionamento di qualsiasi componente o ad un'attività di scansione anti-virus completata ed alla visualizzazione delle statistiche dettagliate dei risultati operativi dell'applicazione.
- **Rapporti** – per passare all'elenco di eventi verificatisi durante il funzionamento dell'applicazione.
- **Assistenza** – per aprire la finestra contenente informazioni sul sistema ed i collegamenti alle risorse informative di Kaspersky Lab (sito del servizio di Assistenza tecnica, forum).

**Nota**

È inoltre possibile modificare l'aspetto dell'applicazione creando e utilizzando grafici e schemi colori personalizzati.

## NOTIFICHE

Se si verificano eventi durante il funzionamento dell'applicazione, sullo schermo verranno visualizzate notifiche speciali sotto forma di messaggi pop-up sopra l'icona dell'applicazione nell'area di notifica di Microsoft Windows.

In funzione del livello di criticità dell'evento relativamente alla sicurezza del computer, l'utente può ricevere i seguenti tipi di avvisi:

- **Allarme.** Si è verificato un evento critico; ad esempio, è stato rilevato un virus o un'attività pericolosa nel sistema. L'utente deve decidere immediatamente come si deve comportare il programma. Questo tipo di notifica è visualizzato in rosso.
- **Attenzione!** Si è verificato un evento potenzialmente pericoloso. Per esempio, sul sistema sono stati rilevati file potenzialmente infetti o un'attività pericolosa. L'utente deve istruire il programma in funzione del livello di pericolosità dell'evento. Questo tipo di notifica è visualizzato in giallo.
- **Nota:** Questo avviso informa l'utente di eventi non critici. Questo tipo, ad esempio, include le notifiche relative al funzionamento del componente **Filtro contenuti**. Le notifiche informative sono di colore verde.

## FINESTRA DI CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni dell'applicazione può essere aperta dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale dell'applicazione" a pagina 46) o dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina 44) dell'applicazione. Per aprire questa finestra, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra principale dell'applicazione, oppure selezionare l'opzione appropriata dal menu di scelta rapida dell'applicazione.

La finestra di configurazione delle impostazioni si compone di due parti:

- la parte sinistra della finestra consente di accedere ai componenti dell'applicazione, alle attività di scansione antivirus, alle attività di aggiornamento, ecc.;
- la parte destra della finestra contiene un elenco di impostazioni del componente, dell'attività, ecc. , selezionato nella parte sinistra della finestra.

---

# GUIDA INTRODUTTIVA

Uno dei principali obiettivi degli specialisti di Kaspersky Lab nell'elaborazione di Kaspersky Internet Security era quello di fornire la configurazione ottimale di tutte le opzioni del programma. Ciò consente agli utenti a qualsiasi livello di conoscenza del computer di garantire la protezione del PC subito dopo l'installazione, senza sprecare ore per la configurazione.

Per praticità, abbiamo unificato i passaggi di configurazione preliminare nell'interfaccia unificata di Configurazione guidata iniziale che si avvia non appena è completata l'installazione del programma. Seguendo le istruzioni della procedura guidata, è possibile attivare l'applicazione, configurare le impostazioni di aggiornamento, limitare l'accesso al programma tramite una password e configurare altre impostazioni.

Il computer può essere infettato con programmi nocivi prima di installare il programma. Per rilevare i programmi nocivi, eseguire la scansione del computer (vedere la sezione "Scansione antivirus del computer" a pagina 54).

In conseguenza del funzionamento del programma pericoloso e dei problemi al sistema, le impostazioni del computer potrebbero essere corrotte. Eseguire un'Analisi della protezione per rilevare le vulnerabilità del software installato e le anomalie d'impostazione del sistema.

I database dell'applicazione inclusi nel pacchetto d'installazione potrebbero inoltre essere obsoleti. Avviare l'aggiornamento dell'applicazione (se non è stato effettuato durante la configurazione guidata o automaticamente subito l'installazione dell'applicazione).

Il componente Anti-Spam incluso nella struttura del programma utilizza un algoritmo di autoapprendimento per rilevare i messaggi indesiderati. Avviare l'apprendimento guidato dell'applicazione per configurare il componente in modo da operare con la corrispondenza.

Al termine delle azioni sopra descritte, l'applicazione sarà pronta per il funzionamento. Per valutare il livello di protezione del computer, utilizzare la gestione guidata della sicurezza (vedere la sezione "Gestione della sicurezza" a pagina 59).

**IN QUESTA SEZIONE:**

---

Selezione del tipo di rete .....	52
Aggiornamento dell'applicazione .....	53
Analisi della protezione.....	53
Scansione antivirus del computer.....	54
Gestione della licenza .....	54
Sottoscrizione al rinnovo automatico della licenza .....	56
Partecipazione a Kaspersky Security Network .....	58
Gestione della sicurezza .....	59
Sospensione della protezione.....	61

## **SELEZIONE DEL TIPO DI RETE**

Una volta installata l'applicazione, il componente Firewall analizza le connessioni di rete attive sul computer. A ciascuna connessione di rete verrà assegnato uno stato che determinerà le attività di rete consentite.

Se è stata selezionata la modalità interattiva di Kaspersky Internet Security, una notifica verrà visualizzata ogni volta che viene rilevata una nuova connessione di rete. È possibile selezionare lo stato delle nuove reti nella finestra di notifica:

- Rete pubblica – alle connessioni di rete con questo stato non è consentito accedere dall'esterno al computer protetto. È consentito l'accesso alle cartelle pubbliche ed alle stampanti. Si consiglia di assegnare questo stato alla rete Internet.
- Rete locale – alle connessioni di rete con questo stato è consentito l'accesso alle cartelle pubbliche ed alle stampanti di rete. Si consiglia di assegnare questo stato alle reti locali protette, quale ad esempio una rete aziendale.
- Rete affidabile – alle connessioni di rete con questo stato è consentita qualsiasi attività. Si consiglia di assegnare questo stato alle aree assolutamente sicure.

Per ciascun stato della rete, Kaspersky Internet Security include l'insieme di regole che gestiscono le attività di rete. Successivamente, è possibile modificare lo stato della rete specificato al primo rilevamento.

## AGGIORNAMENTO DELL'APPLICAZIONE

Attenzione!

Per aggiornare Kaspersky Internet Security è necessario disporre di un collegamento Internet.

Kaspersky Internet Security include database contenenti le firme delle minacce, esempi di frasi caratteristiche della posta spam e descrizioni degli attacchi di rete. Tuttavia, al momento dell'installazione dell'applicazione, il database può divenire obsoleto poiché Kaspersky Lab aggiorna regolarmente i database e i moduli dell'applicazione.

È possibile selezionare la modalità di lancio dell'aggiornamento durante la configurazione guidata dell'applicazione. Per impostazione predefinita, Kaspersky Internet Security controlla automaticamente la presenza di nuovi aggiornamenti sui server di Kaspersky Lab. Se il server contiene un nuovo insieme di aggiornamenti, Kaspersky Internet Security li scaricherà e li installerà in background.

Per mantenere la protezione del computer aggiornata in modo ottimale, si consiglia di aggiornare Kaspersky Internet Security subito dopo l'installazione.

► *Per aggiornare Kaspersky Internet Security manualmente,*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Aggiorna** nella parte sinistra della finestra.
3. Scegliere il pulsante **Avvia aggiornamento**.

## ANALISI DELLA PROTEZIONE

Come risultato delle attività indesiderate sul computer, che possono derivare da guasti del sistema o da attività di programmi nocivi, le impostazioni del sistema operativo possono corrompersi. Inoltre, le applicazioni installate sul computer possono avere vulnerabilità utilizzate dagli intrusi per infliggere danni al computer.

Per rilevare ed eliminare tali problemi di sicurezza, gli esperti di Kaspersky Lab consigliano di lanciare l'Analisi guidata della protezione dopo aver installato l'applicazione. L'analisi guidata della protezione ricerca le vulnerabilità nelle applicazioni installate e i danni e le anomalie nelle impostazioni del sistema operativo e del browser.

► *Per avviare la procedura guidata:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare **Firewall di sistema**.
3. Avviare l'attività **Security Analyzer**.

## SCANSIONE ANTIVIRUS DEL COMPUTER

Gli sviluppatori di programmi nocivi fanno tutto il possibile per nascondere le azioni dei loro programmi, quindi è facile non accorgersi della presenza di programmi nocivi sul computer.

Una volta installata l'applicazione sul computer, essa esegue automaticamente la **Scansione rapida**. Questa attività ricerca e neutralizza i programmi nocivi negli oggetti caricati all'avvio del sistema.

Gli specialisti di Kaspersky Lab raccomandano inoltre di eseguire l'attività di **Scansione completa**.

► *Per avviare / arrestare un'attività di scansione antivirus:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Cliccare su **Avvia scansione** per avviare la scansione. Se si desidera arrestare l'esecuzione dell'attività, scegliere **Interrompi scansione** mentre la scansione è in corso.

## GESTIONE DELLA LICENZA

Per poter funzionare, l'applicazione necessita di una chiave di licenza, fornita insieme al programma, che conferisce il diritto all'utilizzo del software a partire dal giorno dell'acquisto.

A meno che non sia stata attivata una versione di prova, senza una chiave di licenza l'applicazione viene eseguita nella modalità che consente di scaricare un solo aggiornamento, ma non gli aggiornamenti successivi.

Al termine del periodo di prova, l'applicazione di prova attivata non funziona più.

Quando la chiave di licenza scade, il programma continua a funzionare, ma non è possibile aggiornare i database. Resta comunque possibile eseguire la scansione del computer per identificare la presenza di eventuali virus e utilizzare i componenti di protezione, ma solo attraverso i database aggiornati fino alla scadenza della licenza. Ciò significa che la protezione dai virus diffusi dopo la scadenza della licenza del programma non può essere garantita.

Per assicurare una protezione completa, è consigliabile dunque rinnovare la chiave dell'applicazione. Due settimane prima della scadenza della chiave, viene inviato un messaggio di notifica che appare a ogni avvio dell'applicazione.

Le informazioni sulla chiave corrente sono riportate nella sezione **Licenza** della finestra principale dell'applicazione: ID chiave, tipo (commerciale, commerciale con sottoscrizione, commerciale con sottoscrizione di protezione, di prova, per beta testing), numero di host in cui la chiave può essere installata, data di scadenza della chiave e numero di giorni che precedono la scadenza. Le informazioni sulla scadenza della chiave non verranno visualizzate se è installata **licenza commerciale con sottoscrizione o licenza commerciale con sottoscrizione alla protezione** (vedere la sezione "Sottoscrizione al rinnovo automatico della licenza" a pagina [65](#)).

Per visualizzare l'accordo di licenza dell'applicazione, cliccare sul pulsante **Visualizza Contratto di licenza con l'utente finale**. Per rimuovere una chiave dall'elenco, cliccare sul pulsante **Elimina**.

Per acquistare o rinnovare una chiave:

1. Acquistare una nuova chiave. Per farlo, utilizzare il pulsante **Acquista licenza** (se l'applicazione non è stata attivata) o **Rinnova licenza**. La pagina Web visualizzata conterrà tutte le informazioni su come acquistare una chiave dal negozio online Kaspersky Lab o da eventuali partner commerciali. Se si esegue l'acquisto online, un file della chiave o un codice di attivazione verrà inviato tramite e-mail all'indirizzo specificato nel modulo d'ordine dopo aver effettuato il pagamento.
2. Installare la chiave. Per farlo, utilizzare il pulsante **Installare la chiave** nella sezione **Licenza** della finestra principale dell'applicazione o utilizzare il comando **Attivazione** dal menu principale dell'applicazione. La procedura di attivazione guidata si avvia automaticamente.

Nota. Kaspersky Lab propone regolarmente offerte speciali sulle estensioni della licenza dei propri prodotti. Tali offerte sono riportate nel sito Web Kaspersky Lab, nell'area **Prodotti e servizi** → **Sconti e offerte speciali**.

## SOTTOSCRIZIONE AL RINNOVO AUTOMATICO DELLA LICENZA

Quando la licenza viene acquisita mediante sottoscrizione, l'applicazione contatta automaticamente il server di attivazione in determinati intervalli per mantenere la validità della licenza durante l'intera durata della sottoscrizione.

Se la chiave corrente è scaduta, Kaspersky Internet Security verifica la disponibilità di una chiave aggiornata sul server utilizzando la modalità background. In caso di esito positivo della verifica, l'applicazione scarica la chiave trovata e la installa nella modalità di sostituzione della chiave precedente. In questo modo la licenza viene rinnovata senza alcun intervento da parte dell'utente. Se anche il periodo durante il quale l'applicazione rinnova la licenza è scaduto, il rinnovo potrà essere eseguito manualmente. La funzionalità dell'applicazione verrà mantenuta durante il periodo in cui è consentito il rinnovo manuale della licenza. Allo scadere di tale periodo, se la licenza non è stata rinnovata, gli aggiornamenti ai database non verranno più caricati (per la licenza commerciale con sottoscrizione) e la protezione del computer non sarà più garantita (per la licenza commerciale con sottoscrizione alla protezione). Per rifiutare la sottoscrizione al rinnovo automatico della licenza, contattare il negozio online dal quale è stata acquistata l'applicazione.

### Attenzione!

Se al momento dell'attivazione l'applicazione è stata già attivata mediante una chiave commerciale, tale chiave verrà sostituita con una chiave di sottoscrizione (una chiave di sottoscrizione della protezione). Se si desidera avviare l'applicazione utilizzando di nuovo la chiave commerciale, è necessario eliminare la chiave di sottoscrizione e riattivare l'applicazione con il codice di attivazione con il quale in precedenza è stata ottenuta la chiave commerciale.

La condizione della sottoscrizione può presentare i seguenti stati:

- **Danneggiata.** La richiesta di attivazione della sottoscrizione non è stata elaborata. L'elaborazione della richiesta sul server richiede tempo. Kaspersky Internet Security funziona in modalità completamente operativa. Se dopo un determinato periodo la richiesta di sottoscrizione non risulta ancora elaborata, si riceverà una notifica al riguardo. In tal caso, i database dell'applicazione non verranno più aggiornati (per la licenza commerciale con sottoscrizione) e la protezione del computer non sarà più garantita (per la licenza commerciale con sottoscrizione alla protezione).

- *Attivata.* La sottoscrizione al rinnovo automatico della licenza è stata attivata per un periodo illimitato, ovvero senza la specifica di alcuna data, o per un determinato periodo con la specifica della data di scadenza.
- *Rinnovata.* La sottoscrizione è stata rinnovata automaticamente o manualmente per un periodo illimitato, ovvero senza la specifica di alcuna data, o per un determinato periodo con la specifica della data di scadenza.
- *Errore.* Il rinnovo della sottoscrizione ha causato un errore.
- *Scaduta.* Il periodo di validità della sottoscrizione è scaduto. È possibile utilizzare un altro codice di attivazione o rinnovare la sottoscrizione contattando il negozio online da cui è stata acquistata l'applicazione.
- *Negata.* La sottoscrizione al rinnovo automatico della licenza viene annullata.
- *È necessario effettuare il rinnovo.* La chiave per il rinnovo della sottoscrizione non è stata ricevuta in tempo. Utilizzare l'opzione **Rinnova stato sottoscrizione** per rinnovare la sottoscrizione.

Per la licenza commerciale con la sottoscrizione alla protezione, la sottoscrizione è caratterizzata da due stati aggiuntivi:

- *Sospesa.* La sottoscrizione per il rinnovo automatico della licenza è sospesa (data di scadenza della sottoscrizione: data di sospensione della validità della sottoscrizione)
- *Ripresa.* La sottoscrizione per il rinnovo automatico della licenza è stata ripresa (la data di scadenza della sottoscrizione non presenta limiti).

Se sono scaduti il periodo di validità della sottoscrizione e il periodo aggiuntivo concesso per il rinnovo, ovvero se lo stato della sottoscrizione è *Scaduta*, l'applicazione notificherà l'informazione e interromperà i tentativi di ottenere una chiave aggiornata dal server. Per la licenza commerciale con sottoscrizione, la funzionalità dell'applicazione verrà mantenuta, ad eccezione degli aggiornamenti ai database dell'applicazione. Per la licenza commerciale con sottoscrizione alla protezione, i database dell'applicazione non verranno aggiornati e la protezione del computer non verrà garantita.

Se la licenza non è stata rinnovata in tempo, ovvero lo stato della sottoscrizione è *È necessario effettuare il rinnovo*, ad esempio se il computer è stato spento durante tutto il periodo in cui era consentito il rinnovo della licenza, è possibile rinnovarne lo stato manualmente. A tale scopo, è possibile utilizzare il pulsante **Rinnova stato sottoscrizione**. Fino a quando non viene effettuato il rinnovo della sottoscrizione, Kaspersky Internet Security non aggiorna più i database dell'applicazione (per la licenza commerciale con sottoscrizione) e non

garantisce più la protezione del computer (per la licenza commerciale con sottoscrizione alla protezione).

Durante l'utilizzo della sottoscrizione non è possibile installare chiavi di altro tipo o utilizzare un altro codice di attivazione per rinnovare la licenza. È possibile utilizzare un altro codice di attivazione solo allo scadere del periodo di validità della sottoscrizione, ovvero quando lo stato della sottoscrizione è *Scaduta*.

Attenzione!

Quando si utilizza la sottoscrizione al rinnovo automatico della licenza, se si reinstalla l'applicazione nel computer, è necessario riattivare il prodotto manualmente utilizzando il codice di attivazione ottenuto all'acquisto dell'applicazione.

## **PARTECIPAZIONE A KASPERSKY SECURITY NETWORK**

In tutto il mondo appaiono quotidianamente moltissime nuove minacce. Per facilitare la raccolta di statistiche sui nuovi tipi di minacce, le loro origini e sviluppare il metodo da utilizzare per eliminarle, Kaspersky Lab consente di utilizzare il servizio Kaspersky Security Network.

L'utilizzo di Kaspersky Security Network implica l'invio delle seguenti informazioni a Kaspersky Lab:

- Un identificatore univoco assegnato al computer dall'applicazione. Questo identificatore caratterizza le impostazioni hardware del computer e non contiene altre informazioni.
- Le informazioni sulle minacce identificate dai componenti dell'applicazione. La struttura ed i contenuti delle informazioni dipendono dal tipo di minaccia rilevata.
- Informazioni di sistema: versione del sistema operativo, service pack installati, servizi e driver scaricabili, versioni del browser e del client di posta elettronica, estensioni del browser, numero di applicazioni di Kaspersky Lab installate.

Kaspersky Security Network raccoglie inoltre statistiche estese, tra cui informazioni relative a:

- file eseguibili e applicazioni firmate scaricate sul computer;
- applicazioni in esecuzione sul computer.

Le informazioni statistiche vengono inviate una volta completato l'aggiornamento dell'applicazione.

Attenzione!

Kaspersky Lab garantisce che Kaspersky Security Network non raccoglie né distribuisce i dati personali degli utenti.

- ▶ Per configurare le impostazioni di invio delle statistiche:
  1. Aprire la finestra delle impostazioni dell'applicazione.
  2. Selezionare la sezione **Feedback** nella parte sinistra della finestra.
  3. Selezionare la casella **Accetto di partecipare al programma Kaspersky Security Network** per confermare la partecipazione al programma. Selezionare la casella **Accetto di inviare statistiche complete nell'ambito del programma Kaspersky Security Network** per confermare il consenso all'invio di statistiche estese.

## GESTIONE DELLA SICUREZZA

I problemi di protezione del computer vengono indicati dallo stato di protezione del computer nella Finestra principale dell'applicazione, modificando il colore dell'icona che indica lo stato di protezione del computer e del pannello in cui si trova l'icona stessa. Se il sistema di protezione presenta problemi, si consiglia di risolverli immediatamente.



Figura 5. Stato attuale della protezione del computer

È possibile visualizzare l'elenco di problemi occorsi, la loro descrizione e la possibile soluzione nella scheda **Stato** (vedere la figura sotto) che si apre cliccando sul collegamento **Correggi** (vedere figura sopra).

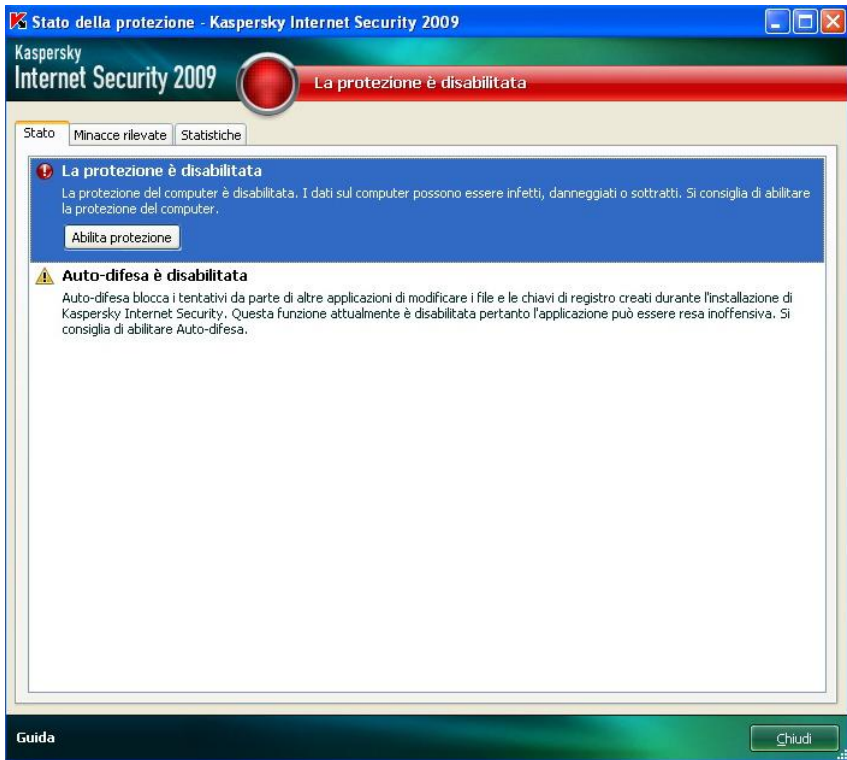


Figura 6. Risoluzione dei problemi di sicurezza

È possibile visualizzare l'elenco di problemi esistenti. I problemi vengono elencati in base a quanto è importante risolverli: innanzitutto i problemi più critici, ovvero quelli visualizzati con l'icona di stato rossa, quindi – meno importanti – quelli con l'icona di stato gialla, infine i messaggi informativi. Per ciascun problema viene fornita una descrizione dettagliata, e sono disponibili le seguenti azioni:

- *Eliminazione immediata.* Con i pulsanti corrispondenti, è possibile passare alla risoluzione del problema, che è l'azione raccomandata.
- *Rimanda l'eliminazione.* Se, per qualsiasi ragione, l'eliminazione immediata del problema non è possibile, è possibile saltare questa azione ed eseguirla più tardi. A tal fine, scegliere il pulsante **Nascondi messaggio**.

Si noti che questa opzione non è disponibile per i problemi più seri. Tali problemi comprendono ad esempio gli oggetti nocivi non disinfettati, il blocco di uno o più componenti o la corruzione dei file di programma.

Per far riapparire i messaggi nascosti nell'elenco generale, selezionare la casella **Ripristina messaggi nascosti**.

## SOSPENSIONE DELLA PROTEZIONE

Sospendere la protezione significa disabilitare temporaneamente tutti i componenti di protezione per un certo periodo di tempo.

► *Per sospendere la protezione del computer:*

1. Selezionare la voce **Sospendi protezione** dal menu di scelta rapida dell'applicazione (vedere la sezione "Menu di scelta rapida" a pagina 44).
2. Nella finestra **Sospendi protezione** che viene visualizzata, selezionare il periodo di tempo dopo il quale si desidera abilitare la protezione:
  - **In <intervallo di tempo>** – la protezione verrà abilitata una volta trascorso questo intervallo di tempo. Utilizzare il menu a discesa per selezionare il valore dell'intervallo di tempo.
  - **Dopo il riavvio** – la protezione verrà abilitata dopo il riavvio del sistema (sempre che la modalità che prevede il lancio dell'applicazione all'accensione del computer sia attivata).
  - **Manualmente** – la protezione verrà abilitata solo dopo averla avviata manualmente. Per abilitare la protezione, selezionare **Riprendi protezione** dal menù di scelta rapida dell'applicazione.

In seguito alla sospensione temporanea della protezione, tutti i componenti di protezione risultano sospesi. Ciò è indicato da:

- I nomi dei componenti della sezione **Protezione** della finestra principale sono inattivi (in grigio).
- Icona dell'applicazione Inattiva (grigia) (vedere la sezione "Icona dell'area di notifica" a pagina 43) nel riquadro di sistema.
- Il colore rosso dell'icona di stato e del pannello della finestra principale dell'applicazione.

Se sono attive connessioni di rete nel momento in cui la protezione è stata sospesa, verrà visualizzata una notifica relativa all'interruzione di tali connessioni.

---

# CONVALIDA DELLE IMPOSTAZIONI DELL'APPLICAZIONE


Una volta installata e configurata l'applicazione, è possibile verificare se l'applicazione è stata configurata correttamente tramite un virus di "prova" e le sue varianti. Una prova separata verrà effettuata per ciascun componente/protocollo di protezione.

## IN QUESTA SEZIONE:

---

“Virus” di prova EICAR e sue varianti .....	62
Prova della protezione del traffico HTTP .....	64
Prova della protezione del traffico SMTP .....	66
Convalida delle impostazioni di Anti-virus file .....	67
Convalida delle impostazioni dell'attività di scansione antivirus .....	68
Convalida delle impostazioni di Anti-Spam.....	68

## “VIRUS” DI PROVA EICAR E SUE VARIANTI

Questo "virus" di prova è stato progettato specificamente dall' (European Institute for Computer Antivirus Research) per il collaudo dei prodotti antivirus.

Il virus di prova NON È UN VIRUS, poiché non contiene codici in grado di danneggiare il computer. Tuttavia, la maggior parte dei prodotti antivirus lo identifica come tale.

**Attenzione!**

Non usare mai virus autentici per verificare il corretto funzionamento di un programma antivirus!

Il "virus" di prova può essere scaricato dal sito web ufficiale di **EICAR** all'indirizzo: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

**Nota**

Prima di scaricare il file, è necessario disabilitare la protezione antivirus, altrimenti l'applicazione identificherà il file *anti\_virus\_test\_file.htm* come file infetto trasferito tramite protocollo HTTP e lo neutralizzerà.

Riattivare la protezione antivirus subito dopo aver scaricato il "virus" di prova.

L'applicazione identifica il file scaricato dal sito **EICAR** come oggetto infetto contenente un virus che **non può essere disinfettato**, ed esegue le azioni specificate per oggetti di questo tipo.

È possibile inoltre utilizzare modifiche del "virus" di prova standard per verificare il funzionamento dell'applicazione. A tal fine, modificare il contenuto del "virus" standard aggiungendo uno dei prefissi elencati nella tabella di seguito. Per creare varianti del "virus" di prova, è possibile utilizzare qualsiasi editore di testo o ipertesto, ad esempio il **Blocco note Microsoft**, **UltraEdit32**, ecc.

**Attenzione!**

È possibile verificare il corretto funzionamento dell'applicazione antivirus tramite il "virus" modificato EICAR solo se i database antivirus sono stati aggiornati il 24 ottobre 2003 o successivamente (Ottobre 2003, aggiornamento cumulativi).

La prima colonna contiene i prefissi che devono essere aggiunti all'inizio della stringa per un "virus" di prova standard. La seconda colonna elenca tutti i valori possibili dello stato che Anti-virus assegna all'oggetto in base ai risultati della scansione. La terza colonna contiene informazioni circa l'elaborazione di oggetti con lo stato specificato dall'applicazione. Si noti che le azioni a eseguire sugli oggetti saranno determinate dai valori delle impostazioni dell'applicazione.

Una volta aggiunto il prefisso al "virus" di prova, salvare il nuovo file con un nome diverso, ad esempio: *ecar\_dele.com*. Assegnare nomi simili a tutti i "virus" modificati.

Tabella 6. Varianti del "virus" di prova

Prefisso	Stato dell'oggetto	Informazioni di elaborazione dell'oggetto
Nessun prefisso, virus di prova standard	<b>Infetto.</b> L'oggetto infetto contiene il codice di un virus noto. La disinfezione non è possibile.	L'applicazione identifica l'oggetto come virus non disinfettabile.  Si verifica un errore al tentativo di disinfettare l'oggetto; verrà eseguita l'azione assegnata agli oggetti non disinfettabili.
CORR-	<b>Corrotto.</b>	L'applicazione ha potuto accedere all'oggetto ma non ha potuto esaminarlo, poiché l'oggetto è corrotto (ad esempio, la struttura del file è corrotta o il suo formato non è valido). Le informazioni sull'elaborazione dell'oggetto possono essere trovate nel rapporto sul funzionamento dell'applicazione.
WARN-	<b>Sospetto.</b> L'oggetto sospetto contiene il codice di un virus sconosciuto. La disinfezione non è possibile.	L'oggetto è stato ritenuto sospetto dall'analizzatore euristico di codice. Al momento del rilevamento, il database dei virus di Anti-virus non contiene alcuna descrizione della procedura di trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
SUSP-	<b>Sospetto.</b> L'oggetto sospetto contiene il codice modificato di un virus noto. La disinfezione non è possibile.	L'applicazione ha rilevato una parziale corrispondenza di una sezione del codice dell'oggetto con una sezione di codice di un virus conosciuto. Al momento del rilevamento, il database dei virus di Anti-virus non contiene alcuna descrizione della procedura di trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.

Prefisso	Stato dell'oggetto	Informazioni di elaborazione dell'oggetto
ERRO-	<b>Errore di scansione.</b>	<p>Si è verificato un errore durante la scansione di un oggetto. L'applicazione non è stata in grado di accedere all'oggetto. l'integrità dell'oggetto è stata compromessa (ad esempio, a causa di un archivio in più volumi), oppure non c'è alcuna connessione ad esso (l'oggetto da esaminare è su un'unità di rete). Le informazioni sull'elaborazione dell'oggetto possono essere trovate nel rapporto sul funzionamento dell'applicazione.</p>
CURE-	<b>Infetto.</b> L'oggetto infetto contiene il codice di un virus noto. Disinfettabile.	L'oggetto contiene un virus che può essere disinfettato. L'applicazione disinfetterà l'oggetto; il testo del corpo del "virus" verrà sostituito dalla parola CURE. Il rilevamento di un oggetto di questo tipo viene notificato.
DELE-	<b>Infetto.</b> L'oggetto infetto contiene il codice di un virus noto. La disinfezione non è possibile.	L'applicazione identifica l'oggetto come virus non disinfettabile.  Si verifica un errore al tentativo di disinfettare l'oggetto; verrà eseguita l'azione assegnata agli oggetti non disinfettabili.  Il rilevamento di un oggetto di questo tipo viene notificato.

## PROVA DELLA PROTEZIONE DEL TRAFFICO HTTP

- ▶ *Per verificare il rilevamento di virus nel flusso dati trasferito tramite il protocollo HTTP, attenersi alla seguente procedura:*

Cercare di scaricare un "virus" di prova dal sito Web ufficiale dell'organizzazione **EICAR** all'indirizzo:

[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Quando si cerca di scaricare il "virus" di prova, Kaspersky Internet Security rileverà questo oggetto identificandolo come oggetti infetto impossibile da disinfettare, ed eseguirà l'azione prevista nelle impostazioni per il traffico HTTP per questo tipo di oggetti. Per impostazione predefinita, quando si cerca di scaricare il "virus" di prova, la connessione col sito Web viene terminata ed il browser visualizza un messaggio che informa l'utente che l'oggetto è infetto con il virus EICAR-Test-File.

## PROVA DELLA PROTEZIONE DEL TRAFFICO SMTP

Per rilevare i virus presenti nei flussi dati trasferiti tramite il protocollo SMTP, è possibile utilizzare un sistema di posta che utilizzi questo protocollo per trasferire i dati.

### Nota

Si consiglia di provare come Kaspersky Internet Security gestisca i messaggi di posta in arrivo ed in uscita comprendendo sia il corpo del messaggio che gli allegati. Per provare il rilevamento dei virus nel corpo del messaggio, copiare il testo del "virus" di prova standard o di quello modificato nel corpo del messaggio.

- ▶ *Per fare ciò:*

1. Creare un messaggio in formato **testo semplice** tramite un client di posta installato sul computer.

**Nota**

Un messaggio contenente un virus di prova in formato RTF o HTML non verrà esaminato!

2. Copiare il testo del "virus" standard o modificato all'inizio del messaggio o allegare un file contenente il "virus" di prova al messaggio.
3. Inviare il messaggio all'amministratore.

L'applicazione rileva l'oggetto e lo identifica come infetto. L'invio di un messaggio contenente un oggetto infetto verrà bloccato.

## **CONVALIDA DELLE IMPOSTAZIONI DI ANTI-VIRUS FILE**

- ▶ *Per verificare la correttezza della configurazione di Anti-virus file, effettuare quanto segue:*
  1. Creare una cartella sul disco, copiare il virus di prova scaricato dal sito Web ufficiale dell'organizzazione ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)), e le modifiche del virus di prova create.
  2. Lasciare che tutti gli eventi vengano registrati, in modo che il file report conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori.
  3. Lanciare il "virus" di prova o una sua variante.

Anti-virus file intercetterà la chiamata al file, lo esaminerà ed eseguirà l'azione specificata nelle impostazioni. Selezionando diverse azioni da eseguire sull'oggetto rilevato, sarà possibile verificare completamente il funzionamento del componente.

Il rapporto sul funzionamento del componente visualizza informazioni sui risultati dell'operazione eseguita da Anti-virus file.

# CONVALIDA DELLE IMPOSTAZIONI DELL'ATTIVITÀ DI SCANSIONE ANTIVIRUS

- ▶ *Per verificare la correttezza della configurazione dell'attività di scansione antivirus, effettuare quanto segue:*
  1. Creare una cartella sul disco, copiare il virus di prova scaricato dal sito Web ufficiale dell'organizzazione ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)), e le modifiche del virus di prova create.
  2. Creare una nuova attività di scansione antivirus e selezionare la cartella contenente il gruppo di "virus" di prova quali oggetti da esaminare.
  3. Lasciare che tutti gli eventi vengano registrati, in modo che il file report conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori.
  4. Eseguire l'attività di scansione anti-virus.

Quando l'attività è in esecuzione, le azioni specificate nelle impostazioni dell'attività verranno eseguite al rilevamento di oggetti infetti o sospetti. Selezionando diverse azioni da eseguire sull'oggetto rilevato, sarà possibile verificare completamente il funzionamento del componente.

Le informazioni complete sui risultati dell'attività sono visualizzabili nel rapporto sul funzionamento del componente.

# CONVALIDA DELLE IMPOSTAZIONI DI ANTI-SPAM

È possibile utilizzare un messaggio di prova identificato come SPAM per testare la protezione antispyam.

Il corpo del messaggio di prova deve contenere la seguente riga:

```
Spam is bad do not send it
```

Un volta ricevuto questo messaggio sul computer, l'applicazione lo esaminerà identificandolo come spam, ed eseguirà l'azione specificata per oggetti di questo tipo.

---

# DICHIARAZIONE SULLA RACCOLTA DATI PER KASPERSKY SECURITY NETWORK

## INTRODUZIONE

SI PREGA DI LEGGERE QUESTO DOCUMENTO CON ATTENZIONE. ESSO CONTIENE IMPORTANTI INFORMAZIONI CHE È IMPORTANTE CONOSCERE PRIMA DI CONTINUARE AD UTILIZZARE I NOSTRI SERVIZI O IL NOSTRO SOFTWARE. CONTINUANDO AD UTILIZZARE IL SOFTWARE ED I SERVIZI DI KASPERSKY LAB SI ACCETTA IMPLICITAMENTE QUESTA DICHIARAZIONE sulla Raccolta Dati DI KASPERSKY LAB. Ci riserviamo il diritto di modificare questa Dichiarazione sulla Raccolta Dati pubblicando le modifiche su questa pagina. Controllare la data di revisione sottoriportata per determinare se la politica sia stata modificata dall'ultima volta in cui è stata consultata. L'utilizzo continuato di qualsiasi porzione dei Servizi Kaspersky Lab in seguito alla pubblicazione della Dichiarazione sulla Raccolta Dati costituirà implicita accettazione delle modifiche.

Kaspersky Lab e suoi affiliati (collettivamente "**Kaspersky Lab**") ha creato questa Dichiarazione sulla Raccolta Dati per chiarire le sue pratiche di raccolta e diffusione dei dati per Kaspersky Anti-Virus e Kaspersky Internet Security.

## Garanzia da Kaspersky Lab

Kaspersky Lab è fortemente impegnata ad offrire un servizio di qualità superiore a tutti i suoi clienti, rispettando particolarmente le loro preoccupazioni relative alla Raccolta dei Dati. Ci rendiamo conto che potreste avere domande su come Kaspersky Security Network raccolga ed utilizzi le informazioni ed i dati ed abbiamo preparato questa dichiarazione per informarvi sui Principi di Raccolta Dati che regolano Kaspersky Security Network (La "**Dichiarazione sulla Raccolta Dati**" o "**Dichiarazione**").

La Dichiarazione sulla Raccolta Dati contiene diversi dettagli di ordine generale e tecnico sui passi implementati per rispettare le vostre preoccupazioni sulla Raccolta dei Dati. Abbiamo organizzato questa Dichiarazione sulla Raccolta Dati per processi ed aree principali, in modo che possiate rivedere rapidamente le informazioni che più vi interessano. Il concetto fondamentale è che soddisfare le vostre necessità ed aspettative è alle fondamenta di tutto quello che facciamo – e ciò include proteggere i vostri Dati.

I dati e le informazioni vengono raccolte da Kaspersky Lab; se dopo aver esaminato questa Dichiarazione sulla Raccolta Dati avete ancora domande o preoccupazioni relative alla Raccolta dei Dati, vi preghiamo di inviare un messaggio di posta elettronica a [support@kaspersky.com](mailto:support@kaspersky.com).

### **Cos'è il Kaspersky Security Network?**

Il servizio Kaspersky Security Network consente agli utenti dei prodotti di sicurezza Kaspersky Lab di tutto il mondo di aiutare a facilitare l'identificazione e quindi ridurre il tempo necessario a garantire la protezione contro i nuovi rischi ("allo stato brado") che prendono di mira il computer. Per identificare le nuove minacce e le loro origini, nonché per aiutare a migliorare la sicurezza degli utenti e la funzionalità del prodotto, Kaspersky Security Network raccoglie dati selezionati sulla sicurezza e le applicazioni in relazione ai potenziali rischi che prendono di mira il computer e li consegna a Kaspersky Lab per l'analisi. **Tali informazioni non contengono informazioni sull'utente identificabili a livello personale, e vengono utilizzate dal Kaspersky Lab per l'unico scopo di potenziare i suoi prodotti di sicurezza e far progredire ulteriormente le soluzioni contro minacce e virus pericolosi. In caso di trasmissione accidentale di qualsiasi dato personale dell'utente, Kaspersky Lab proteggerà e manterrà riservate tali informazioni in ottemperanza a questa Dichiarazione sulla Raccolta Dati.**

Partecipando a Kaspersky Security Network, voi e gli altri utenti dei prodotti di sicurezza di Kaspersky Lab di tutto il mondo contribuite significativamente ad un ambiente Internet più sicuro.

### **Problematiche legali**

Kaspersky Security Network può essere soggetto a diverse giurisdizioni, poiché i suoi servizi possono essere utilizzati in diverse giurisdizioni, tra cui gli Stati Uniti D'America. Kaspersky Lab rivelerà le informazioni identificabili a livello personali senza l'autorizzazione del proprietario se richiesto dalla legge, o se ritiene in buona fede che tale azione sia necessaria per investigare o proteggere gli ospiti, i visitatori, gli associati o le proprietà di Kaspersky Lab o gli altri da azioni nocive. Come detto sopra, le leggi relative ai dati ed alle informazioni raccolte da Kaspersky Security Network possono variare da paese a paese. Ad esempio, alcune informazioni identificabili a livello personale raccolte nell'Unione Europea e nei suoi Paesi Membri sono soggette alle Direttive UE sui dati personali, la Privacy e le comunicazioni elettroniche, comprese senza limitazione la Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, la Direttiva 95/46/Ce del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e le successive legislazioni adottate nei Paesi Membri UE, la decisione della Commissione Europea 497/2001/CE sulle clausole contrattuali standard (trasferimento di dati personali verso paesi terzi) e la successiva legislazione adottata nei Paesi Membri CE.

Kaspersky Security Network informerà debitamente gli utenti coinvolti, quando raccoglie inizialmente le informazioni suddette, di qualsiasi condivisione di tali informazioni, specificatamente in caso di utilizzo per lo sviluppo commerciale, e consentirà a tali utenti Internet di **accettare o rifiutare** (nei Paesi Membri CE e negli altri paesi dove è richiesta tale procedura) o rifiutare (per tutti gli altri paesi) on-line l'utilizzo commerciale di tali dati e/o la trasmissione di tali dati a terzi.

Le autorità giudiziarie o di ordine pubblico potrebbero chiedere a Kaspersky Lab di fornire alcune informazioni identificabili a livello personale alle autorità di governo competenti. Se richiesto dalle autorità giudiziarie o di pubblica sicurezza, forniremo tali informazioni al ricevimento della documentazione appropriata. Kaspersky Lab può inoltre fornire informazioni alle autorità di pubblica sicurezza per proteggere le sue proprietà e la salute e la sicurezza degli individui secondo le legge.

Verranno presentate Dichiarazioni alle Autorità sulla Privacy dei Paesi Membri secondo la legislazione in vigore in tali Paesi Membri UE. Le informazioni su tali dichiarazioni saranno rese accessibili sui servizi Kaspersky Security Network.

## **INFORMAZIONI RACCOLTE**

### **Dati che vengono raccolti**

Il servizio Kaspersky Security Network raccoglierà e sottoporrà a Kaspersky Lab dati essenziali ed estesi sui potenziali rischi per la sicurezza esistenti per il computer dell'utente. I dati essenziali raccolti comprendono:

#### Dati essenziali

- informazioni sul software e l'hardware installato sul computer, compreso il sistema operativo ed i service pack installati, gli oggetti kernel, i driver, i servizi, le estensioni di Internet Explorer, le estensioni del sistema di stampa, le estensioni di Esplora risorse, i programmi scaricati, elementi di impostazione attivi, gli applet del pannello di controllo, le voci del file Hosts e del registro, gli indirizzi IP, i tipi di browser, i client di posta elettronica ed il numero di versione dei prodotti Kaspersky Lab, che sono di solito informazioni non personalmente identificabili.
- una ID univoca generata dal prodotto Kaspersky Lab per identificare le singole macchine senza identificare l'utente, che non contiene informazioni personali.
- informazioni sullo stato della protezione antivirus del computer, e dati su qualsiasi file o attività per cui esista il sospetto di programma nocivo (es. nome virus, data/ora di rilevamento, nomi/percorsi e dimensione dei file infetti, IP e porta dell'attacco di rete, nome dell'applicazione sospettata di essere nociva). Si noti che i dati raccolti menzionati sopra non contengono informazioni identificabili a livello personale.

### Dati estesi

- Informazioni sulle informazioni firmate digitalmente scaricate dell'utente (URL, dimensione file, nome firmatario).
- Informazioni sulle applicazioni eseguibili (dimensioni, attributi, data di creazione, informazioni sulle intestazioni PE, regione, nome, ubicazione e utilità di compressione utilizzata).

### **Protezione della trasmissione e archiviazione dei Dati**

Kaspersky Lab è impegnata a proteggere la sicurezza delle informazioni che raccoglie. Le informazioni raccolte vengono conservate su server computer con accesso limitato e controllato. Kaspersky Lab opera reti di dati sicure, protette da firewall standard del settore e sistemi di protezione tramite password. Kaspersky Lab usa un'ampia gamma di tecnologie e procedure di sicurezza per proteggere le informazioni raccolte dalle minacce quali l'accesso, l'utilizzo o la pubblicazione non autorizzati. Le nostre politiche di sicurezza vengono periodicamente riviste e potenziate secondo necessità, e solo gli individui autorizzati possono accedere ai dati da noi raccolti. Kaspersky Lab fa tutto il possibile per garantire che le vostre informazioni siano trattate secondo quanto previsto dalla presente Dichiarazione. Purtroppo, nessuna trasmissione dei dati può essere garantita come sicura. Di conseguenza, nonostante facciamo il possibile per proteggere i vostri dati, non possiamo garantire la sicurezza di nessun dato trasmessoci da voi o dai nostri prodotti e servizi, includendo senza limitazioni Kaspersky Security Network, il cui utilizzo è pertanto a vostro rischio.

I dati raccolti possono essere trasferiti ai server di Kaspersky Lab e Kaspersky Lab ha preso le necessarie precauzioni per garantire che le informazioni raccolte, se trasferite, siano adeguatamente protette. Trattiamo i dati che raccogliamo come informazioni riservate; sono di conseguenza soggette alle nostre procedure di sicurezza ed alle nostre politiche aziendali riguardanti la protezione e l'utilizzo di dati riservati. Quando i dati raccolti raggiungono Kaspersky Lab, vengono conservati su un server con caratteristiche di sicurezza fisiche ed elettroniche, come da procedure solite del settore, che includono l'utilizzo di procedure di accesso con password e firewall elettronici progettati per bloccare l'accesso non autorizzato dall'esterno di Kaspersky Lab. I dati raccolti da Kaspersky Security Network coperti dalla presente Dichiarazione vengono elaborati e conservati negli Stati Uniti e possibilmente in altre giurisdizioni ed altri paesi dove Kaspersky Lab porta avanti le sue attività. Tutti i dipendenti di Kaspersky Lab conoscono le nostre politiche di sicurezza. I vostri dati sono accessibili esclusivamente ai dipendenti che ne hanno bisogno per il loro lavoro. I dati conservati non saranno associati a nessuna informazione identificabile a livello personale. Kaspersky Lab non combina i dati conservati da Kaspersky Security Network con i dati, le liste di contatti o le informazioni di abbonamento che vengono raccolti da Kaspersky Lab a scopi proporzionali o altri scopi.

## **USO DEI DATI RACCOLTI**

### **Come vengono utilizzate le vostre informazioni personali**

Kaspersky Lab raccoglie i dati per analizzare ed identificare le origini di possibili rischi di sicurezza nonché per migliorare la capacità dei prodotti Kaspersky Lab di rilevare comportamenti malvagi, siti Web fraudolenti, programmi criminali ed altri tipi di minacce alla sicurezza su Internet per offrire in futuro il miglior livello di protezione possibile ai clienti Kaspersky Lab.

### **Divulgazione delle informazioni a Terzi**

Kaspersky Lab può divulgare qualsiasi informazione raccolta se richiesto da un agente di pubblica sicurezza secondo quanto disposto o permesso dalla legge, in risposta ad una citazione in giudizio od altro procedimento legale, se ritiene in buona fede che ciò sia stato richiesto per ottemperare alle leggi e normative applicabili o ad una citazione in giudizio o altro procedimento legale o richiesta esecutiva del governo. Kaspersky Lab può inoltre divulgare informazioni identificabili a livello personale se ci sono ragioni di credere che tale divulgazione sia necessaria per identificare, contattare o procedere legalmente contro chiunque possa stare violando la presente Dichiarazione, i termini dei vostri accordi con l'Azienda o per proteggere la sicurezza dei suoi utenti, o nel rispetto di accordi di riservatezza e licenza con alcune terze parti che collaborano con noi nello sviluppare, utilizzare e gestire Kaspersky Security Network. Per promuovere la sensibilizzazione, l'identificazione e la prevenzione dei rischi alla sicurezza su Internet, Kaspersky Lab può condividere alcune informazioni con organizzazione di ricerca ed altri operatori nel settore del software di sicurezza. Kaspersky Lab può inoltre utilizzare statistiche derivate dalle informazioni raccolte per creare e pubblicare rapporti sulle tendenze relative ai rischi alla sicurezza.

### **Scelte a vostra disposizione**

La partecipazione a Kaspersky Security Network è volontaria. È possibile attivare e disattivare il servizio Kaspersky Security Network in qualsiasi momento visitando le impostazioni di Feedback nella pagina delle opzioni del prodotto Kaspersky Lab. Si noti tuttavia che, se si sceglie di trattenere le informazioni o i dati richiesti, potremmo non essere in grado di fornire alcuni dei servizi dipendenti dalla raccolta di tali dati.

Una volta terminato il periodo di servizio del prodotto Kaspersky Lab, alcune delle funzioni del software Kaspersky Lab potrebbero continuare a funzionare, ma le informazioni non verranno più inviate automaticamente a Kaspersky Lab.

Ci riserviamo inoltre il diritto di inviare messaggi di allarme non frequenti agli utenti per informarli di modifiche specifiche che possano influenzare la loro possibilità di utilizzare i nostri servizi ai quali si sono precedentemente abbonati. Ci riserviamo inoltre il diritto di contattarvi se obbligati ad agire in tal senso a causa di procedimenti legali o se c'è stata una violazione di qualsiasi accordo di licenza, di garanzia o di acquisto.

Kaspersky Lab mantiene tali diritti perché, in casi limitati, riteniamo di poter aver bisogno del diritto di contattarvi per motivi legali o in relazione a problematiche che potrebbero essere importanti per voi. Questi diritti non ci consentono di contattarvi per proporre servizi nuovi o esistenti se ci è stato richiesto di non farlo, e l'invio di comunicazioni di questo tipo è raro.

## **RACCOLTA DEI DATI – RICHIESTE D'INFORMAZIONI E RECLAMI CORRELATI**

Kaspersky Lab prende ed affronta le preoccupazione dei suoi utenti in merito alla Raccolta dei Dati col massimo rispetto e la massima serietà. Se ritenete che ci sia state occasioni di violazione della presente Dichiarazione in relazione alle vostre informazioni o ai vostri dati, o se avete altre richieste d'informazioni o preoccupazioni, potete scrivere a Kaspersky Lab al seguente indirizzo: [support@kaspersky.com](mailto:support@kaspersky.com).

Nel messaggio, descrivete più dettagliatamente possibile la natura della vostra richiesta. Affronteremo la vostra richiesta o il vostro reclamo con prontezza.

Le informazioni vengono fornite volontariamente. L'opzione di raccolta dei dati può essere disattivata dall'utente in qualsiasi momento nella sezione "**Feedback**" alla pagina "**Impostazioni**" di qualsiasi prodotto Kaspersky Lab.

Copyright © 2008 Kaspersky Lab. Tutti i diritti riservati.

---

# KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di software per la sicurezza e offre sistemi anti-virus, anti-spam e anti-hacking ad alte prestazioni.

Kaspersky Lab è un'azienda internazionale. Con sede centrale nella Federazione russa, l'azienda ha uffici di rappresentanza nel Regno Unito, in Francia, Germania, Giappone, nei paesi del Benelux, in Cina, Polonia, Romania e negli USA (California). Recentemente è stata inaugurata una nuova sede aziendale, l'European Anti-Virus Research Centre, in Francia. La rete di partner di Kaspersky Lab conta su oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab ha alle sue dipendenze oltre 450 specialisti qualificati, tra cui 10 laureati in economia e commercio e 16 qualificati in dottorato di ricerca. Gli specialisti più anziani sono membri del CARO (Computer Anti-Virus Researchers Organization).

Il capitale più grande della nostra azienda è costituito dalla conoscenza e la competenza senza pari, accumulate dai suoi specialisti in quattordici anni di lotta incessante contro i virus informatici. L'approfondita analisi delle attività dei virus informatici consente agli specialisti dell'azienda di prevedere le tendenze di sviluppo dei programmi nocivi ed offrire ai nostri utenti una protezione puntuale contro i nuovi tipi di attacchi. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'offrire la protezione anti-virus ai nostri clienti.

Anni di duro lavoro hanno fatto dell'azienda uno dei principali sviluppatori di software anti-virus. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Internet Security, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, file server, sistemi di posta elettronica, firewall, gateway Internet e palmari. I pratici strumenti di gestione offerti dall'azienda sono facili da utilizzare e consentono di automatizzare al massimo la protezione antivirus dei computer e delle reti aziendali. Numerose imprese di grande notorietà si affidano a Kaspersky Internet Security. L'elenco di tali aziende comprende Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di un'ampia gamma di servizi supplementari volti a garantire non solo un funzionamento stabile dei prodotti dell'azienda, ma anche la conformità a qualsiasi esigenza aziendale specifica. Progettiamo, implementiamo e supportiamo sistemi anti-virus aziendali. Il

database antivirus di Kaspersky Lab viene aggiornato ogni ora. Il servizio di supporto tecnico offerto ai clienti dell'azienda è disponibile 24 ore su 24 in diverse lingue.

## IN QUESTA SEZIONE:

---

Altri prodotti Kaspersky Lab.....	77
Recapiti .....	86

# ALTRI PRODOTTI KASPERSKY LAB

## Kaspersky Lab News Agent

Il News Agent del programma viene utilizzato per comunicare rapidamente le novità di Kaspersky Lab, le notifiche sul "clima virale" e gli eventi più recenti. L'applicazione legge l'elenco dei canali di news e le informazioni in essi contenute dai news server di Kaspersky Lab ad intervalli specificati.

Inoltre, il News Agent consente di:

- visualizzare il "clima virale" nell'area di notifica;
- abbonarsi ai canali di news di Kaspersky Lab o di annullare l'iscrizione;
- ricevere news da ciascun canale sottoscritto con la frequenza specificata; inoltre è possibile ricevere notifica delle notizie non lette;
- visualizzare le notizie dei canali sottoscritti;
- rivedere l'elenco dei canali ed il loro stato;
- aprire la pagine con notizie dettagliate nel browser.

Il News Agent viene eseguito in Microsoft Windows e può essere utilizzato come applicazione autonoma o essere incluso nelle soluzioni integrate offerte da Kaspersky Lab.

## Kaspersky® OnLine Scanner

Il programma è un servizio gratuito disponibile ai visitatori del sito Web aziendale, e consente di eseguire efficienti scansioni antivirus on-line del computer. Kaspersky Online Scanner viene eseguito direttamente nel browser. In questo modo, gli utenti possono rapidamente ricevere risposta alle loro

domande relative alle infezioni con programmi nocivi. Nel corso di una scansione, l'utente può:

- escludere gli archivi e i database di posta dalla scansione;
- selezionare database standard o estesi da utilizzare durante la scansione;
- salvare i risultati della scansione in formato txt o html.

### **Kaspersky® OnLine Scanner Pro**

Il programma è un servizio ad abbonamento disponibile ai visitatori del sito Web aziendale, e consente di eseguire efficienti scansioni antivirus on-line del computer, nonché di disinfettare i file infetti. Kaspersky Online Scanner viene eseguito direttamente nel browser. Nel corso di una scansione, l'utente può:

- escludere gli archivi e i database di posta dalla scansione;
- selezionare database standard o estesi da utilizzare durante la scansione;
- disinfetta gli oggetti infetti rilevati;
- salvare i risultati della scansione in formato txt o html.

### **Kaspersky Anti-Virus® Mobile**

Kaspersky® Anti-Virus Mobile garantisce la protezione antivirus ai dispositivi mobili che eseguono i sistemi operativi Symbian OS e Microsoft Windows Mobile. Il programma consente di eseguire complesse scansioni antivirus, fra cui:

- scansioni manuali della memoria del dispositivo mobile, delle memory card e delle singole cartelle, nonché di file specifici. Una volta rilevato un file infetto, esso viene spostato in quarantena o eliminato;
- protezione in tempo reale: tutti gli oggetti in entrata o modificati vengono esaminati, come anche tutti i file nel momento in cui si cerca di accedere ad essi;
- protezione contro la spam sms e mms.

### **Kaspersky Anti-Virus for File Servers**

Questo prodotto software garantisce la protezione affidabile dei file system dei server che utilizzano i sistemi operativi Microsoft Windows, Novell NetWare e Linux da tutti i tipi di software nocivo. La struttura di questo prodotto software include le seguenti applicazioni di Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Vantaggi e capacità funzionali:

- *protezione in tempo reale del file system dei server*: tutti i file del server verranno esaminati quando si cerca di aprirli o salvarli sul server;
- *prevenzione delle pandemie di virus*;
- *scansione manuali* dell'intero file system o di singoli file e singole cartelle;
- *uso di tecnologie di ottimizzazione* durante la scansione di oggetti nel file system del server;
- *ripristino del sistema dopo l'infezione*;
- *scalabilità del prodotto software* in funzione delle risorse di sistema disponibili;
- *mantenimento dell'equilibrio del carico sul sistema*;
- *creazione di un elenco di processi attendibili* la cui attività sul server non sarà monitorata da questo prodotto;
- *gestione remota del prodotto*, compresa l'installazione centralizzata, la configurazione e la gestione;
- *salvataggio delle copie di backup* degli oggetti infetti ed eliminati se fosse necessario ripristinarli;
- *isolamento degli oggetti sospetti* in una memoria speciale;
- *notifica degli eventi* verificatisi durante il funzionamento del prodotto all'amministratore del sistema;
- *conservazione di report dettagliati*;
- *aggiornamento automatico dei database* del prodotto software.

## **Kaspersky Open Space Security**

**Kaspersky Open Space Security** è un prodotto software che implementa un approccio nuovo alla sicurezza delle reti aziendali moderne di qualsiasi dimensione, ed offre la protezione centralizzata ai sistemi informatici ed il supporto agli uffici remoti ed agli utenti mobili.

Questo prodotto software comprende quattro programmi:

- Kaspersky Open Space Security.

- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Ciascun prodotto è descritto dettagliatamente di seguito.

**Kaspersky WorkSpace Security** è un prodotto progettato per garantire la protezione centralizzata delle workstation in una rete aziendale e oltre contro tutti i tipi di moderne minacce Internet: virus, spyware, attacchi di hacking e spam.

Vantaggi e capacità funzionali:

- *protezione completa da virus, attacchi di hacking e spam;*
- *difesa proattiva* contro i programmi nocivi più recenti che ancora non sono stati aggiunti ai database;
- *personal Firewall* con sistema di rilevamento delle intrusioni e prevenzione degli attacchi di rete;
- *ripristino in seguito a modifiche nocive del sistema;*
- *protezione dagli attacchi di phishing e dalla posta spam;*
- *distribuzione delle risorse* dinamica durante le scansioni complete del sistema;
- *gestione remota del prodotto*, compresa l'installazione centralizzata, la configurazione e la gestione;
- *supporto per Cisco® NAC* (Network Admission Control);
- *scansione della posta elettronica e del traffico Internet* in tempo reale;
- *blocco delle finestre pop-up e dei banner pubblicitari* su Internet;
- *funzionamento sicuro in qualsiasi tipo di rete*, tra cui quelle Wi-Fi;
- *strumenti per la creazione di dischi di ripristino* che consentono il ripristino dopo un attacco virale;
- *sistema di reporting completo* sullo stato della protezione;
- *aggiornamenti automatici al database;*
- *supporto completo per sistemi operativi a 64 bit;*
- *ottimizzazione del programma per PC portatili* (tecnologia Intel® Centrino® Duo per PC portatili);

- *capacità di disinfezione remota* (tecnologia Intel® Active Management, componente Intel® vPro™).

**Kaspersky Business Space Security** garantisce la protezione ottimale delle risorse informative dalle moderne minacce su Internet. Kaspersky Business Space Security protegge le workstation ed i file server da tutti i tipi di virus, programmi Trojan e worm, previene le pandemie di virus e protegge le informazioni garantendo nel contempo agli utenti un accesso istantaneo alle risorse di rete.

Vantaggi e capacità funzionali:

- *gestione remota del prodotto*, compresa l'installazione centralizzata, la configurazione e la gestione;
- *supporto per Cisco® NAC* (Network Admission Control);
- *protezione delle workstation e dei server da tutti i tipi di minacce su Internet*;
- *utilizzo della tecnologia iSwift per evitare la ripetizione delle scansioni* nella rete;
- *distribuzione del carico tra i processori del server*;
- *isolamento degli oggetti sospetti* in una memoria speciale;
- *ripristino in seguito a modifiche nocive del sistema*;
- *scalabilità del prodotto software* in funzione delle risorse di sistema disponibili;
- *difesa proattiva* delle workstation contro i programmi nocivi più recenti che ancora non sono stati aggiunti ai database;
- *scansione della posta elettronica e del traffico Internet* in tempo reale;
- *personal Firewall* con sistema di rilevamento delle intrusioni e prevenzione degli attacchi di rete;
- *protezione del funzionamento nelle reti wireless Wi-Fi*;
- *tecnologia di autoprotezione del programma anti-virus* contro i programmi nocivi;
- *isolamento degli oggetti sospetti* in una memoria speciale;
- *aggiornamenti automatici al database*.

### **Kaspersky Enterprise Space Security**

Questo prodotto software comprende componenti di protezione delle workstation e dei server condivisi contro tutti i tipi di minacce Internet moderne, rimuove i virus dai flussi di posta elettronica, garantisce la

sicurezza delle informazioni e un accesso istantaneo e sicuro alle risorse di rete da parte degli utenti.

Vantaggi e capacità funzionali:

- *protezione delle workstation e dei server da virus, programmi Trojan, e worm;*
- *protezione dei server di posta Sendmail, Qmail, Postfix e Exim;*
- *scansione di tutti i messaggi sul server di Microsoft Exchange, comprese le cartelle condivise;*
- *elaborazione di messaggi, database ed altri oggetti su server Lotus Domino;*
- *protezione dagli attacchi di phishing e dalla posta spam;*
- *prevenzione degli invii in massa e delle pandemie di virus;*
- *scalabilità del prodotto software* in funzione delle risorse di sistema disponibili;
- *gestione remota del prodotto*, compresa l'installazione centralizzata, la configurazione e la gestione;
- *supporto per Cisco® NAC (Network Admission Control);*
- *difesa proattiva* delle workstation contro i programmi nocivi più recenti che ancora non sono stati aggiunti ai database;
- *personal Firewall* con sistema di rilevamento delle intrusioni e prevenzione degli attacchi di rete;
- *funzionamento sicuro nelle reti wireless Wi-Fi;*
- *scansione del traffico Internet* in tempo reale;
- *ripristino in seguito a modifiche nocive del sistema;*
- *distribuzione delle risorse* dinamica durante le scansioni complete del sistema;
- *isolamento degli oggetti sospetti* in una memoria speciale;
- *sistema di reporting completo* sullo stato del sistema di protezione;
- *aggiornamenti automatici al database.*

### **Kaspersky Total Space Security**

Questa soluzione controlla tutti i flussi di dati in entrata ed uscita – posta elettronica, traffico Web e tutte le interazioni di rete. Il prodotto comprende componenti utilizzati per proteggere le workstation ed i dispositivi mobili,

assicura agli utenti un accesso istantaneo e protetto alle risorse informatiche aziendali ed Internet e garantisce comunicazioni sicure via posta elettronica.

Vantaggi e capacità funzionali:

- *protezione completa da virus, attacchi di hacking e spam* a tutti i livelli della rete aziendale, dalle workstation ai gateway;
- *difesa proattiva* delle workstation contro i programmi nocivi più recenti che ancora non sono stati aggiunti ai database;
- *protezione dei server di posta e di quelli condivisi*;
- *scansione in tempo reale del traffico Web LAN in entrata (HTTP / FTP)*;
- *scalabilità del prodotto software* in funzione delle risorse di sistema disponibili;
- *blocco dell'accesso dalle workstation infette*;
- *prevenzione delle pandemie di virus*;
- *reporting centralizzato sullo stato di protezione*;
- *gestione remota del prodotto*, compresa l'installazione centralizzata, la configurazione e la gestione;
- *supporto per Cisco® NAC (Network Admission Control)*;
- *supporto dei server proxy di tipo hardware*;
- *filtraggio del traffico Internet secondo un elenco di server affidabili*, tipi di oggetti e gruppi di utenti;
- *utilizzo della tecnologia iSwift per evitare la ripetizione delle scansioni* nella rete;
- *distribuzione delle risorse* dinamica durante le scansioni complete del sistema;
- *personal Firewall* con sistema di rilevamento delle intrusioni e prevenzione degli attacchi di rete;

- funzionamento sicuro in qualsiasi tipo di rete, tra cui quelle Wi-Fi;
- *protezione dagli attacchi di phishing e dalla posta spam;*
- *capacità di disinfezione remota (tecnologia Intel® Active Management, componente Intel® vPro™);*
- *ripristino in seguito a modifiche nocive del sistema;*
- *tecnologia di autoprotezione del programma anti-virus contro i programmi nocivi;*
- *supporto completo per sistemi operativi a 64 bit;*
- aggiornamenti automatici al database.

### **Kaspersky Security for Mail Servers**

Prodotto software per la protezione dei server di posta e di quelli condivisi dai programmi nocivi e dalla posta spam. Il prodotto comprende applicazioni per la protezione del server di posta più diffusi: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim, e consente di creare un gateway di posta dedicato. Questa soluzione comprende:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus® for Linux Mail Server.

Le capacità di questo programma comprendono:

- *protezione affidabile dai programmi nocivi o potenzialmente pericolosi;*
- *filtraggio antispam;*
- *scansione dei messaggi di posta in entrata ed in uscita, nonché degli allegati;*
- *scansione antivirus di tutti i messaggi sul server di Microsoft Exchange, comprese le cartelle condivise;*

- *scansione di messaggi, database ed altri oggetti su server Lotus Domino;*
- *filtraggio dei messaggi per tipo di allegato;*
- *isolamento degli oggetti sospetti in una memoria speciale;*
- *pratico sistema per la gestione del prodotto software;*
- *prevenzione delle pandemie di virus;*
- *monitoraggio dello stato del sistema di protezione tramite notifiche;*
- *sistema di reporting sul funzionamento dell'applicazione;*
- *scalabilità del prodotto software in funzione delle risorse di sistema disponibili;*
- *aggiornamenti automatici al database.*

### **Kaspersky Security for Gateways**

Questo prodotto software garantisce l'accesso sicuro ad Internet per tutti i dipendenti dell'azienda, eliminando automaticamente i programmi nocivi e pericolosi dal flusso di dati in entrata dalla rete tramite i protocolli HTTP/FTP. Questa soluzione comprende:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Le capacità di questo programma comprendono:

- *protezione affidabile dai programmi nocivi o potenzialmente pericolosi;*
- *scansione del traffico Internet (HTTP/FTP) in tempo reale;*
- *filtraggio del traffico Internet secondo un elenco di server affidabili, tipi di oggetti e gruppi di utenti;*
- *isolamento degli oggetti sospetti in una memoria speciale;*
- *pratico sistema di controllo;*

- *sistema di reporting sul funzionamento dell'applicazione;*
- *supporto dei server proxy di tipo hardware;*
- *scalabilità del prodotto software* in funzione delle risorse di sistema disponibili;
- *aggiornamenti automatici al database.*

### **Kaspersky® Anti-Spam**

Kaspersky Anti-Spam è il primo pacchetto software russo utilizzato per garantire la protezione dalla posta spam per le piccole e medie aziende. Il prodotto combina le rivoluzionarie tecnologie di analisi linguistica del testo e tutti i moderni metodi di filtraggio delle posta elettronica (tra cui la lista nera DNS e gli attributi formali dei messaggi) con una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Kaspersky Anti-Spam è un filtro impostato all'ingresso della rete aziendale che esamina il flusso di messaggi in arrivo alla ricerca di spam. È compatibile con qualsiasi sistema di posta già in uso nella rete del cliente, e può essere installato sia su server mail esistenti che dedicati.

L'elevata efficienza del programma è dovuta all'aggiornamento automatico quotidiano dei database di filtraggio dei contenuti con campioni provenienti dagli specialisti del laboratorio linguistico. Gli aggiornamenti vengono rilasciati ogni 20 minuti.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® for MIMESweeper garantisce scansioni antivirus ad alta velocità del traffico sui server che utilizzano Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

L'applicazione viene implementata come plug-in (modulo di estensione) ed esamina ed elabora in tempo reale i messaggi e-mail in entrata ed in uscita alla ricerca di virus.

## **RECAPITI**

In caso di domande, è possibile contattare i nostri rivenditori o direttamente Kaspersky Lab. Sono disponibili consulenze approfondite per telefono o via posta elettronica. Verranno offerte risposte esaustive e complete a qualsiasi domanda.

Indirizzo:	00187 Roma Corso Vittorio Emanuele II, 197
Supporto di emergenza 24/7:	<a href="http://kb.kaspersky.it">http://kb.kaspersky.it</a>
Forum Web di Kaspersky Lab:	<a href="http://forum.kaspersky.com">http://forum.kaspersky.com</a>
Laboratorio Anti-Virus:	<a href="mailto:newvirus@kaspersky.com">newvirus@kaspersky.com</a> (Solo per inviare nuovi virus negli archivi)
Ufficio vendite:	<a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>
Informazioni di carattere generale:	<a href="mailto:info@kaspersky.com">info@kaspersky.com</a>
WWW:	<a href="http://www.kaspersky.com/it">http://www.kaspersky.com/it</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a>

---

# CRYPTOEX LLC

Per la creazione e la verifica delle firme digitali Kaspersky Internet Security utilizza la libreria di software per la sicurezza dei dati Crypto C sviluppata da Crypto Ex LLC.

Crypto Ex possiede la licenza della Federal Agency for Government Communications and Information (FSB – Federal Security Service) per lo sviluppo, la produzione e la distribuzione di sistemi complessi di crittografia per la protezione dei dati non costituenti un segreto di stato.

La libreria Crypto C è progettata per l'utilizzo nei sistemi di protezione complessa delle informazioni riservate di classe KS1 ed ha ottenuto il certificato di conformità nr. SF/114-0901 in data 1 Luglio 2006.

I moduli di questa libreria utilizzano la criptazione e decrittazione di pacchetti di dati e flussi di dati di dimensione fissa, tramite un algoritmo crittografico (GOST 28147-89), la generazione e verifica delle firme digitali elettroniche basate su algoritmi (GOST R 34.10-94 e GOST 34.10-2001), funzione hash (GOST 34.11-94), generazione di informazioni chiave tramite un trasmettitore numeri di programma pseudo-random. Inoltre, CryptoEx LLC ha implementato un sistema di generazione delle informazioni chiave e di simulazione vettoriale (GOST 28147-89).

I moduli della libreria sono stati implementati utilizzando il linguaggio di programmazione C (in conformità allo standard ANSIC) e possono essere integrati nelle applicazioni come codice caricato staticamente e dinamicamente, nonché eseguiti su piattaforme x86, x86-64, Ultra SPARC II e compatibili.

I moduli della libreria possono essere portati sui seguenti ambienti operativi: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris for Ultra SPARC II).

Sito Web aziendale CryptoEx LLC: <http://www.cryptoex.ru>

Posta elettronica: [info@cryptoex.ru](mailto:info@cryptoex.ru)

---

# MOZILLA FOUNDATION

Per lo sviluppo del componente dell'applicazione è stato utilizzata la libreria **Gecko SDK ver. 1.8**.

Questo software è utilizzato secondo i termini e le condizioni della licenza MPL 1.1 Licenza pubblica Mozilla Foundation <http://www.mozilla.org/MPL>.

Per ulteriori dettagli su questa libreria Gecko SDK fare riferimento a: [http://developer.mozilla.org/en/docs/Gecko\\_SDK](http://developer.mozilla.org/en/docs/Gecko_SDK).

© Mozilla Foundation

Sito Web Mozilla Foundation: <http://www.mozilla.org>.

---

# CONTRATTO DI LICENZA

Contratto di licenza standard per l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALMENTE VINCOLANTE ("CONTRATTO") RELATIVO ALLA LICENZA PER KASPERSKY INTERNET SECURITY ("SOFTWARE") PRODOTTO DA KASPERSKY LAB ("KASPERSKY LAB").

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, CLICCANDO SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, CLICCANDO SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

CONFORMEMENTE ALLA NORMATIVA RELATIVA AL SOFTWARE KASPERSKY PER SINGOLI UTENTI E ACQUISTATO SCARICANDO IL FILE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE PUÒ RESTITUIRE IL PRODOTTO AL RIVENDITORE PER LA SOSTITUZIONE O IL RIMBORSO COMPLETO ENTRO QUATTORDICI (14) GIORNI LAVORATIVI DALLA DATA DELL'ACQUISTO, A PATTO CHE LA CONFEZIONE NON SIA STATA APERTA.

IL SOFTWARE KASPERSKY PER UTENTI SINGOLI NON ACQUISTATO ONLINE SU INTERNET NON PUÒ ESSERE RESTITUITO PER IL RIMBORSO NÉ PER LA SOSTITUZIONE SE NON DIVERSAMENTE STABILITO DAL PARTNER CHE RIVENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON È VINCOLATO DALLE CLAUSOLE STABILITE DAL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Tutti i riferimenti al termine "Software" contenuti nel presente documento includeranno il codice di attivazione del software che sarà fornita all'utente da Kaspersky Lab come parte integrante di Kaspersky Internet Security 2009.

1. *Concessione della licenza.* Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione

in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno. È possibile installare una copia del Software su un computer.

1.1 *Uso.* Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un computer o da più di un utente per volta, salvo quanto diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (vale a dire nella memoria ad accesso casuale o RAM) o è installato nella memoria permanente (per esempio disco fisso, CD-ROM, o altro dispositivo di memoria) di quel computer. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di backup, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Il Software protegge i computer dai virus e dagli attacchi di rete la cui firma sia contenuta nei database degli elenchi delle minacce e degli attacchi di rete disponibili presso i server di aggiornamento di Kaspersky Lab.

1.1.3 Qualora l'utente venda il computer su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.4 All'utente è fatto divieto di decompilare, reingegnerizzare, disassemblare o altrimenti ridurre qualsiasi parte del presente Software a una forma leggibile dall'uomo e di permettere a terzi di compiere tali azioni. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi per computer creati indipendentemente sarà fornita da Kaspersky Lab dietro richiesta e dietro pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab notificasse al cliente che, per qualsiasi ragione, inclusa senza tuttavia ad essa limitarsi quella dei costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire le operazioni di decompilazione o reverse engineering entro i limiti previsti dalla legge.

1.1.5 L'utente non deve effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software, né creare opere da esso derivate derivate, né permettere a terzi di copiarlo (in modo diverso da quanto espressamente permesso nel presente documento).

1.1.6 All'utente è fatto divieto di affittare, noleggiare o prestare il Software a terzi oltre che di trasferire o di fornire a terzi la licenza in concessione.

1.1.7 Il codice di attivazione o la chiave di licenza non dovranno essere forniti a terzi, né si consentirà a terzi di accedere al codice di attivazione o alla chiave di licenza. Il codice di attivazione e la chiave di licenza sono dati riservati.

1.1.8 Kaspersky Lab può richiedere all'utente di installare la versione più recente del Software (la versione più recente nonché il più recente pacchetto di manutenzione).

1.1.9 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

1.1.10 L'utente ha il diritto di fornire a Kaspersky Lab informazioni su possibile minacce e vulnerabilità dal computer; ulteriori dettagli sonospecificati nella Dichiarazione sulla raccolta dati. Le informazioni raccolte vengono utilizzate in formato generico all'unico scopo di migliorare i prodotti di Kaspersky Lab.

1.1.11 Per gli scopi dichiarati nella clausola 1.1.10, il Software raccoglierà automaticamente informazioni sulle checksum dei file eseguiti in un computer e li invierà a Kaspersky Lab.

Assistenza<sup>1</sup>.

(i) Kaspersky Lab fornirà all'utente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per il periodo specificato nel File chiave di licenza e indicato nella finestra "Servizio", a partire dalla data di attivazione, dietro:

- (a) pagamento della tariffa di assistenza corrente; e
- (b) compilazione del Modulo di richiesta dei Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale si richiede all'utente di inserire il codice di attivazione fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

I servizi di assistenza saranno disponibili dopo l'attivazione del Software. Il Servizio di assistenza di Kaspersky Lab ha inoltre diritto di richiedere all'utente finale ulteriore identificazione per assegnare l'identificatore che dà diritto ai Servizi di Assistenza.

Fino all'attivazione del software e/o all'ottenimento dell'identificatore dell'utente finale (ID cliente) il servizio di assistenza presterà assistenza esclusivamente per l'attivazione del Software e la registrazione dell'utente finale.

---

<sup>1</sup> Quando l'utente utilizza la versione di prova del Software, non avrà diritto all'Assistenza tecnica specificata nella Clausola 2 del presente Contratto di licenza, né potrà vendere la copia in suo possesso a terzi.

L'utente avrà diritto ad utilizzare il Software a scopi dimostrativi per il periodo specificato nel file chiave di licenza, a partire dal momento in cui viene attivato (questo periodo può essere visualizzato nella finestra Servizio dell'interfaccia grafica utente del software).

- (ii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza.
- (iii) Per "Servizi di assistenza" si intende:
  - (a) Aggiornamento regolare del database antivirus;
  - (b) Aggiornamenti del database contro gli attacchi di rete;
  - (c) Aggiornamenti del database anti-spam;
  - (d) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;
  - (e) Assistenza tecnica tramite Internet o linea telefonica dedicata forniti dal distributore e/o dal rivenditore;
  - (f) Aggiornamenti per la rilevazione e la disinfezione dei virus 24 ore su 24.
- (iv) I servizi di assistenza vengono forniti solo se e quando sul computer dell'utente è installata l'ultima versione del Software come disponibile sul sito Web ufficiale di Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)).

3. *Diritti di proprietà.* Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

4. *Riservatezza.* L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi, costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del codice di attivazione.

#### 5. *Garanzia limitata.*

- (i) Kaspersky Lab garantisce che, per un periodo di sei (6) mesi a decorrere dal primo download o processo d'installazione, il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzionalità descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione stessa.

- (ii) L'utente si assume ogni responsabilità in merito alla scelta del presente Software per le proprie esigenze. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.
- (iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus ed i messaggi spam noti, né esclude che possa occasionalmente riportare erroneamente un virus in un titolo non infettato da quel virus.
- (iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.
- (v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.
- (vi) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilità di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (vi), potrebbero verificarsi tra Kaspersky Lab e l'utente o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o *altro*, che con ciò sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualità, all'idoneità allo scopo o all'uso di competenza e cura ragionevoli).

#### 6. Limitazione di responsabilità.

- (i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente a (a) responsabilità civile per frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle condizioni del presente Contratto, o (c) da qualsiasi altra responsabilità che non possa essere esclusa per legge.
- (ii) Ai sensi del paragrafo (i), Kaspersky Lab non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):
  - (a) Perdita di reddito;

- (b) Perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);
  - (c) Perdita di liquidità;
  - (d) Perdita di risparmi presunti;
  - (e) Perdita di attività;
  - (f) Perdita di opportunità;
  - (g) Perdita di avviamento;
  - (h) Danni alla reputazione;
  - (i) Perdita, danni o corruzione di dati; o
  - (j) Eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i).
- (iii) Ai sensi del paragrafo (i) sopra, la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

7. Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto.