

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



Kaspersky Anti-Virus® Personal 5.0

MANUALE D'USO

KASPERSKY ANTI-VIRUS® PERSONAL 5.0

Manuale d'uso

© Kaspersky Lab
<http://www.kaspersky.com>

Data di revisione: novembre 2004

Sommario

CAPITOLO 1. INTRODUZIONE.....	6
1.1. Virus informatici e programmi maligni.....	6
1.2. Gli obiettivi e le funzioni principali di Kaspersky Anti-Virus® Personal.....	7
1.3. Nuove funzioni della versione 5.0.....	9
1.4. Requisiti di sistema hardware e software.....	10
1.5. Kit di distribuzione.....	11
1.6. Servizi riservati agli utenti registrati.....	12
CAPITOLO 2. INSTALLAZIONE DEL PROGRAMMA SUL COMPUTER.....	13
CAPITOLO 3. IN CASO DI INFEZIONE DEL COMPUTER.....	18
3.1. Sintomi di infezione.....	18
3.2. Cosa fare in presenza di sintomi di infezione.....	19
CAPITOLO 4. PROTEZIONE ANTIVIRUS CON LE IMPOSTAZIONI PREDEFINITE DI KASPERSKY® AV PERSONAL.....	21
4.1. Protezione in tempo reale.....	21
4.2. Scansione manuale.....	22
4.3. Aggiornamento dei database antivirus.....	24
CAPITOLO 5. INTERFACCIA DEL PROGRAMMA.....	25
5.1. L'icona della barra delle applicazioni.....	25
5.2. Il menu di scelta rapida.....	26
5.3. La finestra principale dell'applicazione: struttura generale.....	27
5.3.1. Scheda <i>Protezione</i>	29
5.3.2. Scheda <i>Impostazioni</i>	30
5.3.3. Scheda <i>Assistenza</i>	31
5.4. La finestra Scansione.....	33
5.5. Sistema di riferimento del programma.....	34
CAPITOLO 6. PREVENZIONE DELLE INFEZIONI DA VIRUS.....	35
6.1. Quando eseguire la scansione antivirus.....	37
6.2. Impostazioni di scansione da utilizzare.....	38
6.3. Avvio della scansione manuale.....	43
6.4. Scansione completa programmata.....	44
6.5. Scansione manuale di oggetti selezionati.....	45

6.6. Scansione di archivi.....	48
CAPITOLO 7. SCANSIONE DI UN CD O FLOPPY DISK.....	51
CAPITOLO 8. CONFIGURAZIONE DELLA PROTEZIONE IN TEMPO REALE	53
8.1. Verifica dello status della protezione	53
8.2. Definizione delle azioni del programma e impostazione del livello di protezione.....	54
CAPITOLO 9. PROTEZIONE DEL COMPUTER CONTRO GLI ATTACCHI PROVENIENTI DALLA RETE	59
CAPITOLO 10. PROTEZIONE ANTIVIRUS DELLA POSTA ELETTRONICA	61
CAPITOLO 11. GESTIONE DI OGGETTI CONTAMINATI E SOSPETTI.....	63
CAPITOLO 12. RINNOVO DELLA LICENZA.....	65
CAPITOLO 13. SCARICAMENTO DEGLI AGGIORNAMENTI	67
13.1. Quando scaricare gli aggiornamenti.....	67
13.2. Scaricamento degli aggiornamenti da Internet.....	68
13.3. Scaricamento degli aggiornamenti da una cartella locale	70
13.4. Aggiornamento dei moduli di Kaspersky Anti-Virus® Personal	71
13.5. Configurazione dei parametri del server proxy	72
13.6. Impostazioni della funzione di aggiornamento Aggiornamenti programmati ..	73
13.7. Aggiornamenti manuali. Scaricamento degli aggiornamenti	74
CAPITOLO 14. IMPOSTAZIONI SUPPLEMENTARI	76
14.1. Configurazione della protezione in tempo reale.....	76
14.2. Configurazione della protezione contro gli attacchi provenienti dalla rete	79
14.3. Configurazione dei parametri di scansione manuale.....	80
14.4. Gestione degli oggetti in quarantena	82
14.5. Gestione di copie di backup di oggetti	84
14.6. Impostazioni supplementari per la quarantena e la backup	85
14.7. Uso dei report	87
14.7.1. Visualizzazione delle informazioni nei report.....	91
14.7.2. Esportazione e invio dei report.....	92
14.8. Impostazioni supplementari di Kaspersky Anti-Virus® Personal	93
APPENDICE A. COME CONTATTARE L'ASSISTENZA TECNICA	96
APPENDICE B. GLOSSARIO.....	98

APPENDICE C. KASPERSKY LAB.....	103
C.1. Altri prodotti Kaspersky Lab.....	104
C.2. Recapiti	107
APPENDICE D. CONTRATTO DI LICENZA.....	108

CAPITOLO 1. INTRODUZIONE

1.1. Virus informatici e programmi maligni

Man mano che il numero degli utenti informatici aumenta e che gli scambi di dati tramite Internet e la posta elettronica si intensificano, aumenta anche il rischio di infezione da parte dei virus informatici e della conseguente corruzione o cattura di dati da parte di programmi maligni o malware.

Per acquisire consapevolezza dei rischi potenziali del proprio computer, occorre sapere quali tipi di programmi maligni esistono e come funzionano. In generale, i programmi maligni rientrano in una delle seguenti categorie:

- **Worm** si diffondono attraverso le risorse di rete. Essi sono stati chiamati "worm", vermi, grazie alla capacità di intrufolarsi da un computer all'altro, attraverso reti, posta elettronica ed altri canali. Per questa loro capacità sono in grado di diffondersi in maniera estremamente rapida.

Essi penetrano all'interno di un computer, individuano gli indirizzi IP di altri computer e inviano loro repliche di se stessi. Inoltre utilizzano i dati contenuti nelle rubriche dei programmi di posta elettronica installati nelle macchine infette. Sono anche in grado di creare file di lavoro sui dischi ma non possono utilizzare alcuna risorsa delle macchine infette al di fuori delle risorse di RAM.

- **Virus** infettano programmi del computer aggiungendo codici che ne modificano il funzionamento al fine di ottenere il controllo non appena un file infetto viene eseguito. Questa semplice definizione evidenzia come l'azione principale di un virus consista nell'*infettare programmi informatici*. I virus si diffondono più lentamente dei worm.
- **Cavalli di Troia** eseguono operazioni non autorizzate sui computer infetti, per esempio possono cancellare dati dal disco fisso, "congelare" il sistema, trafugare informazioni confidenziali, ecc. In senso stretto, i cavalli di Troia non sono virus (cioè non infettano programmi o dati), non sono in grado di penetrare autonomamente nei computer e sono distribuiti come software "utili". Tuttavia i danni inflitti dai cavalli di Troia possono essere di gran lunga più gravi delle perdite derivanti da attacchi di virus.

Di recente i worm sono diventati il tipo di malware più diffuso, seguito dai virus e dai cavalli di Troia. Alcuni programmi maligni presentano le caratteristiche tipiche di due o perfino di tutte e tre le categorie descritte.

Sebbene i programmi maligni siano distribuiti principalmente per posta elettronica e Internet, anche floppy disk e CD possono essere veicolo di infezione. Pertanto, un'efficace protezione dai rischi potenziali non può limitarsi alla semplice scansione antivirus e deve comprendere invece la funzione ben più complessa della protezione antivirus in tempo reale.



Per semplicità, da questo momento in poi il termine "virus" sarà utilizzato indifferentemente per indicare virus, cavalli di Troia e worm. Si farà riferimento a tipi specifici di programmi maligni solo se necessario.

1.2. Gli obiettivi e le funzioni principali di Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal è progettato per garantire la protezione antivirus di personal computer con piattaforma Windows (cfr. la sezione 1.3, pag. 9).

Kaspersky Anti-Virus® Personal 5.0 svolge le seguenti funzioni:

- **Protezione contro i virus e i programmi nocivi** – individuazione ed eliminazione di malware introdotti nel computer attraverso dispositivi di memorizzazione amovibili e permanenti, posta elettronica e protocolli Internet. Il programma può essere utilizzato con le seguenti modalità (sia congiuntamente che separatamente):
 - **Protezione antivirus in tempo reale** – esegue una scansione antivirus di tutti gli oggetti eseguiti, aperti o salvati.
 - **Scansione manuale** – esegue la scansione antivirus e la disinfezione del computer o di dischi, file o cartelle sezionati. La scansione può essere lanciata manualmente o programmata a intervalli regolari.
- **Ripristino dell'operatività del computer dopo un attacco informatico** – la scansione completa del computer e l'eventuale disinfezione in base alle impostazioni raccomandate dagli esperti di Kaspersky Lab consente di eliminare alla radice qualsiasi virus che possa aver infettato i file durante un attacco.
- **Scansione e disinfezione di messaggi di posta elettronica in entrata e in uscita** – esegue la scansione antivirus e la disinfezione

in tempo reale dei messaggi di posta elettronica prima che vengano scaricati nella casella della posta in arrivo¹ e di quelli in uscita. Inoltre, il programma consente di eseguire la scansione e la disinfezione manuale dei database di posta elettronica di vari client² (cfr. il Capitolo 9, pag. 59).

- **Protezione del computer contro attacchi di rete** – analisi di tutti i dati che entrano nel computer dell'utente dalla rete (LAN o Internet) per determinare se facciano parte di un attacco noto proveniente da Internet. Se si rileva un attacco proveniente da Internet, è possibile bloccare il computer di origine dell'attacco. Inoltre, il programma consente l'azionamento in modalità invisibile quando il computer dell'utente riceve dati da altri computer solo nei casi in cui lo scambio di dati con una macchina specifica è stato iniziato dall'utente stesso.
- **Aggiornamento del database antivirus e dei moduli di programma** – l'aggiornamento del database antivirus con informazioni relative ai virus più recenti e ai relativi metodi di disinfezione degli oggetti. Gli aggiornamenti vengono scaricati dai server dedicati di Kaspersky Lab oppure copiati nel computer da una cartella locale.
- **Raccomandazioni sulle impostazioni e il funzionamento del programma** – suggerimenti degli esperti di Kaspersky Lab per agevolare l'uso di Kaspersky Anti-Virus® Personal, e impostazioni raccomandate per una protezione antivirus ottimale.

In caso di rilevamento di file infetti o dubbi, se il database antivirus è obsoleto o se il computer non è stato sottoposto a un'accurata scansione da troppo tempo, la finestra principale di Kaspersky Anti-Virus® Personal visualizzerà delle raccomandazioni per l'esecuzione di determinate azioni, con istruzioni dettagliate su come agire. Abbiamo personalizzato il programma in modo da garantire prestazioni ottimali sulla base della vasta esperienza degli esperti di Kaspersky Lab nel settore della protezione antivirus, e dei suggerimenti forniti dagli utenti stessi ai nostri tecnici dell'assistenza. Le impostazioni raccomandate della protezione antivirus vengono applicate dopo l'installazione del programma, alla prima esecuzione.

¹ Il programma controlla esclusivamente i messaggi di posta elettronica ricevuti mediante protocollo POP3 e inviati mediante protocollo SMTP.

² Kaspersky Anti-Virus® consente la scansione antivirus dei database di posta elettronica di qualsiasi programma, ma è in grado di disinfettare solo quelli di MS Outlook e MS Outlook Express.

- **Quarantena** – una speciale area di memorizzazione sicura dove isolare oggetti probabilmente infetti. È possibile decidere se disinfettare o eliminare gli oggetti in quarantena, ripristinarli nella cartella di origine o inviarli agli esperti di Kaspersky Lab per farli analizzare. I file in quarantena vengono memorizzati in un formato speciale e non costituiscono pericolo.
- **Backup** – uno speciale spazio di memorizzazione utilizzato per conservare copie di oggetti create prima della loro riparazione o rimozione. Tali copie vengono create per far fronte all'eventuale necessità di ripristinare un oggetto originale contenente informazioni preziose o per riprodurre una situazione di infezione a fini di analisi.
- **Reporting** – i risultati di tutte le azioni eseguiti da Kaspersky Anti-Virus® Personal vengono documentati in appositi report. Un report dettagliato delle scansioni eseguite contiene tutte le statistiche degli oggetti esaminati, delle impostazioni utilizzate per ogni operazione e l'elenco di tutte le attività eseguite su ogni singolo file. I report vengono generati anche sulla base dei risultati di aggiornamento.

1.3. Nuove funzioni della versione 5.0

Kaspersky Anti-Virus® Personal 5.0 presenta le seguenti funzioni non offerte dalla versione 4.5:

- *Database degli oggetti sottoposti a scansione.* La nuova versione di Kaspersky Anti-Virus® non esamina gli oggetti che non hanno subito variazioni dall'ultima modifica. Questa regola vale non solo per la protezione in tempo reale ma anche per le scansioni manuali. Si tratta di una funzione che migliora in maniera rilevante la velocità e le prestazioni del programma.
- *Kaspersky Anti-Virus® Personal 5.0 consente di effettuare la scansione e la disinfezione di messaggi di posta elettronica in entrata e in uscita per qualsiasi client che utilizza i protocolli POP3 e SMTP.* La versione precedente offriva protezione per i soli client di posta elettronica compatibili con Microsoft Exchange.
- *Disinfezione di archivi infetti.* Kaspersky Anti-Virus® Personal 5.0 disinfecta file infetti in archivi *zip*, *arj*, *cab* e *rar*. La versione precedente consentiva di rilevare e disinfettare file infetti solo in archivi *zip*.



Kaspersky Anti-Virus analizza soltanto archivi a volume multiplo dei tipi specificati nonché archivi autoestraenti, ma non è in grado di ripararli.

- *Interfaccia di facile utilizzo.* La versione 5.0 è costituita da un unico programma, mentre quella precedente consisteva di più componenti, ciascuno dei quali con una specifica funzione di protezione antivirus. Il nuovo approccio semplifica il controllo sulle più importanti funzioni del programma. Per esempio è possibile impostare il livello di protezione antivirus semplicemente spostando un cursore anziché modificando parametri.
- *Impostazioni raccomandate e suggerimenti degli esperti.* Al fine di semplificare il funzionamento del programma, le impostazioni predefinite di questa versione corrispondono alla impostazioni raccomandate dagli esperti di Kaspersky Lab. Non è più necessario configurare il programma prima dell'uso. Quando il livello di protezione antivirus è impostato sul minimo, il programma visualizza un messaggio che propone varie opzioni per passare a un livello di protezione superiore.
- *Rinnovo della licenza del prodotto.* Gli utenti di Kaspersky Anti-Virus® Personal 5.0 hanno la possibilità di installare una nuova chiave di licenza, prolungando così l'abbonamento.
- *Invio di file a Kaspersky Lab per farli analizzare.* Adesso è possibile fare analizzare i file probabilmente infetti rilevati da Kaspersky Anti-Virus® Personal 5.0 o quelli sospetti.
- *È stata rimossa la possibilità di eliminare oggetti composti infetti.* La versione corrente di Kaspersky Anti-Virus® non consente più di eliminare gli oggetti composti infetti (archivi, database di client di posta elettronica o file di posta elettronica). Tuttavia è ancora possibile eliminare tali oggetti per mezzo di strumenti Windows standard, con l'eccezione degli archivi autoestraenti.

1.4. Requisiti di sistema hardware e software

Per consentire il normale funzionamento di Kaspersky Anti-Virus® Personal 5.0, il computer deve soddisfare i seguenti requisiti:

Requisiti di carattere generale:

- Almeno 50 MB di spazio disponibile sul disco fisso

- Unità CD-ROM (per l'installazione di Kaspersky Anti-Virus® da CD)
- Microsoft Internet Explorer 5.5 (per l'aggiornamento dei database antivirus e dei moduli del programma tramite Internet)

Microsoft Windows 98:

- Processore Intel Pentium 133 MHz minimo
- Almeno 32 MB di RAM

Microsoft Windows ME:

- Processore Intel Pentium 150 MHz minimo
- Almeno 32 MB di RAM

Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Processore Intel Pentium 133 MHz minimo
- Almeno 32 MB di RAM

Microsoft Windows 2000 Professional (Service Pack 2 o successivo):

- Processore Intel Pentium 133 MHz minimo
- Almeno 64 MB di RAM

Microsoft Windows XP Home Edition o XP Professional (Service Pack 1 o successivo):

- Processore Intel Pentium 300 MHz minimo
- Almeno 128 MB di RAM

1.5. Kit di distribuzione

Kaspersky Anti-Virus® Personal può essere acquistato presso il proprio rivenditore di fiducia (confezione retail) oppure online (dal sito <http://www.kaspersky.com>, sezione **E-Store**).

La confezione retail include:

- Busta sigillata con CD di installazione contenente i file del programma.
- Manuale d'uso.
- Chiave di licenza su disco a parte.
- Contratto di licenza



Prima di aprire la busta contenente il CD (o i floppy disk) è necessario aver letto attentamente il contratto di licenza.

Nel caso di acquisto online di Kaspersky Anti-Virus® Personal online, è necessario scaricare il file di installazione del prodotto dal sito web di Kaspersky Lab. In questo caso il kit di distribuzione include questo Manuale d'uso con il programma. La chiave di licenza sarà inviata per posta elettronica non appena sarà stato confermato il pagamento.

Il Contratto di licenza è un accordo con valore legale fra l'utente finale e Kaspersky Lab., volto a regolamentare le condizioni di utilizzo del prodotto antivirus acquistato.

Si raccomanda di leggere attentamente il Contratto di licenza!

Qualora l'utente non concordi con i termini e le condizioni del Contratto di licenza, potrà restituire la confezione retail al rivenditore Kaspersky Anti-Virus® presso il quale è stato acquistato il prodotto, e ottenere il rimborso dell'importo pagato per l'iscrizione, a condizione che la busta contenente il CD (o i floppy disk) non sia stata dissigillata.

L'apertura della busta sigillata del CD di installazione (o floppy disk), comporta l'accettazione dei termini e delle condizioni del Contratto di licenza da parte dell'acquirente.

1.6. Servizi riservati agli utenti registrati

Kaspersky Lab. offre a tutti gli utenti registrati dei propri prodotti un pacchetto completo di servizi volti a potenziarne l'efficienza durante l'uso di Kaspersky Anti-Virus®.

Con l'acquisto di un'iscrizione, l'acquirente diventa utente registrato del programma e ottiene il diritto per l'intero periodo di iscrizione a ricevere i seguenti servizi:

- aggiornamenti del programma;
- assistenza relativa all'installazione, configurazione e uso del prodotto; i servizi saranno erogati per telefono o per posta elettronica;
- Informazioni sull'uscita di nuovi prodotti Kaspersky Lab e sui nuovi virus informatici diffusi in tutto il mondo (per gli utenti abbonati alla newsletter di Kaspersky Lab).



Kaspersky Lab non fornisce assistenza relativa alle prestazioni e all'uso dei sistemi operativi o di altre tecnologie.

CAPITOLO 2. INSTALLAZIONE DEL PROGRAMMA SUL COMPUTER

Per installare Kaspersky Anti-Virus® Personal sul computer, eseguire il file kavsetup.exe dal CD di installazione.

Il programma di installazione guidata funziona in maniera interattiva. Ogni finestra di dialogo presenta i seguenti pulsanti che possono essere utilizzati per interagire con il processo di installazione:

- **Avanti>** – conferma e passa alla fase successiva dell'installazione.
- **<Indietro** – torna alla fase precedente del processo di installazione.
- **Annulla** – annulla l'installazione del programma.
- **Fine** – conclude l'installazione del programma.

La sezione che segue contiene una descrizione dettagliata di ogni fase del processo di installazione.

Fase 1. Verifica della versione del sistema operativo installato sul computer

Prima di installare il programma, il sistema operativo del computer e i relativi Service Pack saranno controllati per verificare la conformità ai requisiti di sistema necessari per l'installazione di Kaspersky Anti-Virus® Personal.

Qualora il programma dovesse rilevare la necessità di un Service Pack, verrà visualizzato un apposito messaggio. Installare il Service Pack necessario servendosi della funzione **Windows Update** e ripetere l'installazione di Kaspersky Anti-Virus® Personal.

Fase 2. Ricerca di altri software antivirus



Questa fase del processo di installazione è necessaria solo nel caso in cui sul computer siano installati altri programmi antivirus.

La fase successiva di preparazione all'installazione del programma prevede una ricerca volta a individuare la presenza di altri programmi antivirus sul computer

(compresi altri programmi Kaspersky Lab). Questa fase è necessaria perché l'uso simultaneo di questi programmi con Kaspersky Anti-Virus® Personal può essere causa di conflitti.

In presenza di una versione precedente di Kaspersky Anti-Virus (per esempio la versione 4.5), il sistema chiede all'utente se desidera mantenere la chiave di licenza di tale prodotto, se ancora valida.



Si raccomanda di conservare la chiave di licenza valida utilizzata in precedenza, in quanto utilizzabile anche con Kaspersky Anti-Virus Personal 5.0.

Dopo aver salvato la chiave, il sistema invita l'utente a disinstallare la versione precedente del prodotto perché in conflitto con Kaspersky Anti-Virus Personal 5.0.

Fare clic sul pulsante **OK** e disinstallare la versione precedente di Kaspersky Anti-Virus®, quindi eseguire *kavsetup.exe*.

In presenza di software antivirus di altri produttori installato sul computer, viene visualizzato un messaggio con la raccomandazione di disinstallare il programma prima di installare Kaspersky Anti-Virus® Personal.

In questo caso si raccomanda di annullare il processo di installazione e provvedere prima alla disinstallazione di tali programmi. Fare clic sul pulsante **No**, disinstallare i programmi ed eseguire *kavsetup.exe*.

Se il programma rileva una precedente installazione di Kaspersky Anti-Virus® Personal sullo stesso computer, viene visualizzato un messaggio che avverte che la versione precedentemente installata sarà sovrascritta dal programma che ci si accinge a installare.

Fase 3. Avvio del programma di installazione guidata

Se nel computer non viene rilevato alcun altro software antivirus, subito dopo l'esecuzione di *kavsetup.exe* viene visualizzata una finestra di dialogo che informa che l'installazione di Kaspersky Anti-Virus® Personal è iniziata.

Per procedere con l'installazione fare clic su **Avanti>**. Per annullare l'installazione fare clic su **Annulla**.

Fase 4. Lettura del contratto di licenza

La finestra di dialogo successiva contiene un Contratto di licenza tra l'acquirente e Kaspersky Lab. Leggerlo attentamente e fare clic su **Accetto** se si concorda con tutti i termini e le condizioni del contratto. L'installazione prosegue.

Fase 5. Informazioni sull'utente

In questa fase vengono registrati il nome dell'utente e della sua azienda. Le informazioni predefinite vengono copiate dal registro del sistema operativo e, se lo si desidera, possono essere modificate.

Per procedere con l'installazione fare clic su **Avanti>**.

Fase 6. Lettura delle informazioni importanti sul programma

In questa fase del processo di installazione, si richiede all'utente di leggere delle informazioni importanti sul prodotto prima di iniziare a usarlo.

Questa finestra di dialogo contiene informazioni sulle caratteristiche e le funzionalità principali di Kaspersky Anti-Virus® Personal.

Da qui è possibile inoltre determinare se si desidera utilizzare Kaspersky Anti-Virus nella modalità di prestazione massima garantita dall'uso delle nuove tecnologie Kaspersky Lab.

Per impostazione predefinita, questa modalità è abilitata. Per disabilitarla, deselezionare la casella **Usa le impostazioni raccomandate**.

Per procedere con la fase successiva del processo di installazione, fare clic su **Avanti>**.

Fase 7. Uso della tecnologia iStreams™



Questa fase è necessaria solo se durante la fase precedente la casella **Usa le impostazioni raccomandate** era stata deselezionata.

In questa fase dell'installazione di Kaspersky Anti-Virus è necessario decidere se si desidera utilizzare la tecnologia iStreams™ per la scansione antivirus.

L'uso di questa tecnologia accelera considerevolmente il processo di scansione senza caricare ulteriormente il sistema.

Per disabilitare l'uso di questa tecnologia, deselezionare la casella **Usa la tecnologia iStreams™**.

Per procedere con l'installazione fare clic su **Avanti>**.

Fase 8. Installazione della chiave di licenza



Eeguire questa fase solo se il programma di installazione guidata di Kaspersky Anti-Virus® Personal non riesce a individuare il file chiave automaticamente!

Durante questa fase viene installata la chiave di licenza di Kaspersky Anti-Virus® Personal. Si tratta della "chiave" personale che memorizza tutte le informazioni necessarie per consentire un funzionamento completo e regolare di Kaspersky Anti-Virus® Personal, e cioè:

- Informazioni relative all'assistenza tecnica (fornitore dei servizi di assistenza e indirizzo).
- Nome, numero e data di scadenza della licenza.



Senza chiave di licenza il programma non funziona.

Inserire la chiave di licenza in una finestra di dialogo **Seleziona file standard** e fare clic su **Avanti>** per proseguire il processo di installazione.

Se non si è in possesso della chiave di licenza al momento dell'installazione (per esempio se si è acquistato il prodotto su Internet ma non lo si è ancora ricevuto), è possibile installarla in seguito al momento del primo utilizzo. Non è possibile iniziare a usare Kaspersky Anti-Virus® senza la chiave di licenza.

Fase 9. Selezione della cartella di installazione

In questa fase del processo di installazione di Kaspersky Anti-Virus® viene selezionata la cartella di destinazione del prodotto. Il percorso predefinito è: **...Programmi\Kaspersky Lab\Kaspersky Anti-Virus Personal**.

Per modificare il percorso predefinito fare clic sul pulsante **Sfogli...** nella finestra di dialogo, specificare una nuova cartella di installazione e fare clic su **Avanti>**.

Dopodiché i file di programma di Kaspersky Anti-Virus® vengono copiati sul computer.

Fase 10. Completamento dell'installazione

La finestra di dialogo **Installazione guidata completata** informa che l'installazione di Kaspersky Anti-Virus® Personal sul computer è avvenuta con successo.

Se occorre registrare i servizi, è necessario riavviare il computer. Questa fase è **OBBLIGATORIA** al fine di completare correttamente l'installazione del programma.



Per completare l'installazione:

1. Scegliere una delle seguenti opzioni:
 - Sì, riavviare il computer adesso**
 - No, riavviare il computer in seguito**
2. Fare clic su **Fine**.



Se non è necessario riavviare il computer, eseguire le seguenti fasi per completare l'installazione del programma:

1. Deselezionare la casella **Start Kaspersky Anti-Virus Personal 5.0**, se non si desidera attivare la protezione antivirus del computer subito dopo l'installazione del prodotto.



Se si deselectiona questa casella, la protezione antivirus del computer sarà attivata automaticamente solo dopo il riavvio. È possibile attivare manualmente la protezione antivirus dal menu principale di Windows (**Avvio → Programmi → Kaspersky Anti-Virus Personal**).

2. Fare clic sul pulsante **Fine**.

CAPITOLO 3. IN CASO DI INFEZIONE DEL COMPUTER...

A volta neanche gli utenti più esperti si accorgono che il computer è stato infettato da un virus, perché questi tipi di file si mimetizzano con grande efficienza tra gli altri file. Questo capitolo contiene una descrizione dettagliata dei sintomi di infezione da virus, dei metodi di recupero dati dopo un attacco e delle misure preventive volte ad impedire la corruzione dei dati da parte di programmi nocivi.

3.1. Sintomi di infezione

Esistono vari sintomi che indicano che il computer è infetto. Si tratta per lo più di "strani eventi" come per esempio:

- la visualizzazione inaspettata di messaggi o immagini;
- suoni insoliti o musica eseguita casualmente;
- l'unità del CD-ROM si apre e chiude da sola;
- l'avvio imprevisto di programmi;
- Se sul computer è installato Kaspersky Anti-Hacker, vengono visualizzati avvisi di tentativi di connessione a Internet da parte di alcune applicazioni, non sollecitati dall'utente.

In caso di comparsa di uno o più dei sintomi menzionati, è molto probabile che il computer sia stato colpito da un virus.

Vi sono inoltre alcuni sintomi tipici che indicano che il computer è stato infettato tramite la posta elettronica:

- i vostri conoscenti riferiscono di aver ricevuto messaggi che voi non avete mai spedito;
- la casella della posta elettronica contiene numerosi messaggi privi di intestazione o di mittente.

Osservare tuttavia che questi problemi possono avere anche cause estranee a un'infezione da virus. Per esempio, messaggi infetti apparentemente inviati da

un indirizzo di posta elettronica possono in effetti essere stati inviati da un computer diverso.

Vi sono anche sintomi indiretti che indicano una probabile infezione del computer:

- il computer si blocca frequentemente o provoca errori;
- il computer rallenta notevolmente quando vengono avviati dei programmi;
- non si riesce a caricare il sistema operativo;
- all'improvviso si osserva la scomparsa di file e cartelle, o la variazione del loro contenuto;
- si osserva un numero eccessivo di accessi al disco fisso (la spia dell'unità principale lampeggia rapidamente);
- Microsoft Internet Explorer si blocca o reagisce in maniera imprevista (per esempio non consente di chiudere la finestra dell'applicazione).

Il 90% di tali sintomi indiretti indica un problema di hardware o software ma, sebbene la presenza di un'infezione sia improbabile, in presenza di problemi simili si raccomanda di eseguire ugualmente una scansione completa del computer applicando le impostazioni predefinite raccomandate dagli esperti di Kaspersky Lab.

3.2. Cosa fare in presenza di sintomi di infezione



Se si riscontrano comportamenti "sospetti" da parte del computer:

1. Evitare il panico! Questa regola preziosa può prevenire la perdita di dati importanti memorizzati nel computer ed evitare un carico non necessario di stress.
2. Disconnettere il computer da Internet.
3. Se il computer è collegato a una Local Area Network, disconnetterlo.
4. Se il sintomo riscontrato consiste nell'impossibilità di effettuare il boot dal disco fisso (errore di startup del computer), provare ad avviare la macchina in modalità provvisoria o dal disco di boot di Windows creato durante l'installazione del sistema operativo.
5. Prima di qualsiasi contromisura, eseguire il backup di tutti i dati importanti su un'unità esterna (floppy disk, CD, flash card, ecc.)


6. Se non si è ancora installato Kaspersky Anti-Virus® Personal, è giunto il momento di farlo.
7. Scaricare gli ultimi aggiornamenti del database antivirus. Se possibile, non utilizzare il computer infetto per scaricare gli aggiornamenti ma servirsi di quello di un amico o di un computer in ufficio o presso un Internet café, ecc. Ciò è molto importante perché se si è connessi a Internet, è possibile che il virus invii informazioni importanti all'aggressore o repliche di se stesso agli indirizzi di posta elettronica presenti nella rubrica. Pertanto, se si sospetta che il computer sia infetto, è consigliabile disconnetterlo immediatamente da Internet. È possibile inoltre richiedere il database antivirus su CD-ROM o floppy disk direttamente a Kaspersky Lab o a un rivenditore autorizzato, e aggiornare così i propri database (per ulteriori informazioni consultare la sezione 13.3, pag. 70).
8. Applicare le impostazioni raccomandate dagli esperti di Kaspersky Lab (cfr. la sezione 6.2, pag. 38).
9. Eseguire una scansione completa del sistema (cfr. la sezione 6.3, pag. 43).

CAPITOLO 4. PROTEZIONE ANTIVIRUS CON LE IMPOSTAZIONI PREDEFINITE DI KASPERSKY® AV PERSONAL

Kaspersky Anti-Virus® Personal può essere utilizzato subito dopo l'installazione. Non è infatti necessario personalizzare il programma prima di utilizzarlo per la prima volta poiché tutti i parametri importanti necessari per un funzionamento efficiente di Kaspersky Anti-Virus® Personal sono preimpostati in base alle raccomandazioni degli esperti di Kaspersky Lab. Il livello di protezione antivirus offre un equilibrio ottimale tra l'efficienza della protezione e le prestazioni del computer.

Le pagine che seguono contengono una descrizione dettagliata del funzionamento di Kaspersky Anti-Virus® Personal con le impostazioni raccomandate dai nostri esperti.

4.1. Protezione in tempo reale

Subito dopo l'avvio (indicato dall'icona rossa  nella barra delle applicazioni), Kaspersky Anti-Virus® Personal esamina *tutti gli oggetti eseguiti dal sistema operativo all'avvio*, nonché la *memoria del computer e i moduli dei programmi*.

La protezione in tempo reale del computer viene attuata utilizzando le impostazioni raccomandate dagli esperti di Kaspersky Lab con le seguenti modalità:

- Gli oggetti aperti, salvati o eseguiti sul disco fisso e sulle unità rimovibili e *potenzialmente infetti* vengono sottoposti a scansione. Tra questi:
 - *i settori di boot del disco (esaminati immediatamente dopo l'avvio del sistema);*

- *i file compressi e gli oggetti collegati a file o incorporati in essi (oggetti OLE);*
- *messaggi di posta elettronica in arrivo (al momento della ricezione).*




La protezione in tempo reale non include la scansione di oggetti che non possono contenere virus.



- Quando viene individuato un *oggetto infetto*, il programma vi impedisce l'accesso e richiede l'intervento dell'utente.
- Quando viene individuato un oggetto *probabilmente infetto da un virus o da una sua variante*, il programma vi impedisce l'accesso e richiede l'intervento dell'utente.
- Quando viene rilevato un attacco da Internet, il programma blocca l'attacco e il computer da cui esso proviene.
- I risultati di tutte le azioni del programma sono documentati in appositi report (cfr. la sezione 14.7, pag. 86).

La protezione antivirus in tempo reale viene attivata automaticamente dopo l'avvio del sistema e rimane attiva fino allo spegnimento.



È possibile disattivare manualmente la protezione in tempo reale agendo come segue:

- Fare clic con il pulsante destro del mouse sull'icona  nella barra delle applicazioni.
- All'apertura del menu di scelta rapida, selezionare **Disattiva Protezione in tempo reale**.

La protezione in tempo reale del computer viene disabilitata e l'icona rossa  diventa inattiva  (colore grigio).



La disattivazione della protezione antivirus in tempo reale aumenta considerevolmente il rischio di infezioni, pertanto si consiglia di mantenere sempre attiva la funzione.

4.2. Scansione manuale

La funzione di **scansione manuale** consente di effettuare la scansione antivirus integrale del computer oppure di dischi, cartelle o file specifici. Di seguito sono

elencate le impostazioni di scansione predefinite raccomandate dagli esperti di Kaspersky Lab:

- la scansione manuale dell'intero sistema prevede anche l'esame di tutti gli oggetti memorizzati sui dischi fissi, tra cui:
 - i file di avvio e i settori di boot del disco;
 - gli archivi, i file eseguibili compressi e gli archivi autoestraenti;
 - gli oggetti collegati a file o incorporati in essi (*oggetti OLE*);
 - la RAM utilizzata dai processi in esecuzione;
- la scansione antivirus di dischi, cartelle o file specifici prevede l'analisi di tutti i file memorizzati nell'area selezionata, tra cui:
 - *gli archivi, i file eseguibili compressi e gli archivi autoestraenti*;
 - gli oggetti collegati a file o incorporati in essi (*oggetti OLE*);
- richiesta di intervento da parte dell'utente quando viene rilevato un *oggetto infetto*;
- richiesta di intervento da parte dell'utente quando viene individuato un oggetto *probabilmente infetto da un virus o da una sua variante*;
- documentazione dei risultati di tutte le azioni del programma in appositi report (cfr. la sezione 14.7, pag. 86).

Per impostazione predefinita, ogni venerdì alle 20:00 è prevista una scansione manuale completa del computer. L'indicatore di status della scansione completa (cfr. la Figura 3) è ubicato nella sezione destra della scheda **Protezione**.




La scansione completa del computer è in corso

Se il computer viene spento prima delle 20:00 la scansione non viene effettuata.



È possibile avviare manualmente una scansione completa del computer agendo come segue:

Fare clic con il pulsante destro del mouse sull'icona  nella barra delle applicazioni. All'apertura del menu di scelta rapida, selezionare **Cerca virus nel computer**.

oppure

aprire la scheda **Protezione** nella finestra dell'applicazione e fare clic su [Esamina Risorse del computer](#) nella sezione a sinistra.

4.3. Aggiornamento dei database antivirus


Il programma rileva virus e ripara gli oggetti infetti basandosi sui registri del database antivirus contenente le definizioni di tutti i programmi nocivi noti e dei relativi metodi di riparazione degli oggetti infetti.

È estremamente importante aggiornare regolarmente il database antivirus poiché ogni giorno compaiono nuovi virus.

L'aggiornamento del database antivirus è un'altra importante funzione di Kaspersky Anti-Virus® Personal. Per impostazione predefinita, il database viene automaticamente scaricato da uno dei server di aggiornamento di Kaspersky Lab e installato ogni 3 ore. Se il computer viene utilizzato per meno di tre ore al giorno, si raccomanda di modificare la frequenza di aggiornamento del database antivirus, di lasciare il computer acceso o di aggiornare il database manualmente. In caso contrario sarà impossibile aggiornare il database antivirus.



È possibile aggiornare il database manualmente agendo come segue:

Fare clic con il pulsante destro del mouse sull'icona  nella barra delle applicazioni. All'apertura del menu di scelta rapida, selezionare **Aggiorna database antivirus**.

oppure

aprire la scheda **Protezione** (cfr. la Figura 3) della finestra principale dell'applicazione e fare clic sul collegamento [Aggiorna adesso](#) nella sezione a sinistra.

oppure

fare clic sul collegamento [Aggiorna database antivirus](#) nella sezione a destra della scheda **Protezione**.





Per ulteriori informazioni sull'aggiornamento del database antivirus cfr. il Capitolo 13, pag. 67.




CAPITOLO 5. INTERFACCIA DEL PROGRAMMA

Kaspersky Anti-Virus® Personal è caratterizzato da un'interfaccia semplice e facile da usare. Questo capitolo presenta una descrizione dei principali elementi dell'interfaccia: l'icona della barra delle applicazioni, il menu di scelta rapida, la finestra principale dell'applicazione e alcune delle finestre dei servizi.

5.1. L'icona della barra delle applicazioni

Dopo l'avvio del programma, la barra delle applicazioni di Windows visualizza un'icona che indica lo status della protezione antivirus.

Se la protezione antivirus in tempo reale è abilitata, l'icona appare di colore rosso (status attivo) ; se la protezione in tempo reale è disabilitata, l'icona diventa grigia (inattiva) , anche se la scansione antivirus della posta e degli script è abilitata.

Quando il programma analizza il computer o un disco o file specifico, oppure quando sta analizzando un oggetto in modalità di protezione in tempo reale, l'icona si trova sopra a una cartella di colore bianco e blu intermittente:  / . Durante la scansione della posta elettronica, in luogo della cartella viene visualizzata una busta. Durante lo scaricamento degli aggiornamenti viene visualizzata l'icona .

Quando si verifica un evento importante relativo alla sicurezza antivirus del computer, sopra l'icona viene visualizzata temporaneamente una raccomandazione da parte degli esperti di Kaspersky Lab (cfr. la Figura 1).

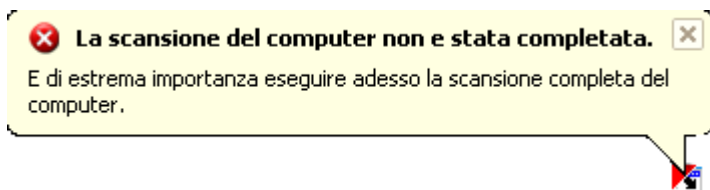



Figura 1. Messaggio

5.2. Il menu di scelta rapida

Per aprire un menu di scelta rapida, fare clic con il pulsante destro del mouse sull'icona dell'applicazione nella barra delle applicazioni (cfr. la Figura 2). Il menu si compone dei seguenti elementi:

- **Apri Kaspersky Anti-Virus** – apre la finestra principale dell'applicazione con la scheda **Protezione** attiva. È possibile aprire la finestra principale anche facendo doppio clic sull'icona  nella barra delle applicazioni.
- **Cerca virus nel computer** – esegue una scansione completa del computer in base al livello di protezione antivirus selezionato.
- **Aggiorna database antivirus** – aggiorna il database antivirus da un server di aggiornamento di Kaspersky Lab.
- **Attiva/Disattiva Protezione in tempo reale** – attiva o disattiva la protezione in tempo reale del computer. L'icona dell'applicazione nella barra delle applicazioni cambia colore in base allo status della protezione in tempo reale.



La disattivazione della protezione antivirus in tempo reale aumenta considerevolmente il rischio di infezioni, pertanto si consiglia di mantenere sempre attiva la funzione.

- **Informazioni** – visualizza informazioni di carattere generale su Kaspersky Anti-Virus® Personal.
- **Esci** – chiude Kaspersky Anti-Virus® Personal e lo scarica dalla memoria del computer.



Non è possibile accedere all'opzione **Esci** nel menu di scelta rapida se non si dispone dei diritti di amministratore per il computer.

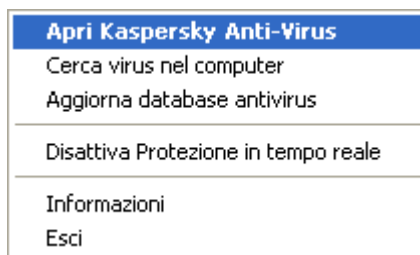


Figura 2. Il menu di scelta rapida

5.3. La finestra principale dell'applicazione: struttura generale

La finestra principale dell'applicazione di Kaspersky Anti-Virus® Personal è progettata in modo da consentire uno sfruttamento ottimale di tutte le funzionalità di protezione antivirus offerte dal programma. Dalla finestra principale dell'applicazione è possibile attivare le seguenti funzioni:

- configurazione delle impostazioni di protezione antivirus;
- avvio e arresto della scansione integrale del sistema o di dischi, cartelle o file specifici per escludere la presenza di virus o di altri programmi dannosi;
- scaricamento del database antivirus e degli aggiornamenti dei moduli del programma;
- programmazione delle scansioni complete e degli aggiornamenti;
- gestione degli oggetti in quarantena;
- gestione di report, ecc.

Tutte le impostazioni della protezione antivirus con le informazioni richieste e le attività specifiche sono accessibili dalle seguenti schede nella finestra principale:

- **Scheda Protezione** – una scheda della finestra principale dell'applicazione che visualizza le attività antivirus e il rispettivo status. Questa scheda è il principale componente dell'interfaccia del programma (cfr. la sezione 5.3.1, pag. 28).
- **Scheda Impostazioni** – una scheda della finestra principale dell'applicazione che visualizza le attività utilizzate per definire le impostazioni della protezione antivirus e il rispettivo status (cfr. la sezione 5.3.2, pag. 29).
- **Scheda Assistenza** – una scheda che visualizza le informazioni necessarie per contattare Kaspersky Lab in caso di domande o di necessità di assistenza (cfr. la sezione 5.3.3, pag. 31).

Ogni scheda si compone di due sezioni:

- *La sezione a sinistra* visualizza i collegamenti utilizzati per il controllo delle prestazioni della protezione antivirus. Ogni scheda contiene un elenco di attività specifiche.

Per esempio, la scheda **Protezione** consente di scegliere tra una serie di attività relative alla scansione antivirus. La scheda **Impostazioni** contiene comandi necessari per regolare le impostazioni di tali attività. La scheda **Assistenza** contiene comandi relativi all'assistenza per la protezione antivirus.

- *La sezione a destra* contiene informazioni sullo status corrente della protezione antivirus del computer, inclusi la protezione in tempo reale e la scansione manuale, nonché informazioni relative al database antivirus e alla licenza.

Così, per esempio, la scheda **Protezione** visualizza lo status della protezione antivirus, la scheda **Impostazioni** visualizza lo status delle impostazioni correnti del programma e la scheda **Assistenza** visualizza lo status della licenza (informazioni sulla chiave), le informazioni necessarie per contattare il personale di assistenza e quelle sul programma il sistema in uso.

Nelle schede **Protezione** e **Impostazioni** sono visualizzati tre stati di protezione antivirus, indicati dalle seguenti icone:



Livello di protezione antivirus critico. Questo status significa che la protezione in tempo reale è disattivata o che determinate attività (scansione e/o aggiornamento) non vengono eseguite da molto tempo, o che le impostazioni correnti non forniscono una protezione antivirus affidabile del computer.



Il livello di protezione in tempo reale non corrisponde alle impostazioni raccomandate. Questo status indica che le impostazioni di protezione antivirus correnti non corrispondono a quelle raccomandate dagli esperti di Kaspersky Lab o che è necessario eseguire una determinata attività di protezione antivirus.



Il livello di protezione antivirus impostato è quello raccomandato. Questo status indica che le impostazioni correnti sono perfettamente compatibili con quelle raccomandate dagli esperti di Kaspersky Lab.

Le informazioni relative allo status sono visualizzate nel seguente ordine: innanzitutto lo status della protezione in tempo reale, seguito da quello della scansione manuale e infine quello della validità del database antivirus.

Ciascuno degli stati sopra descritti è accompagnato da commenti e raccomandazioni. Così, per esempio, se il livello corrente di protezione antivirus non corrisponde a quello raccomandato, il programma offre l'opportunità di ripristinare le impostazioni raccomandate in modo da garantire un livello di protezione ottimale.

5.3.1. Scheda *Protezione*

Tramite la scheda **Protezione** (cfr. Figura 3) è possibile eseguire la scansione integrale del computer o di dischi, cartelle o file specifici. È inoltre possibile:

- lanciare l'aggiornamento del database antivirus, dei moduli dell'applicazione e del database degli attacchi di rete;
- visualizzare i report di avanzamento di tutte le operazioni in corso (visualizzazione, eliminazione, esportazione su file, ecc.)
- passare alla gestione degli oggetti in quarantena perché probabilmente infetti da virus o varianti di virus.
- passare alla gestione delle copie di backup di oggetti riparati o eliminati.

Per avviare le attività è possibile fare clic sugli ipertesti corrispondenti nella sezione sinistra della scheda.

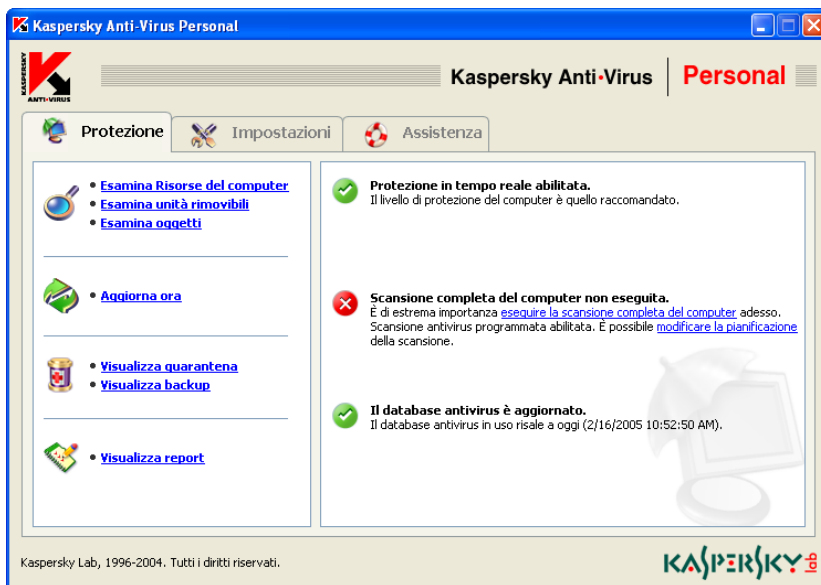


Figura 3. Scheda Protezione

Nella sezione destra della scheda è indicato lo *status corrente della protezione in tempo reale, della scansione manuale e del database antivirus*. L'esempio illustrato (cfr. la Figura 3) indica che la protezione in tempo reale è abilitata ma che la scansione completa non viene eseguita da lungo tempo. In questa stessa

finestra sono indicati inoltre i commenti sullo status di ogni attività di protezione antivirus.

Se lo status della protezione è critico o non corrispondente alle impostazioni raccomandate, il programma visualizza le *raccomandazioni degli esperti di Kaspersky Lab*. È così possibile modificare le impostazioni correnti, ripristinare quelle raccomandate, avviare una determinata attività, ecc. Tali raccomandazioni sono organizzate come ipertesti, agevolando la selezione dell'azione raccomandata.

5.3.2. Scheda *Impostazioni*

La scheda **Impostazioni** (cfr. la Figura 4) consente di valutare e personalizzare sia le impostazioni standard sia quelle avanzate, in modo da ottimizzare il funzionamento di Kaspersky Anti-Virus® Personal.

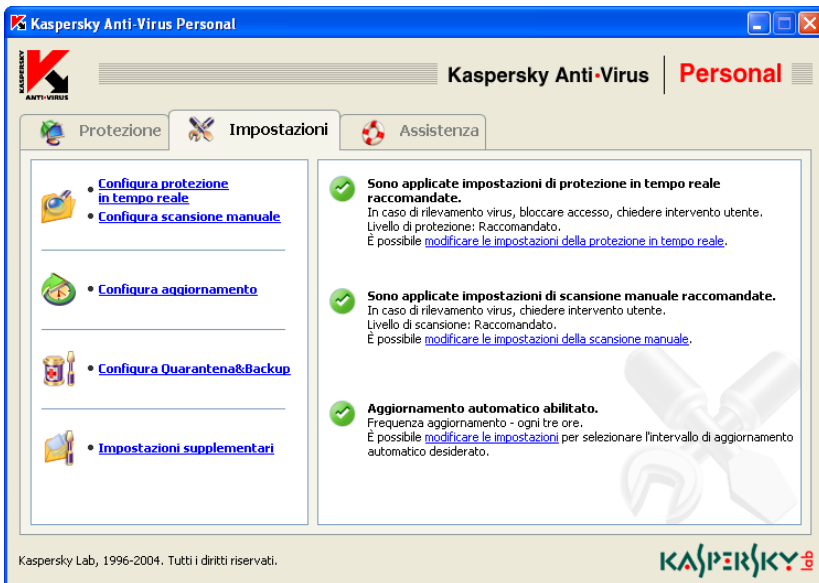


Figura 4. La scheda **Impostazioni**

La sezione destra della scheda visualizza le impostazioni correnti di protezione antivirus in tempo reale, scansione manuale e aggiornamento automatico del database antivirus, dei moduli dell'applicazione e del database degli attacchi di rete noti, oltre a commenti dettagliati e suggerimenti da parte degli esperti di Kaspersky sulla personalizzazione di alcune impostazioni. Per esempio, se in

passato il database antivirus era stato aggiornato manualmente, il programma suggerirà di impostare aggiornamenti automatici programmati.

Facendo clic sui collegamenti ubicati nella sezione sinistra della scheda **Impostazioni**, è possibile accedere a strumenti che consentono di impostare e modificare i parametri della protezione in tempo reale, della scansione manuale e dell'aggiornamento del database antivirus.

Da questa scheda è inoltre possibile personalizzare i parametri della quarantena, dove sono memorizzati gli oggetti probabilmente infetti da virus o varianti di virus, oltre ai parametri della backup utilizzata per conservare le copie di riserva degli oggetti. È inoltre possibile accedere a uno strumento che consente di personalizzare ulteriori impostazioni seguendo il collegamento [Impostazioni supplementari](#).

5.3.3. Scheda Assistenza

La scheda **Assistenza** (cfr. la Figura 5) contiene informazioni sul servizio di assistenza tecnica e su chi contattare in caso di problemi di funzionamento del programma che non sia possibile risolvere autonomamente. Contiene inoltre le informazioni sul programma, la chiave di licenza e il sistema operativo installato sul computer, da comunicare se necessario al servizio di assistenza tecnica di Kaspersky Lab. Tutte queste informazioni sono indicate nella sezione destra della scheda.

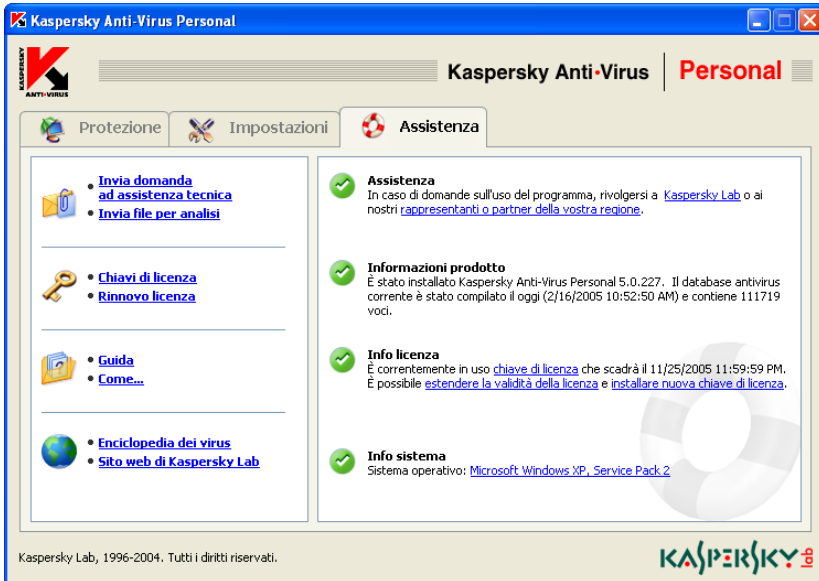


Figura 5. La scheda **Assistenza**

I collegamenti presenti nella sezione sinistra della scheda consentono di:

- inviare domande e oggetti probabilmente infetti da virus o varianti di virus al servizio di assistenza tecnica di Kaspersky Lab;
- rinnovare la licenza di Kaspersky Anti-Virus Personal.

La sezione sinistra della scheda contiene inoltre i seguenti collegamenti di riferimento:

- [Guida](#) – riferimento per l'esecuzione di attività e l'individuazione di problemi.
- [Come...](#) – riferimento all'uso generale del programma.
- [Enciclopedia dei virus](#) – collegamento al sito web www.viruslist.com contenente descrizioni dettagliate di tutti i programmi dannosi attualmente noti.
- [Sito web di Kaspersky Lab](#) – collegamento al sito web del produttore, Kaspersky Lab.

5.4. La finestra Scansione

All'avvio della scansione antivirus del computer o di dischi, cartelle o file specifici si apre la finestra Scansione (cfr. la Figura 6).

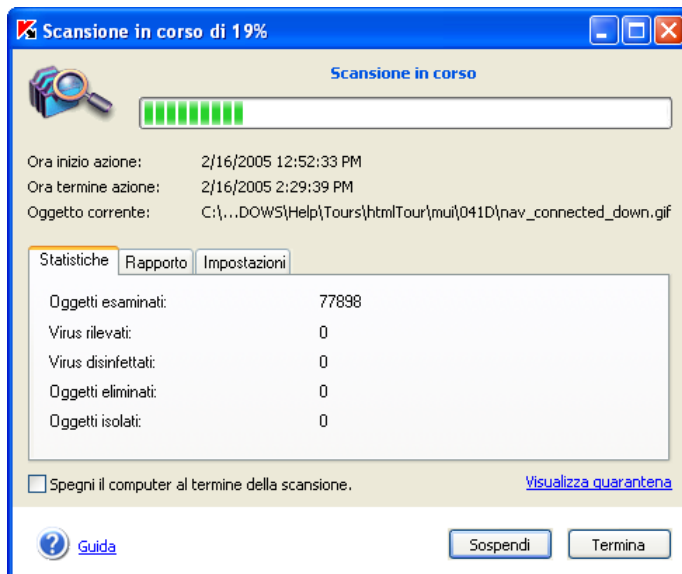


Figura 6. La finestra **Scansione**

La finestra si compone di due parti:

- Nella parte superiore della finestra è visualizzata una barra di progressione della scansione, che indica la percentuale di scansione eseguita, il tempo residuo previsto e il nome dell'oggetto in fase di scansione.
- Nella parte inferiore della finestra principale sono visualizzate tre schede: **Statistiche**, che indica i risultati della scansione; **Rapporto**, contenente un elenco degli eventi verificatisi durante la scansione; e **Impostazioni**, contenente un elenco delle impostazioni utilizzate per la scansione corrente o per l'ultima eseguita.



Per ulteriori informazioni sui report cfr. la sezione 14.7, pag. 86.

Da questa finestra è possibile abilitare lo spegnimento automatico del computer al termine della scansione. Questa modalità è utile per avviare la scansione del

computer al termine della giornata lavorativa senza dover attendere il termine della scansione per spegnere manualmente il computer.

Questa modalità richiede tuttavia alcuni preparativi: prima di lanciare la scansione è necessario disabilitare la richiesta di password per la scansione di oggetti (cfr. paragrafo 14.3, pag. 80), e configurare la modalità di elaborazione automatica per gli oggetti infetti/probabilmente infetti o l'eliminazione/isolamento automatici (cfr. paragrafo 6.2, pag. 38). Queste operazioni disabilitano la modalità interattiva e il programma non richiederà più interventi dell'utente che interrompono il processo di scansione.

Per spegnere automaticamente il computer al termine della scansione, selezionare la casella corrispondente nella finestra di scansione.

5.5. Sistema di riferimento del programma

Dalla scheda **Assistenza** della finestra principale dell'applicazione si può accedere a un esauriente sistema di riferimento seguendo semplicemente il collegamento [Come...](#) nella sezione sinistra della scheda.

In caso di necessità di ulteriori informazioni su come eseguire un'attività specifica, seguire il collegamento [Guida](#) nella finestra principale di Kaspersky Anti-Virus® Personal. La [Guida](#) contiene una descrizione dettagliata delle principali attività di protezione antivirus eseguite da Kaspersky Anti-Virus® Personal nonché le risposte alle domande più frequenti (FAQ).

In caso di domande su una finestra di dialogo specifica, premere il tasto **<F1>** oppure fare clic su [Guida](#) nell'angolo inferiore sinistro della finestra di dialogo in questione.

CAPITOLO 6. PREVENZIONE DELLE INFEZIONI DA VIRUS

Neppure le più affidabili e collaudate misure preventive sono in grado di garantire una protezione assoluta contro i virus informatici e i cavalli di Troia, ma è possibile ridurre in maniera considerevole il rischio di danni dovuti a un attacco, e quindi le perdite dovute a una possibile infezione, stabilendo e applicando determinate regole.

Analogamente a quanto avviene per la nostra salute fisica, uno dei metodi principali per combattere la diffusione dei virus è la *prevenzione* delle infezioni. Nel caso dei computer, la prevenzione di un'infezione da virus comporta l'applicazione di poche regole che, se rispettate, riducono il rischio di contagio e di perdita dei dati.

Di seguito sono elencate le principali regole di sicurezza da seguire per prevenire gli attacchi dei virus.

Regola 1: proteggere il computer installando programmi antivirus e software per la sicurezza della navigazione in Internet. A questo proposito:

- Installare Kaspersky Anti-Virus® Personal
- Aggiornare quotidianamente il database antivirus. Nei periodi di maggior diffusione dei virus è possibile scaricare gli aggiornamenti più volte al giorno perché quando il rischio è maggiore i server dedicati di Kaspersky Lab vengono costantemente aggiornati.
- Applicare le impostazioni di protezione in tempo reale raccomandate dagli esperti di Kaspersky Lab. La protezione antivirus in tempo reale viene attivata immediatamente all'avvio del sistema per evitare la penetrazione dei virus nel computer.
- Applicare le impostazioni di scansione manuale raccomandate dagli esperti di Kaspersky Lab e programmare almeno una scansione la settimana.
- Si raccomanda inoltre di installare Kaspersky Anti-Hacker per una protezione più completa durante la navigazione in Internet.

Regola 2: osservare la massima *cautele* durante la copia di qualsiasi nuovo dato sul computer:

- Eseguire sempre la scansione di tutte le unità rimovibili (floppy disk, unità CD-ROM, flash card, ecc.) per escludere la presenza di virus prima dell'uso.

- Trattare con prudenza i messaggi di posta elettronica. Non aprire mai un allegato, neanche se proveniente da una persona conosciuta, a meno che non lo si stesse aspettando. In particolare, non fidarsi dei messaggi di posta elettronica inviati da presunte società antivirus.
- Trattare con prudenza qualsiasi dato scaricato da Internet. Se si viene invitati a scaricare un programma, verificare sempre che disponga di un certificato di sicurezza.
- Se si scarica un file eseguibile da Internet o da una LAN, esaminarlo prima con Kaspersky Anti-Virus® Personal.
- Visitare solo siti web selezionati. Alcuni siti web contengono script pericolosi o worm di Internet.

Regola 3: leggere attentamente ogni informazione fornita da Kaspersky Lab.

Nella maggior parte dei casi, gli esperti di Kaspersky Lab avvertono gli utenti delle epidemie di nuovi virus con largo anticipo rispetto al periodo di massima diffusione. In quella fase il rischio di infezione è ancora ridotto e scaricando il database antivirus aggiornato è possibile proteggere il computer da questi nuovi virus.

Regola 4: essere sospettosi delle cosiddette "bufale": messaggi di posta elettronica che dichiarano di voler mettere in guardia contro autentiche minacce da parte di virus.

Regola 5: aggiornare regolarmente il sistema operativo per mezzo dell'utilità di aggiornamento di Windows.

Regola 6: acquistare sempre software dotato di regolare licenza da rivenditori autorizzati.

Regola 7: limitare il numero di persone che possono accedere al computer.

Regola 8: Ridurre le perdite potenziali dovute a una possibile infezione:

- Eseguire regolarmente una copia di backup dei propri dati. In caso di perdita di dati, le copie di backup consentono un ripristino piuttosto rapido del sistema. Conservare i propri dischi di distribuzione, floppy disk e altri supporti contenenti software e altri dati importanti in un luogo sicuro.
- Creare sempre un disco di avvio per il ripristino che consenta di riavviare il computer utilizzando un sistema operativo "pulito".


6.1. Quando eseguire la scansione antivirus

Kaspersky Anti-Virus® Personal è in grado di effettuare una scansione antivirus integrale del computer oppure di dischi, cartelle, file o oggetti di posta elettronica specifici.



Durante una scansione completa del computer, il programma non analizza le unità rimovibili né quelle di rete (se disponibili).

Anche se al termine della scansione manuale non sono stati rilevati virus, non vi è alcuna garanzia che il computer ne sia esente. Pertanto Kaspersky Anti-Virus® Personal verifica sempre che l'intero computer sia stato sottoposto a scansione antivirus.

Durante una scansione completa, il programma esamina una maggior quantità di oggetti memorizzati nel computer rispetto alla modalità di protezione in tempo reale. Si raccomanda quindi di eseguire la scansione antivirus del computer almeno una volta la settimana, come misura preventiva. Nel momento più indicato per eseguire una scansione completa il programma visualizza un promemoria. Se la finestra principale dell'applicazione è chiusa, sopra l'icona di Kaspersky Anti-Virus® Personal  nella barra delle applicazioni viene visualizzato un messaggio con la raccomandazione di avviare una scansione completa (se i messaggi a comparsa non sono disattivati, cfr. la sezione 14.8, pag. 93).

Per ulteriori informazioni, aprire la finestra principale dell'applicazione e visualizzare lo status della scansione completa nella sezione destra della scheda **Protezione** (cfr. la Figura 3). Gli stati di scansione possibili sono:



– È di estrema importanza eseguire adesso la scansione completa del computer.



– Si consiglia di eseguire la scansione completa del computer adesso. È possibile dover ripristinare le impostazioni di scansione manuale raccomandate dagli esperti di Kaspersky Lab prima di iniziare la scansione.



– La scansione completa viene effettuata regolarmente o è in corso.

Se necessario, è possibile avviare una scansione completa del computer direttamente dall'area di stato seguendo il collegamento [eseguire la scansione completa del computer](#).

Gli esperti di Kaspersky Lab raccomandano di programmare scansioni complete automatiche (cfr. la sezione 6.4, pag. 43). Lo status di scansione completa indica se la modalità di scansione programmata è abilitata.



Scansione completa del computer non eseguita.

È di estrema importanza [eseguire la scansione completa del computer](#) adesso. Scansione antivirus programmata abilitata. È possibile [modificare la pianificazione](#) della scansione.



Figura 7. Messaggio sulla necessità di eseguire una scansione completa

6.2. Impostazioni di scansione da utilizzare

Dopo l'installazione di Kaspersky Anti-Virus® Personal, tutte le scansioni (scansione antivirus, scansione di oggetti specifici o di unità rimovibili) utilizzeranno le impostazioni raccomandate dagli esperti di Kaspersky Lab (cfr. il Capitolo 3, pag. 18). Lo status delle impostazioni di scansione correnti è indicato nella sezione destra della scheda **Impostazioni** della finestra principale dell'applicazione (cfr. la Figura 4) per mezzo delle seguenti icone:



– Le impostazioni di scansione manuale non corrispondono a quelle raccomandate.



– Le impostazioni di scansione manuale corrispondono a quelle raccomandate.

Se necessario, è possibile modificare le impostazioni predefinite. È possibile modificare il livello di protezione e specificare le azioni che si desidera far eseguire al programma in caso di rilevazione di oggetto infetto o probabilmente infetto da virus o varianti di virus.



Osservare che il livello di protezione e le altre impostazioni assegnate SARANNO APPLICATI a tutti i tipi di scansione, comprese le scansioni complete del computer e quelle di dischi, cartelle o file specificati, ecc.

Se per esempio si esclude un disco specifico dalla scansione (cfr. la sezione 14.2, pag. 79), esso non sarà esaminato neanche quando lo si seleziona per la scansione manuale (cfr. la sezione 6.5, pag. 45). Le uniche eccezioni a questa regola sono le caselle di posta di Microsoft Outlook e Microsoft Outlook Express. Se selezionate, saranno esaminate anche se escluse dalla scansione.



Per modificare il livello di protezione e/o le azioni che si desidera far eseguire al programma in caso di rilevazione di oggetto infetto o probabilmente infetto da virus o varianti di virus, agire come segue:

1. Fare clic su [modifica impostazioni](#) nella sezione destra della scheda **Impostazioni**, oppure su [Configura scansione manuale](#) nella sezione sinistra della stessa scheda.
2. Nella finestra **Impostazioni scansione manuale** (cfr. la Figura 8) che si apre facendo clic sul collegamento sopra indicato, selezionare il *livello di scansione* desiderato per la protezione antivirus del computer. Il livello predefinito è **Raccomandato**. Esso può essere modificato spostando il cursore **Livello di scansione** verso l'alto o verso il basso. Di seguito è riportata la descrizione dei livelli di protezione disponibili e delle situazioni in cui l'uso di un livello è preferibile rispetto a un altro:

- **Massima protezione** – durante la scansione integrale del computer o di dischi, cartelle o file specifici.

Questo livello di protezione è raccomandato qualora si sospetti che il computer sia infetto. Per una descrizione dettagliata dei sintomi di infezione, consultare il Capitolo 1, pag. 6.

- **Raccomandato** – per la scansione integrale del computer o di oggetti specifici con le impostazioni raccomandate dagli esperti di Kaspersky Lab.

L'uso di questo livello di protezione è raccomandato nella maggior parte dei casi in quanto garantisce una combinazione ottimale di velocità di scansione e numero di oggetti esaminati.

- **Alta velocità** – per la scansione antivirus ad alta velocità del computer (compresi la RAM e i settori di boot del disco) o di oggetti selezionati.

Questo livello di protezione garantisce la massima velocità di scansione riducendo il numero degli oggetti da esaminare.

La tabella sottostante contiene un elenco di tutti gli oggetti che possono essere sottoposti a scansione antivirus. Il simbolo + indica che l'oggetto sarà esaminato se è stato selezionato il livello di protezione corrispondente, mentre il simbolo – indica che l'oggetto non sarà esaminato.

	Massima protezione	Raccomandato	Alta velocità
Area selezionata dall'utente	+	+	+ ³
Settori di boot del disco, RAM	+	+	+
Oggetti OLE	+	+	+
File compressi	+	+	+
Archivi autoestraenti	+	+	+
Oggetti eseguiti all'avvio del sistema operativo	+	+	-
Archivi	+	+	-
Caselle di posta di MS Outlook e MS Outlook Express	+	+	-
Database e messaggi di posta elettronica	+	-	-

Per ciascuno dei livelli di protezione disponibili è possibile specificare delle *esclusioni*, cioè un elenco di oggetti da escludere dalla scansione (per ulteriori informazioni cfr. la sezione 14.2, pag. 79). Si raccomanda tuttavia di indicare tali esclusioni solo in caso di problemi di funzionamento di Kaspersky Anti-Virus® Personal, per esempio se il computer ha registrato un rallentamento considerevole.

2. Specificare le azioni che si desidera far eseguire al programma ogni volta che vengono rilevati oggetti infetti, programmi dannosi (worm o cavalli di Troia) o oggetti probabilmente infetti da virus o varianti di virus.

³ La scansione antivirus include solo gli oggetti potenzialmente a rischio di infezione.

- **Richiedi intervento utente** – chiede all'utente quali operazioni eseguire sugli oggetti durante la scansione. Il programma visualizza un elenco di operazioni che è possibile eseguire. Una di esse sarà raccomandata dagli esperti di Kaspersky Lab. Selezionare questa modalità se si ha intenzione di lavorare al computer durante la scansione.

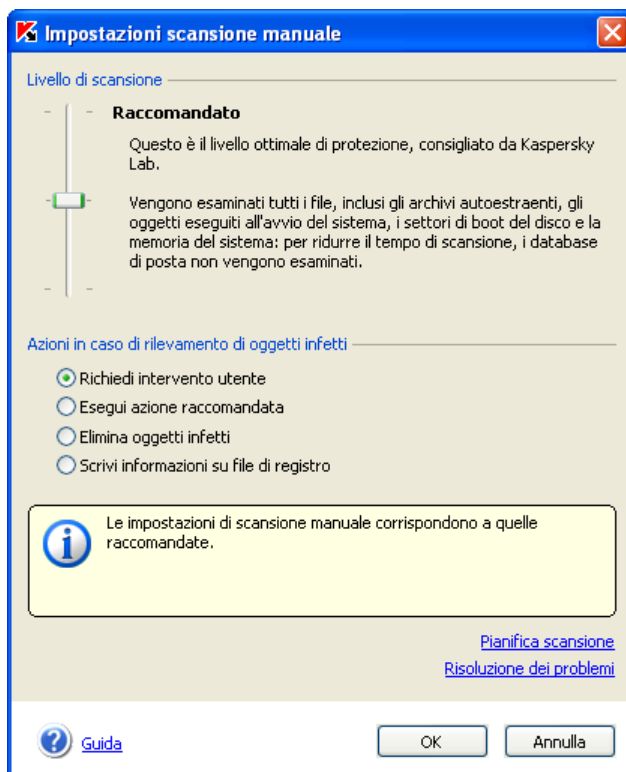


Figura 8. Le impostazioni di scansione manuale

- **Esegui azione raccomandata** – esegue un'azione raccomandata dagli esperti di Kaspersky Lab. Poiché le azioni raccomandate hanno sempre una valida giustificazione, questa modalità può essere selezionata nella maggior parte dei casi. Le azioni raccomandate possono essere le seguenti:
 - riparazione degli oggetti infetti;
 - isolamento degli oggetti probabilmente infetti da virus o varianti di virus.



Talvolta, dopo che un file è stato messo in quarantena, viene visualizzato un messaggio che informa che l'oggetto non può essere eliminato. Ciò dipende dal fatto che l'elaborazione degli oggetti in quarantena richiede lo spostamento fisico dell'oggetto nell'apposita cartella e la cancellazione dello stesso dalla posizione originaria. Tuttavia, alcuni oggetti (per esempio quelli contenuti in un archivio autoestraente) non possono essere cancellati durante tale processo.

- eliminazione di programmi dannosi (*cavalli di Troia e worm*) oppure di oggetti infetti impossibili da riparare.
- **Elimina oggetti infetti** – elimina gli oggetti infetti rilevati durante la scansione, senza tentare di ripararli né chiedere la conferma dell'utente. Questa modalità è consigliata solo se si è certi di non perdere informazioni utili.
- **Scrivi informazioni su file di registro** – il programma indica solo gli oggetti infetti e sospetti rilevati durante la scansione ma senza effettuare alcuna operazione su di essi. Questa modalità è sconsigliata nella maggior parte dei casi perché tutti gli oggetti infetti e sospetti resteranno nel computer, rendendo virtualmente inevitabile la diffusione del virus.

In alcune situazioni non è possibile eseguire alcuna operazione sugli oggetti; per esempio se un oggetto infetto è utilizzato da un altro programma nel momento in cui si cerca di eliminarlo, è impossibile tentarne la riparazione. In questo caso viene visualizzato un messaggio (cfr. Figura 19) che suggerisce di:

- *riparare l'oggetto all'avvio del sistema*. Questa azione viene proposta solo se l'oggetto è riparabile;
- *eliminare l'oggetto all'avvio del sistema*;
- *ignorare l'oggetto*. Non viene eseguita alcuna operazione sull'oggetto interessato. Il programma si limita a registrarne il rilevamento nell'apposito report.

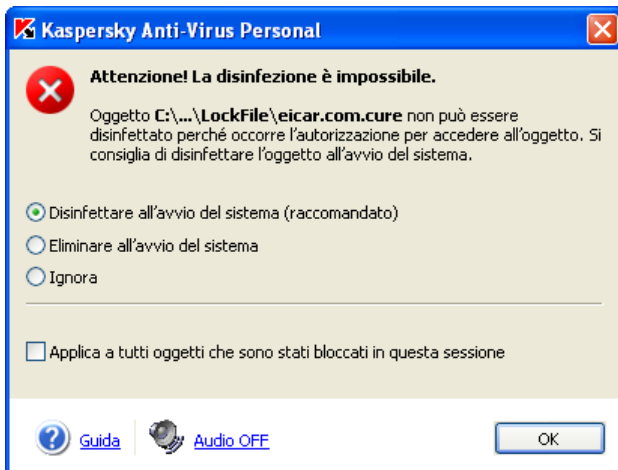


Figura 9. La riparazione immediata non è possibile



Per riparare o eliminare con successo gli oggetti all'avvio del sistema è necessario che la procedura di scansione durante la quale tali oggetti sono stati rilevati sia stata completata. Se la procedura di scansione è stata interrotta tali oggetti non saranno riparati/eliminati.

6.3. Avvio della scansione manuale



Per avviare manualmente una scansione antivirus del computer:

fare clic su [Esamina Risorse del computer](#) nella sezione sinistra della scheda Protezione (cfr. la Figura 3).

Dopo aver fatto clic su questo ipertesto, si apre la finestra di dialogo **Scansione** (cfr. la Figura 6), che indica la percentuale di scansione eseguita, il tempo di inizio, il tempo residuo previsto e il nome dell'oggetto in fase di scansione.

I risultati della scansione saranno sintetizzati in un report (per ulteriori informazioni consultare la sezione 14.7, pag. 86).

6.4. Scansione completa programmata

È possibile programmare una scansione completa del computer a un'ora specifica di giorni della settimana prestabiliti. Per esempio, se la pausa pranzo è alle 13:00, si può scegliere di programmare l'inizio di una scansione completa proprio a quell'ora.



Per programmare l'avvio automatico di una scansione completa:

1. fare clic su [Configura scansione manuale](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4).
2. Quando si apre la finestra di dialogo **Impostazioni scansione manuale** (cfr. la Figura 8), fare clic su [Pianifica scansione](#) per aprire la finestra di dialogo **Pianifica scansione**.
3. All'apertura della finestra di dialogo the **Pianifica scansione** (cfr. la Figura 10), impostare gli orari in cui si desidera che il programma esegua l'operazione:
 - **Specifica intervalli scansione in giorni** – esegue la scansione antivirus in base all'intervallo in giorni specificato. L'impostazione predefinita prevede una scansione quotidiana alle 20:00. Se si desidera modificare l'impostazione predefinita e l'ora di inizio, digitare l'intervallo di scansione desiderato in giorni nel campo **Ogni** della sezione **Parametri di scansione**. Indicare quindi l'orario di inizio nel campo **Inizio scansione**.
 - **Scansione in giorni specifici** – specificare i giorni della settimana in cui si desidera che il programma esegua la scansione. Per impostazione predefinita, il programma suggerisce una scansione settimanale ogni venerdì alle 20:00. Se si desidera modificare l'impostazione predefinita e l'ora di inizio, selezionare i giorni della settimana nella sezione **Parametri di scansione** e specificare l'ora di inizio nel campo **Inizio scansione**.
 - ☑ **Non eseguire scansione programmata se la batteria è inferiore a** – per computer portatili: annulla la scansione manuale se la carica della batteria è inferiore al livello minimo consentito specificato. Per mezzo del cursore, selezionare il livello minimo consentito di carica della

batteria (in percentuale) al di sotto del quale non è possibile avviare le scansioni programmate.

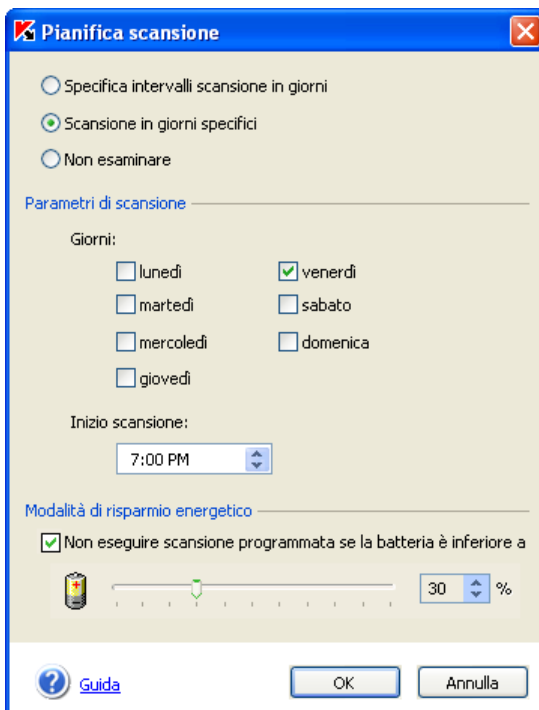


Figura 10. Impostazione di una scansione programmata

4. Fare clic sul pulsante **OK**.

6.5. Scansione manuale di oggetti selezionati

Talvolta è necessario escludere la presenza di virus da oggetti specifici piuttosto che sottoporre a scansione l'intero computer. Tali oggetti possono includere, per esempio, un disco fisso con file di programmi e giochi, database di posta elettronica prelevati dall'ufficio, archivi allegati a messaggi ricevuti, ecc. È possibile selezionare gli oggetti da sottoporre a scansione mediante Kaspersky Anti-Virus® Personal o strumenti Windows standard (per esempio, **Windows Explorer**, **Risorse del computer**, ecc.).



Per esaminare un oggetto da selezionato mediante strumenti Windows standard:

selezionare e fare clic con il pulsante destro del mouse sull'oggetto che si desidera sottoporre a scansione; quando si apre il menu di scelta rapida selezionare il comando **Scansione antivirus** (cfr. la Figura 11).

Per selezionare ed esaminare oggetti servendosi di Kaspersky Anti-Virus® Personal seguire queste istruzioni:



Per selezionare ed esaminare oggetti servendosi di Kaspersky Anti-Virus® Personal:

fare clic su [Esamina oggetti](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3).

Si apre la finestra **Seleziona oggetti da esaminare** (cfr. la Figura 12), contenente un elenco di oggetti che possono essere sottoposti a scansione antivirus e dotata di pulsanti di interfaccia per modificare questo elenco e controllare la scansione.

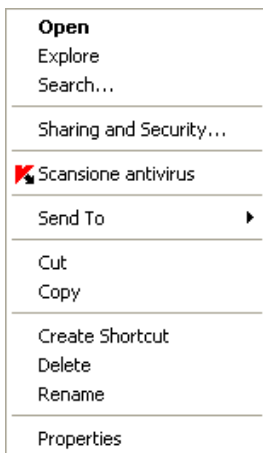


Figura 11. Scansione di un oggetto mediante strumenti Windows standard



Figura 12. Selezione di oggetti da sottoporre a scansione

L'elenco iniziale include i seguenti oggetti:

- unità rimovibili, tra cui floppy disk e CD-ROM;
- dischi fissi;
- caselle di posta di Microsoft Outlook e Microsoft Outlook Express;
- cartella **Documenti**.

Per aggiungere un oggetto all'elenco, fare clic su **Aggiungi** e cercare nella finestra che si apre il file o la cartella che si desidera aggiungere. Tutti gli oggetti aggiunti saranno disponibili in questo elenco per scansioni future.

Per eliminare un oggetto dall'elenco, selezionare la casella corrispondente e fare clic su **Elimina**. Osservare tuttavia che è possibile eliminare dall'elenco solo gli oggetti aggiunti manualmente. Gli oggetti facenti parte dell'elenco originario non possono essere eliminati.



Per selezionare ed esaminare oggetti inclusi nell'elenco:

1. Selezionare dall'elenco gli oggetti che si desidera esaminare.
2. Fare clic su **Esamina** per iniziare la scansione.

Indipendentemente dalla modalità di avvio della scansione (da Kaspersky Anti-Virus® Personal o mediante il menu di scelta rapida di Windows), si apre la finestra **Scansione** (cfr. la Figura 6), contenente una barra di avanzamento che indica la percentuale di scansione eseguita, il tempo di inizio, il tempo residuo previsto e il nome dell'oggetto in fase di scansione.

I risultati della scansione vengono documentati in un apposito report (cfr. la sezione 14.7, pag. 86).

6.6. Scansione di archivi

Kaspersky Anti-Virus® Personal esamina gli archivi se è stato selezionato il livello di **Massima protezione** o **Raccomandata** e se tali archivi non erano stati precedentemente esclusi dalla scansione (cfr. la sezione 14.2, pag. 79).

Kaspersky Anti-Virus® Personal esamina gli archivi se questo tipo di file è stato specificamente selezionato ai fini della scansione (cfr. la sezione 6.5, pag. 45) oppure durante una scansione completa del computer se è stato selezionato il livello di **Massima protezione** o **Raccomandata**, a condizione che tali archivi non fossero stati precedentemente esclusi dalla scansione (cfr. la sezione 14.2, pag. 79).



Kaspersky Anti-Virus® Personal esamina tutti gli oggetti contenuti all'interno di archivi, ma ripara esclusivamente archivi *zip*, *arj*, *cab* e *rar*.

Il programma non disinfetta gli archivi autoestraenti! In presenza di un virus rilevato all'interno di un archivio autoestraente, l'archivio viene eliminato.

Se un archivio o un oggetto all'interno di un archivio è protetto da password e la modalità di richiesta password è abilitata, il programma richiede l'inserimento della password prima di proseguire la scansione (cfr. la Figura 13).



È possibile abilitare o disabilitare la richiesta di password selezionando la casella **Non chiedere password durante scansione oggetti** nella finestra **Individuazione errori** accessibile da **Impostazioni scansione manuale** (cfr. la sezione 14.3, pag. 80).



Figura 13. Inserimento della password necessaria per esaminare un archivio

Nel campo **Inserire la password** inserire la password richiesta per accedere a questo archivio o a un oggetto al suo interno e fare clic su **OK**. Dopo l'inserimento della password il programma esamina l'archivio e tutti gli oggetti in esso contenuti.



Per poter analizzare oggetti all'interno di archivi, Kaspersky Anti-Virus® Personal scompatta l'archivio in una cartella temporanea, esamina gli oggetti, li elabora e li comprime in un nuovo archivio con lo stesso nome, copiato nella stessa posizione dell'archivio originale, sovrascrivendo così quello preesistente. Una procedura simile viene utilizzata per l'elaborazione di oggetti protetti da password all'interno di archivi. Dopo l'elaborazione, gli oggetti vengono compressi in un nuovo archivio senza uso di password.

Se all'interno dell'archivio esaminato viene rilevato un nuovo archivio protetto da password, Kaspersky Anti-Virus® Personal applica automaticamente la password utilizzata per accedere al primo archivio. La nuova password viene richiesta solo se quella utilizzata non è valida.

Se non si desidera esaminare un oggetto specifico protetto da password all'interno di un archivio, fare clic sul pulsante **Ignora** e proseguire la scansione.

Se non si conosce la password, il programma non è in grado di esaminare l'archivio protetto né gli oggetti in esso contenuti. In questo caso è consigliabile fare clic su **Ignora** e proseguire la scansione.

Se si seleziona la casella **Applica a tutti gli oggetti protetti da password in questa sessione**, l'azione scelta successivamente sarà applicata a tutti gli oggetti protetti da password.

Per esempio, se si seleziona questa casella e si fa clic sul pulsante **Ignora archivio**, tutti gli archivi protetti da password saranno ignorati durante questa scansione.

Se si inserisce la password, selezionare la casella e fare clic sul pulsante **OK**; in tal modo la password inserita sarà utilizzata automaticamente per tutti gli oggetti protetti in tutti gli archivi della sessione. Se la password non è valida per un determinato oggetto, quell'oggetto sarà ignorato.

CAPITOLO 7. SCANSIONE DI UN CD O FLOPPY DISK

Il computer può facilmente infettarsi a causa di virus presenti su floppy disk, CD e altri supporti mobili. Se uno dei floppy disk (o CD d'avvio) utilizzati era infetto da un virus d'avvio e si è riavviato il computer lasciando il disco nell'unità, il sistema può aver subito gravi danni.

È pertanto consigliabile esaminare tutti i supporti mobili prima dell'uso.

I supporti mobili possono essere esaminati sia dalla finestra principale di Kaspersky Anti-Virus® Personal sia tramite il menu di scelta rapida di Windows accessibile da **Windows Explorer**, dal **desktop**, ecc.



Per esaminare i supporti mobili tramite il menu di scelta rapida di Windows:

selezionare e fare clic con il pulsante destro del mouse sulle unità (è possibile selezionare CD-ROM e floppy disk simultaneamente). All'apertura del menu di scelta rapida selezionare **Scansione antivirus** (cfr. la Figura 11).



Per esaminare un CD-ROM o floppy disk dalla finestra principale di Kaspersky Anti-Virus® Personal:

1. Inserire il supporto da esaminare nell'unità corrispondente. Il programma è in grado di esaminare simultaneamente CD e floppy disk.
2. fare clic su [Esamina unità rimovibili](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3).

oppure

Fare clic sul collegamento [Esamina oggetti](#), aprire la finestra **Seleziona oggetti da esaminare** (cfr. la Figura 12), selezionare le unità rimovibili e premere il pulsante **Esamina**.

L'avanzamento della scansione (percentuale completata) è visibile nella finestra **Scansione** che si apre subito dopo l'avvio della scansione (cfr. la Figura 6).

Se si seleziona una sola unità rimovibile da esaminare, Kaspersky Anti-Virus® chiede di inserire il disco nell'unità rimovibile successiva al termine della scansione.



Osservare le seguenti caratteristiche del programma:

- Se si dimentica di inserire nell'unità il CD o il floppy disk da esaminare, o se le rispettive unità non sono collegate, l'unità non sarà esaminata. Non vengono visualizzati messaggi.
- Se il floppy disk da esaminare viene inserito nella rispettiva unità dopo l'inizio della scansione, esso non sarà esaminato. Lo stesso vale per i CD-ROM e altri supporti rimovibili.
- Se si estrae il floppy disk dalla relativa unità o si scollega quest'ultima durante la scansione, il programma inserisce un'informazione di errore nel report ma senza visualizzare alcun messaggio. Quindi, il programma esamina, se presente, l'unità mobile successiva.

Nel momento in cui viene collegata un'unità rimovibile al sistema (vale a dire quando il sistema rileva l'unità come nuovo hardware), l'antivirus la esamina per escludere la presenza di virus d'avvio.

CAPITOLO 8. CONFIGURAZIONE DELLA PROTEZIONE IN TEMPO REALE

La funzione di protezione in tempo reale di Kaspersky Anti-Virus® Personal offre il monitoraggio costante di tutte le operazioni potenzialmente a rischio eseguite sul computer. Così, il programma effettua la ricerca di virus nei file aperti o salvati (dopo la modifica), nei messaggi inviati o ricevuti, all'esecuzione di un file oppure di uno script in Microsoft Internet Explorer. Quando l'utente o qualsiasi programma cerca di eseguire una qualsiasi delle azioni sopra menzionate, Kaspersky Anti-Virus® blocca dapprima l'azione, esamina l'oggetto, infine, in base ai risultati della scansione, permette o proibisce l'azione o visualizza un messaggio.

8.1. Verifica dello status della protezione

Nella sezione destra della scheda **Protezione** (cfr. la Figura 3) nella finestra principale di Kaspersky Anti-Virus® Personal sono visualizzate delle informazioni sullo status corrente della protezione in tempo reale, identificato dalle seguenti icone:



– La protezione in tempo reale è abilitata. Il livello di protezione del computer è quello raccomandato.



– La protezione in tempo reale è abilitata. Le impostazioni di protezione non corrispondono a quelle raccomandate.



– La Protezione in tempo reale è disabilitata o non funziona. Se la protezione è disabilitata si raccomanda di abilitarla. Se invece non funziona, si raccomanda di configurare i parametri della protezione in tempo reale (cfr. sezione 14.1, pag. 76) e quindi di abilitarla.

8.2. Definizione delle azioni del programma e impostazione del livello di protezione

Per impostazione predefinita, Kaspersky Anti-Virus® Personal applica le impostazioni raccomandate, impedendo l'accesso a tutti gli oggetti infetti, ai programmi dannosi (worm, cavalli di Troia) e agli oggetti probabilmente infetti da virus o varianti di virus che l'utente stia cercando di aprire a fini di lettura, scrittura o esecuzione. Quindi visualizza un messaggio che richiede l'intervento dell'utente.



Nella modalità di protezione in tempo reale, il programma **NON ESEGUE LA SCANSIONE** di archivi, database di posta elettronica e messaggi di posta in formato testo! Fanno eccezione gli archivi autoestraenti, che vengono sottoposti a scansione se il livello di **Massima protezione** è selezionato.

Se la modalità di protezione in tempo reale è abilitata, è possibile selezionare sia il livello di protezione del computer sia le azioni che si desidera far eseguire al programma ogni volta che vengono rilevati oggetti infetti, programmi dannosi o oggetti probabilmente infetti da virus o varianti di virus.



Per configurare le azioni che si desidera far eseguire al programma in caso di rilevazione di oggetto dannoso:

1. Fare clic sul collegamento [Configura protezione in tempo reale](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4) o su [modifica impostazioni](#) nell'area di stato della scheda **Impostazioni**.
2. All'apertura della finestra di dialogo **Impostazioni protezione in tempo reale** (cfr. la Figura 14), selezionare il livello di protezione per mezzo del cursore. Modificando il livello di protezione si modifica anche il rapporto tra la velocità di scansione e il numero degli oggetti da analizzare. Il numero degli oggetti da analizzare è inversamente proporzionale alla velocità di scansione.



Nella modalità di protezione in tempo reale, il programma non esegue la scansione degli archivi. Per analizzare e riparare anche gli archivi è necessario avviare una scansione completa del computer (cfr. sezione 6.3, pag. 43).

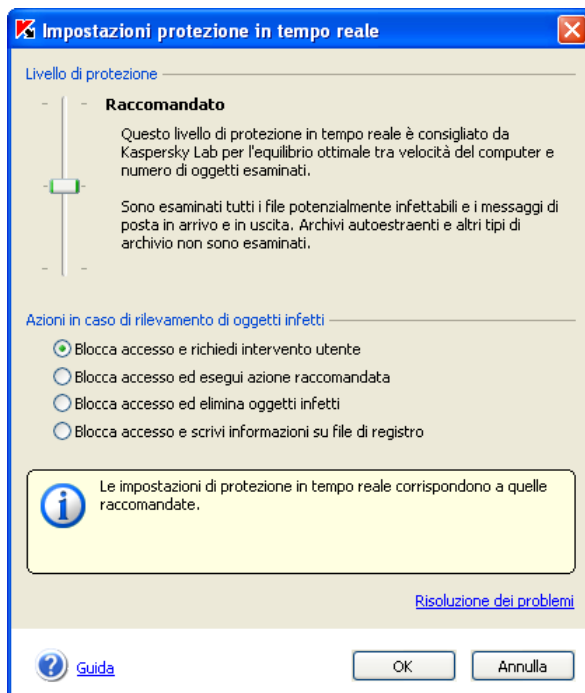


Figura 14. Configurazione della protezione in tempo reale

Kaspersky Anti-Virus® Personal consente all'utente di scegliere tra tre livelli di protezione:

- **Massima protezione** – garantisce la massima accuratezza di monitoraggio degli oggetti aperti, salvati o eseguiti.
- **Raccomandato** – è il livello consigliato dagli esperti di Kaspersky Lab. A questo livello di protezione, il programma analizza lo stesso tipo di oggetti previsto dal livello di **Massima protezione**, con l'eccezione di archivi autoestraenti e messaggi di posta elettronica in uscita.
- **Alta velocità** – le impostazioni di questo livello di protezione garantiscono prestazioni ottimali del computer durante l'uso di programmi che richiedono notevoli risorse RAM, poiché la scansione coinvolge un numero inferiore di oggetti.

La tabella sottostante contiene un elenco di tutti gli oggetti che possono essere sottoposti a scansione antivirus. Il simbolo + indica che l'oggetto sarà esaminato se è stato selezionato il livello di protezione

corrispondente, mentre il simbolo – indica che l'oggetto non sarà esaminato.

	Massima protezione	Raccomandato	Alta velocità
File potenzialmente infettabili	+	+	+
Settori di boot del disco	+	+	+
File compressi	+	+	+
Oggetti OLE	+	+	+
Messaggi di posta elettronica in uscita⁴	+	+	+
Messaggi di posta elettronica in uscita⁵	+	–	–
Archivi autoestraenti⁶	+	–	–
Database e messaggi di posta elettronica	–	–	–


⁴ Posta POP3 in arrivo

⁵ Posta SMTP in uscita

⁶ Gli archivi autoestraenti vengono sottoposti a scansione limitatamente all'area eseguibile.

È possibile specificare i file da escludere dalla scansione a qualsiasi livello di protezione in tempo reale, oppure disabilitare la protezione in tempo reale stessa. Per informazioni più dettagliate, cfr. la sezione 14.1a pag. 76.

3. Specificare le azioni che si desidera far eseguire al programma ogni volta che vengono rilevati oggetti infetti, programmi dannosi (worm o cavalli di Troia) o oggetti probabilmente infetti da virus o varianti di virus:

 **Blocca accesso e richiedi intervento utente** – nega l'accesso all'oggetto e visualizza un messaggio che invita l'utente a scegliere l'azione da eseguire sull'oggetto. È la modalità predefinita.

Se non si specifica l'azione entro 30 secondi dalla visualizzazione del messaggio, il programma esegue l'azione raccomandata. Per ogni tipo di oggetto rilevato esiste un'azione specifica raccomandata. Per esempio, in caso di oggetto infetto l'azione raccomandata è *Disinfetta*. Accanto al nome dell'azione raccomandata è sempre visualizzato il testo **(raccomandato)**.

Esaminiamo di seguito l'elenco di tutte le azioni possibili suggerite da Kaspersky Anti-Virus® Personal (l'elenco può variare per ogni tipo di oggetto):

- *Disinfetta*: riparazione degli oggetti infetti.
- *Quarantena*: isolamento degli oggetti probabilmente infetti da virus o varianti di virus.



Talvolta, dopo che un file è stato messo in quarantena, viene visualizzato un messaggio che informa che l'oggetto non può essere eliminato. Ciò dipende dal fatto che l'elaborazione degli oggetti in quarantena richiede lo spostamento fisico dell'oggetto nell'apposita cartella e la cancellazione dello stesso dalla posizione originaria. Tuttavia, alcuni oggetti (per esempio quelli contenuti in un archivio autoestraente) non possono essere cancellati durante tale processo.

- *Elimina*: eliminazione di programmi dannosi (*cavalli di Troia* e *worm*) oppure di oggetti infetti impossibili da riparare.
- *Ignora*: non viene eseguita alcuna operazione sull'oggetto interessato; il programma si limita a registrare il rilevamento nel report.



Se si desidera mettere in quarantena un oggetto infetto, selezionare *Ignora* e isolare quindi l'oggetto manualmente (cfr. la sezione 13.3, pag. 81).

- **Blocca accesso ed esegui azione raccomandata** – nega l'accesso all'oggetto ed esegue una delle azioni raccomandate per l'oggetto. L'azione raccomandata in caso di oggetti è *Disinfetta*; per quelli probabilmente infetti è *Quarantena*; per i cavalli di Troia e i worm è *Elimina*.
- **Blocca accesso ed elimina oggetti infetti** – elimina gli oggetti senza ulteriori avvertimenti all'utente.
- **Blocca accesso e scrivi informazioni su file di registro** – nega l'accesso all'oggetto e non visualizza alcun messaggio per richiedere l'intervento dell'utente.

In alcune situazioni non è possibile eseguire alcuna operazione sugli oggetti; per esempio se un oggetto infetto è utilizzato al momento della rilevazione da un altro programma è impossibile tentarne la riparazione. In questo caso viene visualizzato un messaggio (cfr. la Figura 9) che suggerisce di:

- *riparare l'oggetto all'avvio del sistema*. Questa azione viene proposta solo se l'oggetto è riparabile;
- *eliminare l'oggetto all'avvio del sistema*;
- *ignorare*.



Osservare che le azioni sopra elencate non vengono applicate né ai messaggi di posta elettronica né agli script dannosi:

- Al rilevamento di un messaggio di posta elettronica infetto o probabilmente infetto, Kaspersky Anti-Virus® Personal esegue l'azione raccomandata senza ulteriori notifiche all'utente.
- Al rilevamento di uno script dannoso, il programma avverte sempre l'utente, al quale è concessa la possibilità di stabilire autonomamente le ulteriori azioni da intraprendere.

CAPITOLO 9. PROTEZIONE DEL COMPUTER CONTRO GLI ATTACCHI PROVENIENTI DALLA RETE

Kaspersky Anti-Virus Personal 5.0 garantisce la protezione del computer contro gli accessi non autorizzati ai dati e contro gli attacchi di pirati informatici provenienti dalle reti locali (LAN) e da Internet..

Per rilevare gli attacchi di pirateria informatica, il programma si serve di un database degli attacchi informatici attualmente noti. Esso viene aggiornato e installato con il database antivirus (per informazioni cfr. il Capitolo 13 a pag. 67).

Per impostazione predefinita, la protezione dagli attacchi informatici viene abilitata automaticamente all'avvio di Kaspersky Anti-Virus. Tale funzione esegue il monitoraggio di tutte le connessioni di rete e analizza tutti i dati ricevuti tramite la rete, indipendentemente dalla loro provenienza (rete locale LAN oppure Internet).



Se la funzione di protezione dagli attacchi informatici è disabilitata, si raccomanda di abilitarla procedendo come segue:

1. Seguire il collegamento [Protezione in tempo reale](#) nella parte sinistra della barra della scheda **Impostazioni** (cfr. la Figura 4) o il collegamento [modificare le impostazioni della protezione in tempo reale](#) dall'area delle informazioni di stato nella scheda **Protezione**.
2. Nella finestra **Impostazione Protezione in tempo reale** seguire il collegamento [Individuazione errori](#) per accedere alla finestra **Individuazione errori** e selezionare la casella di controllo **Disabilita protezione contro attacchi di rete**.

Ogni tentativo di attacco al computer viene bloccato e seguito dalla visualizzazione dell'avviso corrispondente (cfr. la Figura 15) contenente informazioni sul tipo di attacco perpetrato, l'indirizzo IP del computer di provenienza dell'attacco e la porta locale (se possibile).



Figure 15. Avviso dell'attacco proveniente dalla rete

Per ulteriori informazioni su altre impostazioni della protezione contro gli attacchi provenienti dalla rete, consultare il paragrafo 14.2 a pag. 79).

CAPITOLO 10. PROTEZIONE ANTIVIRUS DELLA POSTA ELETTRONICA

Kaspersky Anti-Virus® Personal protegge in tempo reale i messaggi di posta elettronica in entrata e in uscita.



Per proteggere la posta dai virus:

Abilitare la protezione in tempo reale e accertarsi che la casella **Disattiva protezione posta in tempo reale** nella finestra di dialogo **Individuazione errori** sia deselezionata (cfr. la sezione 14.1, pag. 76).

Per quanto riguarda la gestione della posta elettronica, Kaspersky Anti-Virus® Personal applica le seguenti regole:

- Kaspersky Anti-Virus® Personal protegge la posta elettronica dai virus, indipendentemente dal programma utilizzato ⁷. Esamina tutti i messaggi in entrata e in uscita nel momento in cui l'utente o il programma di posta li ricevono o li inviano.
- Al rilevamento di un oggetto infetto in un messaggio di posta elettronica viene eseguita una delle azioni raccomandate per tale tipo di oggetto: Kaspersky Anti-Virus® Personal cerca di riparare l'oggetto e, se la riparazione risulta impossibile, lo elimina dal messaggio.
- Se si utilizzano i servizi di posta elettronica di server remoti tramite un browser di Internet, per esempio Microsoft Internet Explorer, Kaspersky Anti-Virus® Personal esamina gli allegati nel momento in cui vengono aperti o salvati sul disco.

I database di posta elettronica importati da altri computer ma non ancora attivati possono essere esaminati avviando una scansione manuale.

⁷ Kaspersky Anti-Virus® Personal protegge in tempo reale tutti i messaggi POP3 in entrata e SMTP in uscita.



Per poter esaminare le caselle di posta di Microsoft Outlook o Microsoft Outlook Express:

1. Accertarsi che la casella **Non esaminare caselle di posta** nella finestra di dialogo **Individuazione errori** sia deselezionata (cfr. la sezione 14.3, pag. 79).
2. Fare clic su [Esamina oggetti](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3).
3. Nella finestra di dialogo **Selezione oggetti da esaminare** (cfr. la Figura 12), selezionare la casella **Caselle di posta**.
4. Fare clic su **Esamina**.

Il programma avvia la scansione di tutti i database e i file formato posta di Microsoft Outlook e Microsoft Outlook Express.



In seguito all'elaborazione dei database di posta elettronica di Microsoft Outlook e Microsoft Outlook Express, la data e l'ora delle variazioni apportate vengono sempre modificate, indipendentemente dal tipo di azione selezionata per l'oggetto.



Per poter eseguire la scansione di database nel formato di altri programmi di posta elettronica (per esempio, TheBat) o di database prelevati da un disco (per esempio portati dall'ufficio),

1. Fare clic sul collegamento [Esamina oggetti](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3).
2. Nella finestra **Selezione oggetti da esaminare** che si apre (cfr. la Figura 12) selezionare un disco o cartella in cui tali database sono memorizzati.
3. Premere **Esamina**.

CAPITOLO 11. GESTIONE DI OGGETTI CONTAMINATI E SOSPETTI

Le azioni eseguite da Kaspersky Anti-Virus® Personal al rilevamento di oggetti infetti, programmi dannosi o oggetti probabilmente infetti da virus o varianti di virus dipendono totalmente dalle impostazioni di protezione in tempo reale e scansione manuale specificate dall'utente. Questo capitolo presenta alcune situazioni in cui Kaspersky Anti-Virus® Personal offre una scelta di azioni da eseguire su oggetti e programmi infetti o sospetti.

Esse si verificano quando si selezionano le seguenti azioni da eseguire su oggetti e programmi infetti o sospetti:


- Protezione in tempo reale (cfr. la Figura 14):
 - 🔒 **Blocca accesso e richiedi intervento utente**
- Scansione manuale (cfr. la Figura 8):
 - 🔒 **Richiedi intervento utente**

Al rilevamento di un oggetto infetto, programma dannoso o oggetto probabilmente infetti da virus o varianti di virus, viene visualizzato un messaggio (cfr. la Figure 16), contenente:

- una descrizione dettagliata dell'oggetto con l'indicazione del nome del virus che lo ha infettato o potrebbe averlo infettato, o il nome del programma dannoso;
- un elenco delle azioni che è possibile eseguire sull'oggetto, che prevede sempre un'azione raccomandata dagli esperti di Kaspersky Lab (tale azione è sempre accompagnata dalla dicitura "raccomandata"). In base al tipo di oggetto rilevato, le azioni proposte possono essere:
 - **Disinfetta** – tenta di riparare l'oggetto infetto, se possibile.
 - **Elimina** – elimina l'oggetto infetto o probabilmente infetto.
 - **Ignora** – non esegue alcuna operazione sull'oggetto interessato; il programma si limita a registrare il rilevamento nel report.
 - **Quarantena** – mette in quarantena l'oggetto probabilmente infetti da virus o varianti di virus, in modo da consentirne

successivamente il controllo, il ripristino, l'invio a Kaspersky Lab per un'analisi o l'eliminazione (cfr. la sezione 14.4, pag. 81).

È possibile inoltre applicare l'azione selezionata a tutti gli oggetti accomunati dallo stesso status selezionando la casella corrispondente. Per esempio, per applicare l'azione selezionata a tutti gli oggetti infetti che non possono essere riparati, selezionare la casella **Applica a tutti infetti oggetti, che possono essere disinfettati (in questa sessione).**

Se si chiude questa finestra premendo il pulsante  nell'angolo superiore destro della finestra l'oggetto sarà ignorato.

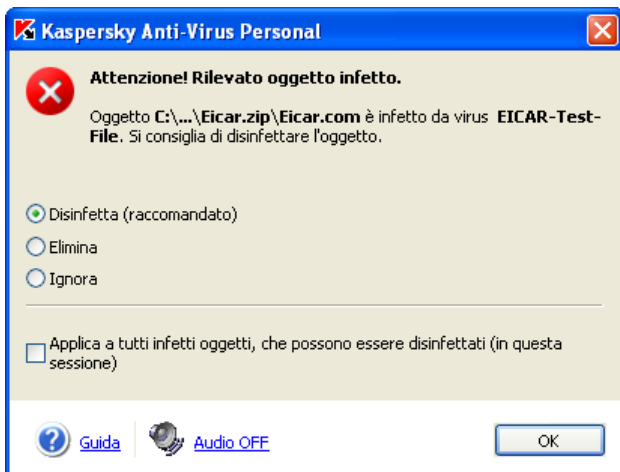


Figure 16. Messaggio sul rilevamento di un oggetto infetto

CAPITOLO 12. RINNOVO DELLA LICENZA

Per poter utilizzare Kaspersky Anti-Virus® Personal è necessario disporre di una chiave di *licenza*. La chiave è fornita in dotazione con il kit di distribuzione e consente di utilizzare il programma dalla data dell'acquisto e dell'installazione della chiave.



Senza la chiave di licenza Kaspersky Anti-Virus® Personal **NON FUNZIONA!**

Dopo la scadenza della licenza, Kaspersky Anti-Virus® Personal conserva la funzionalità ma non consente di usufruire del servizio di aggiornamento del database antivirus. È possibile continuare ad eseguire la scansione antivirus del computer e della posta elettronica e riparare gli oggetti infetti, ma solo utilizzando database obsoleti risalenti alla data di scadenza della licenza. Pertanto non possiamo garantire una protezione al 100% dai nuovi virus apparsi dopo la scadenza della licenza dell'antivirus.

Per evitare il rischio di infezione del computer da parte di nuovi virus, è consigliabile rinnovare la licenza di Kaspersky Anti-Virus® Personal.

Kaspersky Anti-Virus® Personal avvisa l'utente due settimane prima della scadenza della licenza, visualizzando un promemoria ogni volta che si apre il programma.



Per rinnovare la licenza è necessario acquistare e installare una nuova chiave per Kaspersky Anti-Virus® Personal. Per ottenere una nuova chiave:

1. Rivolgersi al rivenditore presso il quale si è acquistato il prodotto e acquistare una nuova chiave di licenza per Kaspersky Anti-Virus® Personal.

oppure

Per acquistare una nuova licenza direttamente da Kaspersky Lab, seguire il collegamento [Rinnovo della licenza](#) nella scheda **Assistenza** (cfr. Figura 5) e compilare l'apposito modulo visualizzato nella pagina web che si aprirà. La chiave di licenza sarà inviata all'indirizzo di posta elettronica indicato nell'ordine non appena sarà stato ricevuto il pagamento.

2. Installare la nuova chiave di licenza secondo la modalità descritta di seguito:
 - fare clic su [Chiavi di licenza](#) nella sezione sinistra della scheda **Assistenza** (cfr. la Figura 5).
 - All'apertura della finestra **Gestione delle chiavi di licenza** (cfr. la Figura 17), fare clic su **Aggiungi** e selezionare la nuova chiave nella finestra di dialogo standard **Seleziona** di Windows.

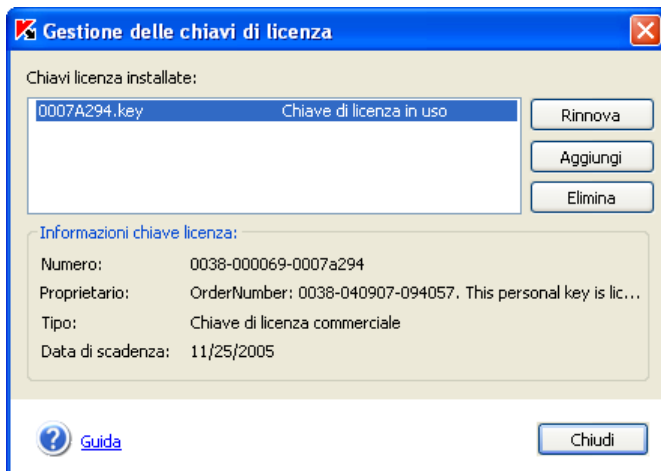


Figura 17. La finestra di dialogo **Gestione delle chiavi di licenza**

CAPITOLO 13. SCARICAMENTO DEGLI AGGIORNAMENTI

Oltre a consentire l'aggiornamento dei database antivirus usati dal programma per rilevare la presenza di software nocivi e riparare oggetti infetti e del database degli attacchi di rete, Kaspersky Lab offre ai propri utenti la possibilità di aggiornare i moduli dell'applicazione Kaspersky Anti-Virus Personal.



L'unico modo per garantire la sicurezza del computer consiste nell'**aggiornare tempestivamente il database antivirus**. Ogni giorno compaiono centinaia di nuovi virus, e ogni giorno gli esperti di Kaspersky Anti-Virus® aggiornano il database antivirus in base alle più recenti informazioni sulle nuove minacce. Si raccomanda di aggiornare il database antivirus almeno ogni 12 ore; nei periodi di maggior diffusione dei virus è opportuno aggiornare il database con la massima frequenza possibile, preferibilmente ogni 3 ore.

Per scaricare gli aggiornamenti, Kaspersky Anti-Virus® Personal si connette a uno dei server dedicati di Kaspersky Lab accessibile via Internet oppure copia i file necessari da una cartella locale del computer, in base alle impostazioni (per ulteriori informazioni vedere di seguito).

Gli aggiornamenti possono essere scaricati manualmente o automaticamente (aggiornamenti programmati). Per scaricare gli aggiornamenti è necessario che il computer sia connesso a Internet. Kaspersky Anti-Virus® Personal copia gli aggiornamenti dai server remoti dedicati e installa sul computer i file necessari.



Talvolta, dopo l'aggiornamento del database antivirus viene visualizzato un messaggio che invita a riavviare il computer. Di regola ciò avviene dopo l'aggiornamento di moduli dell'applicazione o del database degli attacchi di rete. Il riavvio del sistema è necessario per installare e attivare tutti gli aggiornamenti scaricati.

13.1. Quando scaricare gli aggiornamenti

Quando il database antivirus necessita di un aggiornamento il programma visualizza un messaggio. È possibile decidere di dover aggiornare il database antivirus anche dopo averne verificato lo stato nella sezione destra della scheda **Protezione** (cfr. la Figura 3).

Lo stato del database antivirus è identificato dai seguenti simboli:



– il database antivirus è stato aggiornato di recente o è in fase di aggiornamento.



– il database antivirus deve essere aggiornato. Se l'aggiornamento è impossibile perché la licenza è scaduta, il programma offre di visualizzare le informazioni sulle modalità di rinnovo della licenza.



– è necessario aggiornare il database antivirus poiché è completamente obsoleto o addirittura assente.

13.2. Scaricamento degli aggiornamenti da Internet

Kaspersky Lab aggiorna il database antivirus residente sui server dedicati ogni tre ore.

I server di aggiornamento di Kaspersky Lab sono siti web in cui Kaspersky Lab conserva e aggiorna il database antivirus.



Al fine di garantire l'aggiornamento costante del proprio database antivirus dai server dedicati di Kaspersky Lab è necessario applicare le impostazioni descritte nelle seguenti istruzioni:

1. Fare clic sul link [Configura aggiornamento](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4).
2. All'apertura della finestra di dialogo **Impostazioni aggiornamento** (cfr. la Figura 18), selezionare una delle seguenti modalità di aggiornamento dall'elenco a discesa **Tipo aggiornamento**:

da Internet, database standard – database antivirus che consente di rilevare tutti i programmi dannosi esistenti e riparare gli oggetti e i dati colpiti.

da Internet, database estesi – *database standard* e database supplementare che consente di rilevare i programmi che aprono l'accesso ai non autorizzati.



Il database antivirus standard da solo è in grado di garantire un'efficiente protezione del computer. L'uso del database esteso può influire sulla velocità di funzionamento del programma.

3. Se ci si serve di una connessione Internet Dial-up e non si desidera che Kaspersky Anti-Virus® interrompa il processo di aggiornamento in caso di disconnessione temporanea dalla rete, selezionare la casella **Attendi connessione remota rete.**



Questa impostazione serve solo per gli aggiornamenti programmati automatici del database antivirus!

4. Fare clic su **OK**.

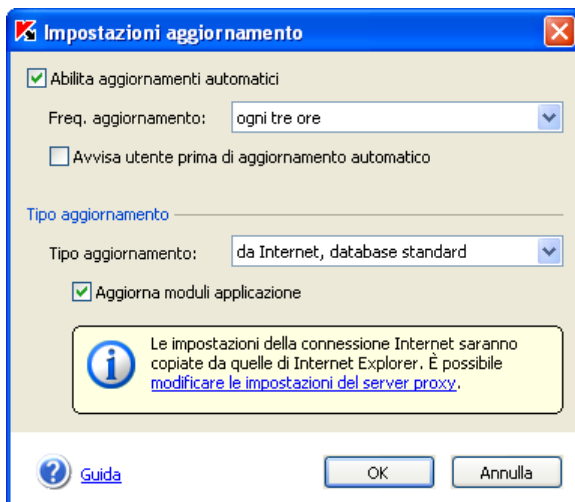


Figura 18. La finestra di dialogo **Impostazioni aggiornamento**

Le impostazioni della connessione Internet saranno copiate da quelle di MS Internet Explorer. Per visualizzare e/o modificare tali impostazioni, selezionare **Avvio** → **Impostazioni** → **Pannello di controllo** → **Opzioni Internet** → **Connessioni**.



Se si utilizza un collegamento Internet via server proxy, è possibile modificarne i parametri. Per poter accedere alle impostazioni del server proxy, seguire il collegamento [modificare le impostazioni del server proxy](#) (per ulteriori informazioni, cfr. paragrafo 13.5, pag. 72)

13.3. Scaricamento degli aggiornamenti da una cartella locale

Se non si ha la possibilità di accedere ai server di aggiornamento di Kaspersky Lab (per esempio se non si dispone di un accesso Internet), è possibile telefonare al nostro ufficio principale al numero +7 (095) 797-87-00 e chiedere informazioni sui partner di Kaspersky Lab in grado di fornire il database antivirus su floppy disk o CD-ROM in file compressi di formato zip.



Al momento di ordinare il database antivirus, ricordarsi di specificare il tipo di database (standard o esteso) che si desidera ricevere.

Dopo aver ricevuto il file in formato zip contenente il database antivirus, è possibile decomprimerlo e copiarlo in qualsiasi cartella del computer.



Per configurare gli aggiornamenti del database antivirus da una cartella locale:

1. Fare clic sul link [Configura aggiornamento](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4).
2. All'apertura della finestra **Impostazioni aggiornamento** (cfr la Figura 19) selezionare la voce **da una cartella locale** nell'elenco a discesa **Tipo aggiornamento**.
3. Indicare il percorso della cartella in cui era stato copiato l'archivio zip decompresso contenente il database antivirus tramite la finestra standard di Windows **Seleziona cartella locale**.
4. Fare clic su **OK**.

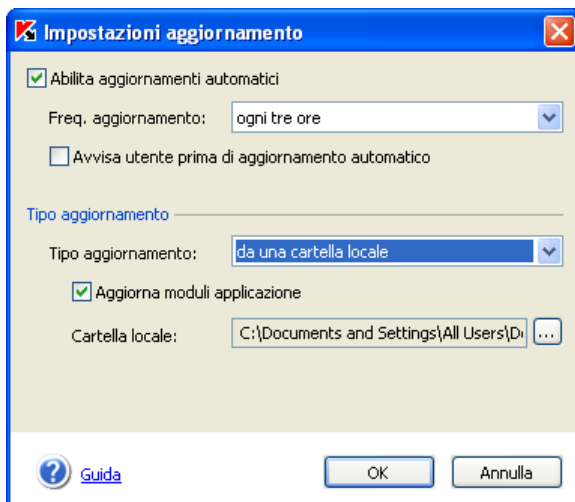


Figura 19. La finestra di dialogo **Impostazioni aggiornamento**

13.4. Aggiornamento dei moduli di Kaspersky Anti-Virus® Personal

Oltre al database antivirus è possibile aggiornare anche i moduli di Kaspersky Anti-Virus® Personal. Gli aggiornamenti dei moduli del programma vengono caricati periodicamente nei server di aggiornamento, quando necessario.

È possibile aggiornare i moduli del programma sia dai server di aggiornamento sia da una cartella locale, selezionando la casella **Aggiorna moduli applicazione** nella finestra di dialogo **Impostazioni aggiornamento** (cfr. la Figura 19).



Se si desidera aggiornare i moduli del programma da una cartella locale, al momento di ordinare il database antivirus presso il proprio rivenditore è necessario specificare che si desiderano gli aggiornamenti dei moduli.

13.5. Configurazione dei parametri del server proxy

Per impostazione predefinita, per aggiornare il database antivirus vengono utilizzate le impostazioni di connessione di Microsoft Internet Explorer. Se per la connessione Internet si utilizza un server proxy, è necessario specificarne i parametri, vale a dire l'indirizzo IP, la porta, i parametri di autenticazione, ecc.

Per configurare i parametri del server proxy, aprire la finestra di dialogo **Impostazioni server proxy** (cfr. la Figura 20).



Per aprire questa finestra agire come segue

1. Seguire il collegamento **Configura aggiorn.** nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4).
2. Nella finestra **Impostazioni aggiornamento** che si apre (cfr. la Figura 19), seguire il collegamento **modifica impostazioni server proxy** nella sezione delle informazioni.

Esistono due metodi per determinare i parametri del server proxy:



Rileva automaticamente le impostazioni del server proxy



Usa un server proxy diverso

Se il server proxy non richiede l'autenticazione, selezionare la prima opzione e i parametri saranno copiati da MS Internet Explorer.

Se, al contrario, il server proxy richiede l'autenticazione, selezionare la seconda opzione e specificare manualmente i parametri.

Protocollo – il tipo di protocollo usato per il trasferimento dei dati. Selezionare una delle opzioni dall'elenco a discesa: *http, ftp, socks4*

Indirizzo – L'indirizzo IP del server proxy in formato *aaa.bbb.ccc.ddd* o URL.

Porta – Il numero della porta su cui si trova il server proxy. Selezionare una delle opzioni dall'elenco a discesa: *3128, 8080, 8082, 8903* o inserire un valore diverso.

Se il server proxy richiede la registrazione, selezionare la casella **Usa autenticazione** e specificare il nome utente e la password nei campi di testo sottostanti. Se la rete fa uso di autenticazione NTLM, non è necessario indicare il nome utente e la password.

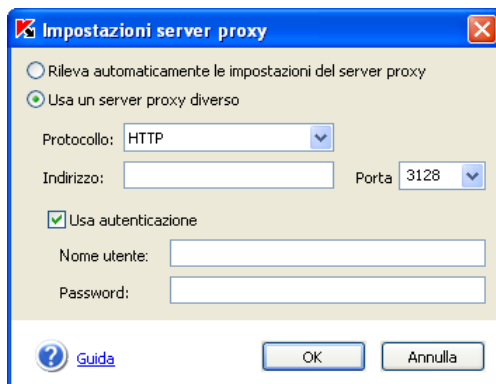


Figure 20. Impostazioni server proxy



Se erano stati programmati aggiornamenti con una certa frequenza, per esempio ogni 3 ore, e il computer è rimasto spento più a lungo dell'intervallo specificato (per esempio per 10 ore), l'aggiornamento del database antivirus sarà avviato alla prima riaccensione del computer.

13.6. Impostazioni della funzione di aggiornamento Aggiornamenti programmati

Gli esperti di Kaspersky Lab raccomandano di scaricare gli aggiornamenti ogni 3 ore; nei periodi di maggior diffusione dei virus è opportuno aggiornare il database con la massima frequenza possibile.



Per programmare gli aggiornamenti del database antivirus:

1. Fare clic sul link [Configura aggiornamento](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4).
2. All'apertura della finestra di dialogo **Impostazioni aggiornamento** (cfr. la Figura 19) selezionare la casella **Abilita aggiornamenti automatici**.
3. Selezionare la frequenza di aggiornamento desiderata dall'elenco a discesa **Freq. aggiornamento**.



Se erano stati programmati aggiornamenti con una certa frequenza, per esempio ogni 3 ore, e il computer è rimasto spento più a lungo dell'intervallo specificato (per esempio per 10 ore), l'aggiornamento del database antivirus sarà avviato alla prima riaccensione del computer.

13.7. Aggiornamenti manuali.

Scaricamento degli aggiornamenti



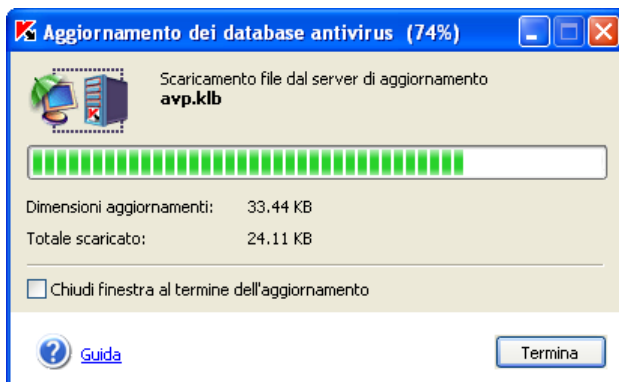
Per scaricare gli aggiornamenti del database antivirus:

fare clic su [Aggiorna ora](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3) o su un ipertesto nel messaggio relativo alla necessità di aggiornare il database antivirus nella sezione destra della scheda **Protezione**.

Il programma può avviare lo scaricamento manuale o programmato degli aggiornamenti solo se il computer è connesso a Internet. Se la connessione Internet non è disponibile, il programma non può avviare il processo di aggiornamento.

Il processo di scaricamento degli aggiornamenti si compone delle seguenti fasi:

1. Il programma riceve un elenco degli aggiornamenti disponibili dal server dedicato di Kaspersky Lab con le rispettive dimensioni.
2. Kaspersky Anti-Virus® Personal pone quindi a confronto il database antivirus e i moduli del programma installati sul computer con i dati prelevati dal server. Se il database antivirus installato sul computer è il più recente disponibile, viene visualizzato un messaggio che conferma che il database di cui si dispone è aggiornato.
3. Nel campo **Dimensioni aggiornamenti** della finestra di dialogo **Aggiornamento** (cfr. la Figura 21), è possibile visualizzare le dimensioni totali degli aggiornamenti necessari. Se l'aggiornamento non è necessario il processo viene interrotto. In caso contrario, il programma inizia a copiare i file dal server di aggiornamento di Kaspersky Lab. Il processo di scaricamento viene visualizzato dalla barra di avanzamento, e il campo **Totale scaricato** indica le dimensioni in kilobyte degli aggiornamenti scaricati. Al completamento di questa fase, il database antivirus viene automaticamente installato sul computer.

Figura 21. La finestra di dialogo **Aggiornamento**

CAPITOLO 14. IMPOSTAZIONI SUPPLEMENTARI

Kaspersky Anti-Virus® Personal offre numerose opzioni supplementari per configurare e usare il prodotto:

- Configurazione dei parametri di protezione in tempo reale e scansione completa del computer.
- Gestione degli oggetti in quarantena.
- Report analitici sulle prestazioni del programma.
- Impostazioni supplementari.

Questo capitolo contiene una descrizione dettagliata di ciascuna di tali opzioni.

14.1. Configurazione della protezione in tempo reale

Per impostazione predefinita, la protezione in tempo reale del computer applica le impostazioni raccomandate dagli esperti di Kaspersky Lab. Oltre ad offrire la possibilità di modificare i principali parametri della protezione in tempo reale (cfr. Capitolo 8, pag. 53), Kaspersky Anti-Virus® Personal consente di configurare ulteriori parametri di protezione, in particolare di escludere determinati gruppi di oggetti dalla protezione in tempo reale. È possibile disattivare parzialmente la protezione in tempo reale o disabilitarla del tutto. Tali esclusioni consentono di ridurre il numero totale dei file esaminati durante la protezione in tempo reale. Per esempio, è possibile disabilitare la scansione della posta elettronica o di file di script e ridurre a secondi il tempo massimo di scansione di un oggetto.



I parametri supplementari sono applicabili a tutti i livelli di protezione in tempo reale (**Massima protezione, Raccomandato e Alta velocità**).

Questi parametri di protezione in tempo reale sono accessibili dalla finestra di dialogo **Individuazione errori** (cfr. la Figura 22). Per aprire questa finestra, fare clic su [Individuazione errori](#) nella finestra di dialogo **Configura protezione in tempo reale** (cfr. la Figura 14).

Per escludere determinati tipi di file o cartelle specifiche dalla scansione, selezionare la casella **Abilita elenco oggetti esclusi** e fare clic su **Modifica**.

Per definire le esclusioni, indicare il percorso ai file selezionati oppure specificarne l'estensione mediante una maschera (per esempio, *.bmp).

Ecco alcuni esempi di maschere di esclusione:

- Maschere utilizzate senza specificare il percorso:
 - *.exe – tutti i file con estensione exe
 - *.ex? – tutti i file con estensione ex?, in cui "?" è un carattere jolly che può rappresentare qualsiasi carattere singolo
 - test – tutti i file di nome test
- Maschere utilizzate specificando percorsi assoluti:
 - C:\dir*. – tutti i file contenuti nella cartella C:\dir\
 - C:\dir*.exe – tutti i file con estensione exe contenuti nella cartella C:\dir\
 - C:\dir*.ex? – tutti i file con estensione ex? contenuti nella cartella C:\dir\, in cui "?" è un carattere jolly che può rappresentare qualsiasi carattere singolo
 - C:\dir\test – solo il file C:\dir\test
 - C:\dir\ – tutti i file contenuti nella cartella C:\dir\ e nelle sue sottocartelle
- Maschere utilizzate specificando percorsi relativi:
 - dir*. – tutti i file contenuti in tutte le cartelle in dir\
 - dir\test – tutti i file di nome test nelle cartelle in dir\
 - dir*.exe – tutti i file con estensione exe nelle cartelle in dir\
 - dir*.ex? – tutti i file con estensione ex? contenuti in tutte le cartelle in dir\, in cui "?" è un carattere jolly che può rappresentare qualsiasi carattere singolo
 - dir\ – tutti i file in tutte le cartelle in dir\ e nelle sue sottocartelle



Le maschere *.* e * non sono valide senza l'indicazione di un percorso.

All'apertura della finestra **Esclusioni** (cfr. la Figura 23), modificare l'elenco delle esclusioni per mezzo dei pulsanti **Aggiungi**, **Modifica** e **Rimuovi**. Dopo aver modificato l'elenco delle esclusioni fare clic su **OK**. L'elenco modificato è applicato immediatamente.

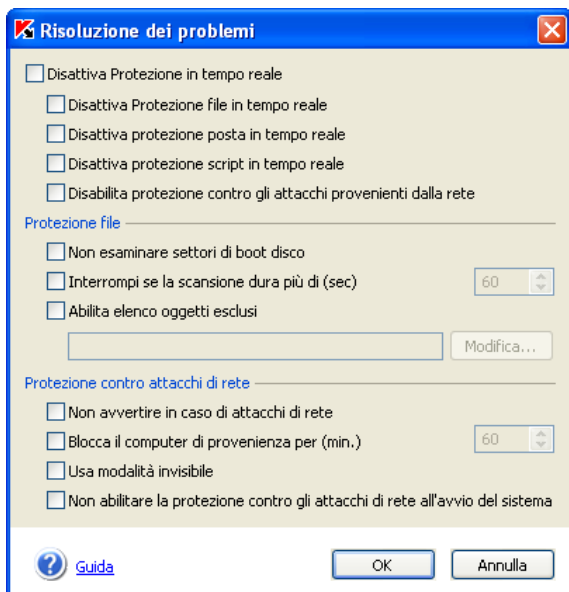


Figura 22. Individuazione errori

Kaspersky Anti-Virus® Personal consente di applicare in qualsiasi momento le impostazioni raccomandate, ignorando le impostazioni personalizzate.

Per ripristinare le impostazioni di protezione in tempo reale raccomandate, fare clic su [Sono applicate le impostazioni di protezione in tempo reale raccomandate](#) (cfr la Figura 24) nella sezione destra della scheda **Impostazioni** della finestra principale dell'applicazione.

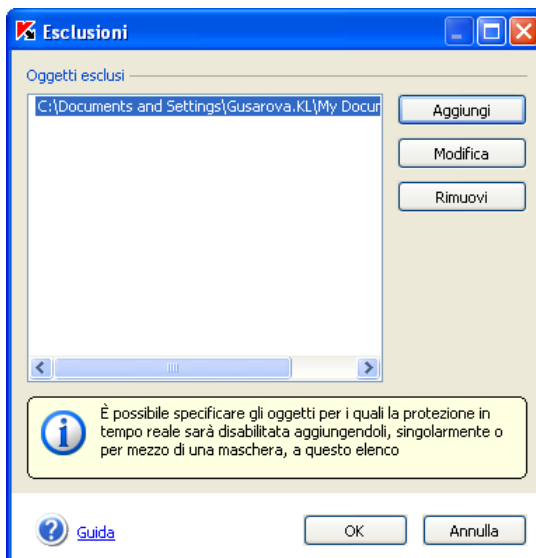


Figura 23. Definizione delle esclusioni dalla protezione in tempo reale



Sono applicate impostazioni di protezione in tempo reale raccomandate.

In caso di rilevamento virus, bloccare accesso, chiedere intervento utente.
Livello di protezione: Raccomandato.

È possibile [modificare le impostazioni della protezione in tempo reale](#).

Figura 24. Informazioni sullo status della protezione in tempo reale

14.2. Configurazione della protezione contro gli attacchi provenienti dalla rete

La protezione contro gli attacchi provenienti dalla rete è uno dei componenti della protezione in tempo reale. I suoi parametri sono disponibili nella finestra di dialogo **Individuazione errori** (cfr. la Figura 22).

Da questa finestra è possibile abilitare e disabilitare la protezione contro gli attacchi provenienti dalla rete e configurare ulteriori parametri:

Avvisi sugli attacchi provenienti dalla rete. Per impostazione predefinita, il programma informa l'utente ogni volta che viene perpetrato un tentativo di attacco al computer. Viene visualizzato un messaggio (cfr. la Figura 15) contenente informazioni sul tipo di attacco perpetrato, l'indirizzo IP del computer di provenienza dell'attacco e la porta locale (se possibile determinarla). Poiché questo avviso svolge unicamente una funzione di riferimento, è possibile disabilitarne la visualizzazione selezionando la casella **Non avvertire in caso di attacchi di rete.**

Blocco del computer di provenienza dell'attacco. Kaspersky Anti-Virus blocca tutti i computer che tentano di attaccare la macchina protetta. Per impostazione predefinita, il computer di provenienza dell'attacco viene bloccato per 60 minuti. In questo periodo tale computer non è in grado di stabilire una connessione di rete con il computer protetto. Per modificare il periodo di blocco, specificare il valore desiderato nel parametro **Blocca il computer di provenienza per (min.)**. Per disabilitare la modalità di blocco, deselegionare la casella di controllo a fianco di questo parametro.

Modalità Invisibile. Questa modalità permette solo le attività di rete iniziate dall'utente; qualsiasi altra azione (connessione remota al computer, ecc.) non saranno consentite. Ciò significa che il computer diventa virtualmente "invisibile" agli altri. La modalità Invisibile consente inoltre di prevenire qualsiasi tipo di attacco DoS (Denial of Service). Al tempo stesso, la modalità Invisibile non ha alcun impatto negativo sulle attività di navigazione Internet del computer protetto, in quanto Kaspersky Anti-Virus consente qualsiasi attività iniziata dall'utente.



Attenzione! La modalità Invisibile non protegge il computer contro i programmi dannosi tipo cavalli di Troia!

Per impostazione predefinita, la modalità Invisibile è abilitata. Per disabilitarla, deselegionare la casella **Usa modalità Invisibile.**

14.3. Configurazione dei parametri di scansione manuale

Per impostazione predefinita, Kaspersky Anti-Virus® Personal sottopone a scansione manuale tutti gli oggetti memorizzati nel disco fisso (cfr. il Capitolo 3, pag. 18) in base alle impostazioni raccomandate dagli esperti di Kaspersky Lab.

Oltre a selezionare il livello di protezione antivirus e a personalizzare le azioni del programma in caso di rilevamento di oggetti infetti (cfr. la sezione 8.2, pag. 53), è possibile, come per la protezione in tempo reale, configurare parametri

supplementari per tutti i livelli, in modo da ridurre il numero di oggetti da esaminare.



È possibile configurare ulteriori parametri di scansione per tutti i livelli di protezione in tempo reale (**Massima protezione, Raccomandato e Alta velocità**).

Questi parametri di scansione sono accessibili dalla finestra di dialogo **Individuazione errori** (cfr. la Figura 25). Per aprire questa finestra, fare clic su [Individuazione errori](#) nella finestra di dialogo **Impostazioni scansione manuale** (cfr. la Figura 8).

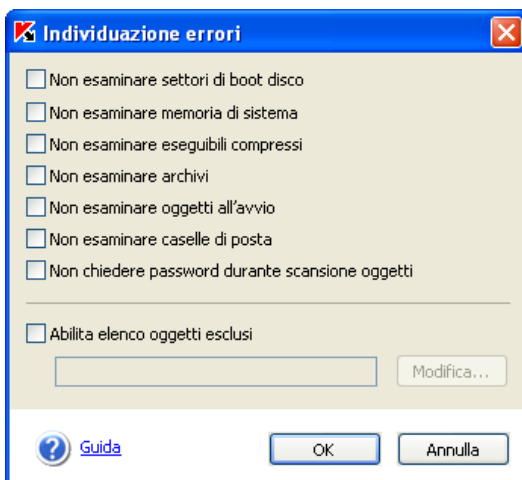


Figura 25. Definizione delle esclusioni dalla scansione manuale

Da questa finestra è possibile escludere oggetti dalla scansione associandoli agli indicatori corrispondenti, oppure selezionare cartelle o file (per mezzo delle apposite maschere) da escludere dalla scansione con un processo analogo a quello seguito per definire le esclusioni dalla protezione in tempo reale (cfr. la sezione 14.1, pag. 76).



Si raccomanda di non escludere i dischi logici con i sistemi di file creati con il comando *subst*. Una simile operazione non avrebbe alcun effetto poiché Kaspersky Anti-Virus® Personal riconosce il disco logico come cartella e di conseguenza la sottopone a scansione.

Per ripristinare le impostazioni raccomandate per qualsiasi livello, fare clic su [Sono applicate le impostazioni di protezione in tempo reale raccomandate](#) nella sezione destra della scheda **Impostazioni** (cfr. la Figura 4) o nei commenti sullo status della protezione in tempo reale nella scheda **Protezione**.

14.4. Gestione degli oggetti in quarantena

Un analizzatore euristico di codici, in grado di rilevare fino al 92% dei nuovi virus, stabilisce se un file è sospetto in termini di possibile presenza di virus. Si tratta di un meccanismo estremamente efficace ma che, talvolta, determina dei falsi positivi. È tuttavia possibile stabilire se un file è effettivamente infetto da un nuovo virus non ancora registrato nel database antivirus o se si tratta semplicemente di un falso allarme del programma.

Durante la scansione integrale del computer o di dischi o file specifici e in modalità di protezione in tempo reale, Kaspersky Anti-Virus® Personal mette in quarantena tutti gli oggetti probabilmente infetti da virus o varianti di virus. In seguito è possibile intraprendere vari tipi di azione (scansione, recupero, eliminazione ecc.) nei confronti degli oggetti isolati. I file in quarantena vengono memorizzati in un formato speciale e non costituiscono pericolo.

Si raccomanda di aggiornare il database antivirus prima di esaminare i file in quarantena. È possibile infatti che nel frattempo il database sia stato aggiornato con le informazioni relative ai virus di cui si sospetta la presenza in tali file, consentendone in tal modo la riparazione.

È possibile gestire i file probabilmente infetti dalla finestra **Quarantena** (cfr. la Figura 26), accessibile facendo clic su [Vis. quarantena](#) nella scheda **Protezione** (cfr. la Figura 3) della finestra principale dell'applicazione, oppure facendo clic sul collegamento [Vis. quarantena](#) nella finestra **Scansione** (cfr. la Figura 6).

Dalla finestra **Quarantena** è possibile eseguire le seguenti azioni:

- Mettere in quarantena un file che si sospetta attaccato da un virus non rilevato da Kaspersky Anti-Virus® Personal. Per mettere in quarantena un file, fare clic su [Aggiungi](#) e selezionare il file sospetto nella finestra standard di selezione file. Il file viene aggiunto all'elenco con lo status *Isolato dall'utente*.
- Esaminare e riparare tutti i file sospetti o solo quelli selezionati nell'elenco utilizzando il database antivirus corrente. Per far ciò, fare clic su [Esamina tutto](#) o [Esamina](#) dopo aver selezionato i file da esaminare.

Dopo la scansione e l'eventuale riparazione di un oggetto in quarantena, il suo status può cambiare in *infetto*, *falso allarme*, *non infetto*, ecc. In questo caso si apre un messaggio contenente alcuni consigli su come gestire il file in questione.

Lo status *infetto* significa che l'oggetto è stato riconosciuto come infetto ma non è stato possibile ripararlo. Si raccomanda di eliminare gli oggetti appartenenti a questa categoria.

Tutti gli oggetti identificati dallo status *falso allarme* possono essere ripristinati in tutta sicurezza in quanto il precedente status *probabilmente infetto* era stato erroneamente assegnato da Kaspersky Anti-Virus® Personal.

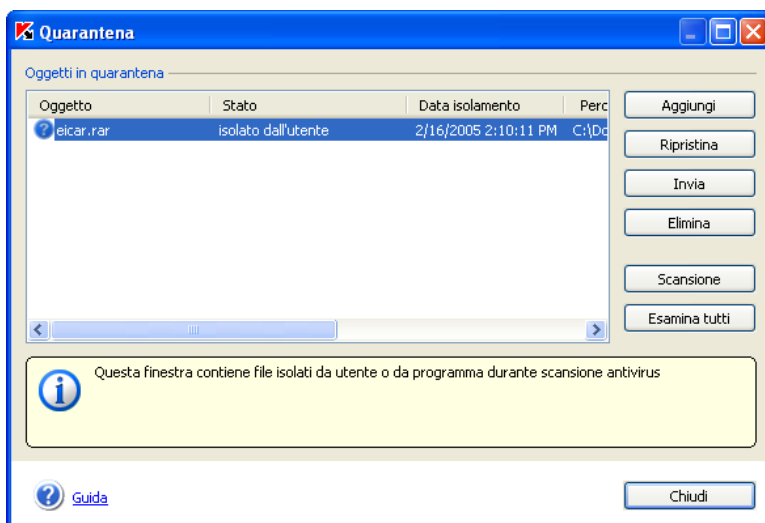


Figura 26. Quarantena di file sospetti

- Ripristinare file dalla cartella della quarantena nelle cartelle originarie da cui erano stati trasferiti. Per ripristinare un oggetto, selezionarlo nell'elenco e fare clic sul pulsante **Ripristina**. Durante il ripristino di oggetti messi in quarantena da archivi, database di posta elettronica e file di formato posta, è necessario specificare la cartella in cui si desidera trasferirli.



Si raccomanda di ripristinare solo gli oggetti identificati dagli status *falso allarme*, *non infetto* o *disinfettato* poiché il ripristino di altri oggetti può provocare l'infezione del computer!

- Inviare gli oggetti probabilmente infetti a Kaspersky Lab per farli analizzare. Si raccomanda di inviare solo gli oggetti che hanno conservato lo status *probabilmente infetto* dopo numerosi tentativi di scansione e riparazione. Per inviare un file a Kaspersky Lab, fare clic su [Invia](#) (per ulteriori informazioni cfr. l'Appendice A, pag. 96).



Osservare che ogni file inviato a Kaspersky Lab per un'analisi deve essere stato esaminato con Kaspersky Anti-Virus® Personal con un database aggiornato non prima del giorno precedente l'invio.

- Eliminare oggetti o gruppi selezionati di oggetti in quarantena. Eliminare solo i file che non possono essere riparati. Per eliminare tali file, selezionarli nell'elenco e fare clic sul pulsante **Elimina**.

14.5. Gestione di copie di backup di oggetti

La backup è una speciale area utilizzata per la conservazione di copie di backup di oggetti. Le copie di backup vengono eseguite la prima volta che si cerca di riparare o eliminare un oggetto. La funzione principale della backup consiste nel conservare tali copie in modo da consentire in qualsiasi momento il ripristino dell'oggetto iniziale.

È possibile gestire le copie di backup tramite una finestra di dialogo **Backup** (cfr. la Figure 27). Per accedere a tale finestra, seguire il collegamento [Visualizza backup](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3).

La sezione centrale della finestra contiene l'elenco delle copie di backup. Per ogni copia sono fornite le seguenti informazioni: nome dell'oggetto per il quale è stata creata la copia, stato dell'oggetto, data di creazione della copia e percorso completo dell'oggetto iniziale.

Per ripristinare o eliminare una o più copie infette, utilizzare i pulsanti corrispondenti sul lato destro dell'elenco.

L'oggetto viene ripristinato dalla copia di backup con il nome originario.

Se nella posizione iniziale si trova un oggetto con lo stesso nome (ciò è possibile nel caso in cui si sia ripristinato un oggetto precedentemente copiato e riparato), viene visualizzato un apposito avviso. È possibile quindi salvare l'oggetto ripristinato in una posizione diversa oppure rinominarlo.

Quando è possibile ripristinare le copie di backup in tutta sicurezza?

Quando un oggetto viene riparato, talvolta la sua integrità viene compromessa. Se l'oggetto riparato conteneva informazioni importanti rese totalmente o parzialmente inutilizzabili in seguito all'operazione, è possibile tentare di ripristinare l'oggetto iniziale dalla copia di backup. Si raccomanda in tal caso di analizzare immediatamente tale oggetto subito dopo il ripristino per escludere la presenza di virus, poiché esso può essere riparato con successo e senza perdita di dati utilizzando un database antivirus aggiornato.



Si sconsiglia di ripristinare oggetti dalle copie di backup se non strettamente necessario, poiché tale operazione può provocare un'infezione del computer.

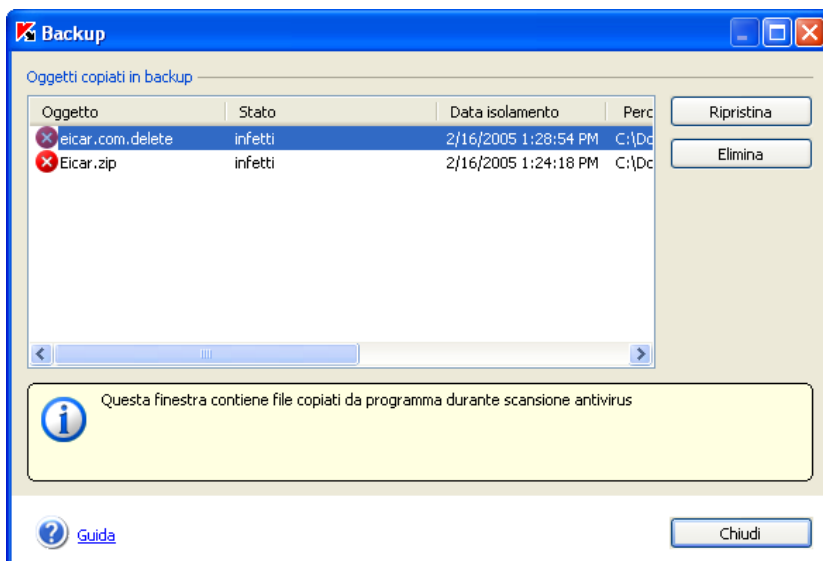


Figure 27. Backup

Per impostazione predefinita, il periodo di conservazione delle copie di backup e le dimensioni massime dell'area di memorizzazione non sono limitati. Si raccomanda di esaminare e pulire periodicamente l'area di backup. È inoltre possibile impostare il programma in modo da rimuovere automaticamente le copie più obsolete e avvertire l'utente dell'eccesso di copie memorizzate (per ulteriori informazioni cfr. il paragrafo 14.6 a pag. 85).

14.6. Impostazioni supplementari per la quarantena e la backup

Le impostazioni per la creazione e l'uso della quarantena e dello spazio di backup possono essere personalizzate. Per configurare le impostazioni della quarantena, fare clic su [Configura Quarantena&Backup](#) nella scheda **Impostazioni** (cfr. la Figura 4) della finestra principale dell'applicazione e modificare i seguenti parametri (cfr. la Figura 28) nella finestra che si apre:

- ✓ **Esamina automaticamente oggetti isolati ad ogni aggiornamento del database antivirus.** Questa modalità consente di eseguire la scansione automatica degli oggetti in quarantena ogni volta che il database antivirus viene aggiornato, senza richiedere l'intervento dell'utente.



Kaspersky Anti-Virus® non è in grado di esaminare gli oggetti in quarantena immediatamente dopo l'aggiornamento del database antivirus se, al momento dell'aggiornamento, si stava lavorando con la quarantena.

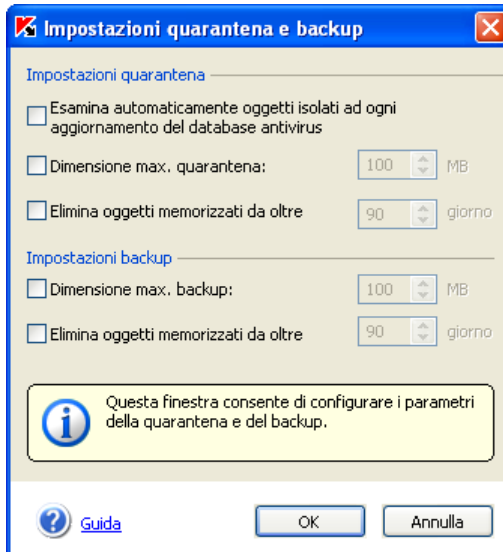


Figura 28. Impostazioni quarantena e backup

- ✓ **Dimensione max. quarantena ... MB.** Per impostazione predefinita, le dimensioni della quarantena non sono limitate (la casella corrispondente non è selezionata). Se si desidera impostare una restrizione sulle dimensioni totali dei file in quarantena, selezionare la casella e indicare le dimensioni servendosi delle frecce del pulsante di selezione verticale corrispondente (il valore predefinito è 100 MB). Se le dimensioni massime della quarantena vengono superate, il programma avvisa l'utente con un messaggio.
- ✓ **Elimina oggetti memorizzati da oltre ... giorno.** Per impostazione predefinita, i file in quarantena possono essere conservati per un periodo di tempo indefinito. Per limitare tale periodo, selezionare la casella corrispondente e indicare il numero dei giorni nella casella del pulsante di selezione verticale corrispondente (il valore predefinito è 90 giorni).

Le dimensioni massime dello spazio di backup e la durata del periodo di conservazione delle copie memorizzate sono analoghe ai parametri corrispondenti della quarantena.

14.7. Uso dei report

Durante la scansione del computer o di oggetti selezionati, l'aggiornamento del database antivirus o la protezione in tempo reale, il programma redige report contenenti le informazioni relative agli oggetti esaminati, i risultati dell'elaborazione e i dati statistici generali.

L'elenco completo delle attività eseguite da Kaspersky Anti-Virus® Personal può essere visualizzato nella finestra **Report** (cfr. la Figura 29). Per aprire questa finestra, fare clic su [Visualizza report](#) nella sezione sinistra della scheda **Protezione** (cfr. la Figura 3). Nei report viene registrato lo stato delle attività e la data e l'ora di completamento di ciascuna di esse.

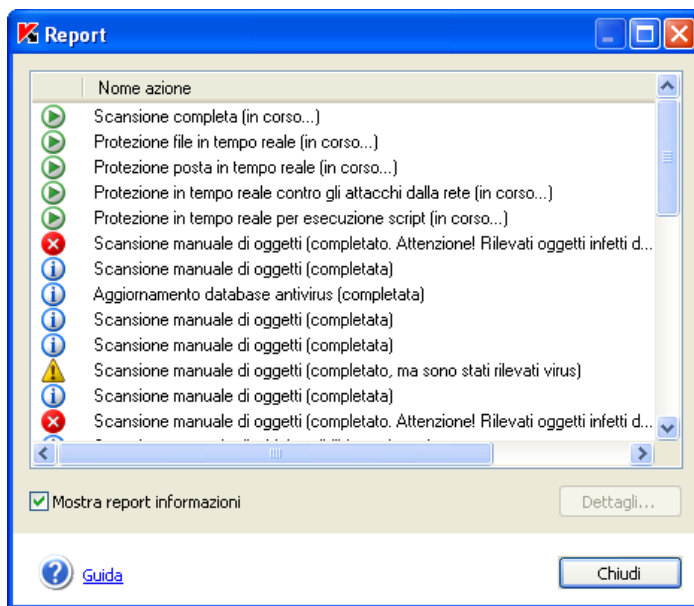







Figura 29. Report

Alle diverse attività possono essere assegnati i seguenti tipi di report:

 o  – Report informativi (per esempio: attività avviata, attività completata, attività in corso, attività sospesa).

 – Attenzione (per esempio, Attenzione! Rimangono oggetti non esaminati).

 – Nota (per esempio, l'attività è stata interrotta).

Normalmente i messaggi di informazione servono solo come riferimento e non rivestono interesse particolare. La visualizzazione dei messaggi informativi può essere disabilitata deselegnando la casella  **Mostra report informazioni**.

È inoltre possibile ordinare i report per tipo, titolo (in ordine alfabetico) e per ora di completamento dell'attività. Per poter organizzare i report secondo una delle colonne di cui sopra, fare clic sull'intestazione della colonna corrispondente.

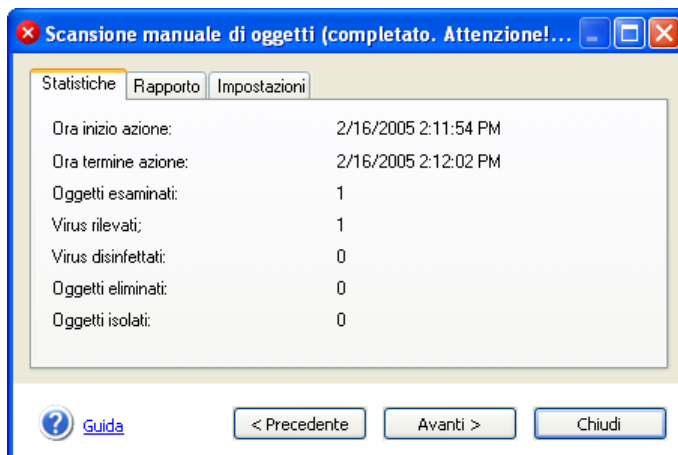
Per visualizzare nelle rispettive schede le impostazioni di una specifica attività elencata nel registro, le statistiche e il report sui risultati dell'attività, fare clic sul pulsante **Dettagli** dopo avere selezionato l'attività che si desidera visualizzare, oppure fare doppio clic sull'attività.

Nelle schede **Statistiche**, **Rapporto** e **Impostazioni** si aprirà una nuova finestra contenente un report dettagliato sull'attività.

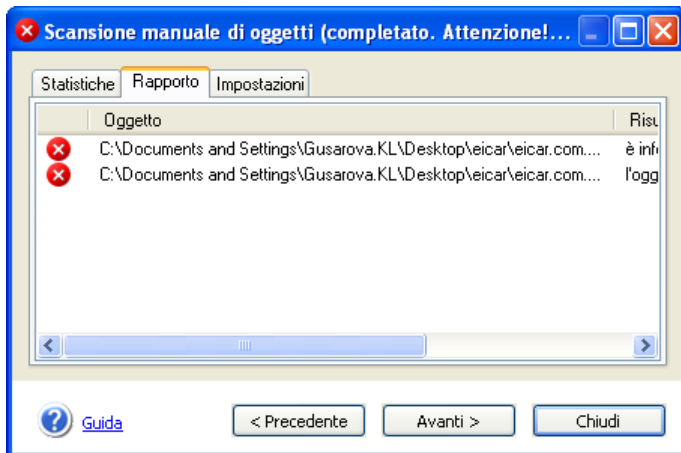


Durante la scansione completa, è possibile monitorare le prestazioni dell'attività nelle apposite schede (cfr. Figura 6).

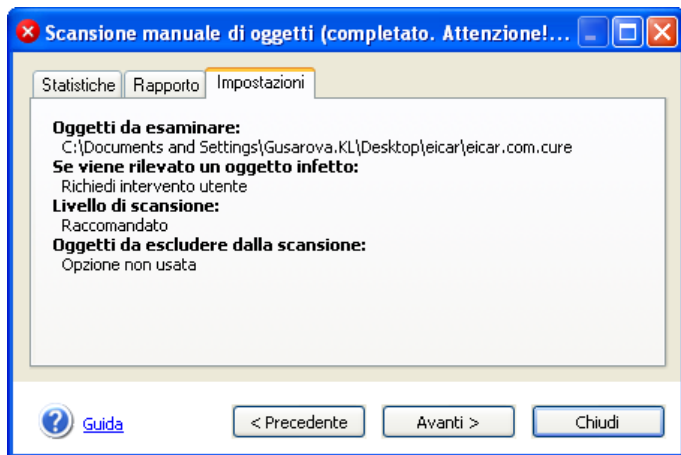
La scheda **Statistiche** visualizza le informazioni generali per ogni attività eseguita da Kaspersky Anti-Virus® Personal, compresi data e ora di avvio dell'attività, numero totale di file analizzati e numero di oggetti infetti, riparati e in quarantena (cfr. la Figura 30). Per l'attività di aggiornamento, la scheda visualizzerà la dimensione totale dei file aggiornati all'origine (server di aggiornamento di Kaspersky Lab, cartella locale) e la dimensione totale dei file scaricati sul computer.

Figura 30. La scheda **Statistiche**

Per impostazione predefinita, la scheda **Rapporto** (cfr. la Figura 31) non contiene informazioni sugli oggetti riparati ma visualizza solo le informazioni relative ai virus rilevati. Per visualizzare tutte le informazioni, selezionare la casella **Registra tutti i messaggi** nella finestra **Impostazioni supplementari** di Kaspersky Anti-Virus® Personal (cfr. la sezione 14.8, pag. 93). In questo modo la scheda **Rapporto** conterrà le informazioni su ogni oggetto esaminato. Per l'attività di aggiornamento, la scheda visualizzerà le informazioni relative a ciascun passaggio: collegamento con i server di aggiornamento, file scaricati, informazioni sull'installazione. Per questa attività, le informazioni saranno sempre visualizzate, indipendentemente dalla selezione della casella **Registra tutti i messaggi** nella finestra **Impostazioni supplementari**.

Figura 31. La scheda **Rapporto**

Nella scheda **Impostazioni** (cfr. la Figura 32) sono visualizzati i parametri utilizzati dall'attività, compresi gli oggetti sottoposti a scansione, il livello di protezione impostato per l'attività e le azioni che il programma deve eseguire sugli oggetti infetti, i programmi dannosi e i file sospetti. Queste informazioni comprendono anche l'elenco degli elementi esclusi dalla scansione, se tali esclusioni sono state specificate. Per l'attività di aggiornamento, sono visualizzati i seguenti dati: tipo di aggiornamento e origine dell'aggiornamento.

Figura 32. La scheda **Impostazioni**

Utilizzando i pulsanti **Avanti** > e < **Indietro**, oppure selezionando il nome dell'attività dal corrispondente elenco a discesa, le attività potranno essere visualizzate nelle finestre dei **Rapporto** o nella finestra di dialogo del report dettagliato delle attività.

14.7.1. Visualizzazione delle informazioni nei report

Kaspersky Anti-Virus® Personal permette di scegliere le informazioni che saranno visualizzate nel report. È possibile configurare il programma in modo da visualizzare solo le informazioni importanti, mentre i messaggi di informazione e gli altri messaggi di riferimento saranno esclusi.

Se si desidera memorizzare nei report tutti i messaggi, selezionare la casella **Registra tutti i messaggi** nella finestra **Impostazioni supplementari** (cfr. la sezione 14.8, pag. 93). Sarà possibile visualizzare tutti i messaggi quando, per esempio, si avvia una scansione completa del computer nella finestra **Scansione** (cfr. la Figura 6) nella scheda **Rapporto**.

Se la casella **Registra tutti i messaggi** è selezionata, tutte le informazioni sulla scansione saranno registrate nel report, compresi i messaggi relativi alla corretta esecuzione della scansione.

Se la casella non è selezionata, saranno visualizzate solo le informazioni importanti, per esempio i messaggi di errore relativi alla mancata scansione di un oggetto. I messaggi sulle scansioni correttamente eseguite non saranno visualizzati.



*Per disabilitare la visualizzazione dei messaggi di informazione all'interno della sessione corrente senza deselegionare la casella **Registra tutti i messaggi**,*

fare clic con il pulsante destro del mouse sulla finestra, durante la visualizzazione dei report nella scheda **Rapporto**, per aprire il menu di scelta rapida (cfr. la Figura 33) e deselegionare l'indicatore **Mostra report dettagliato**.

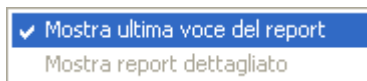


Figura 33. Menu di scelta rapida – scheda **Rapporto**



Se la casella **Registra tutti i messaggi** nella finestra **Impostazioni supplementari** è deselezionata, anche l'opzione **Mostra report dettagliato** nel menu contestuale sarà deselezionata e la funzione non potrà essere configurata.

Per impostazione predefinita, quando si visualizza il report in modalità di monitoraggio (cioè durante una scansione, nella scheda **Rapporto**), sarà sempre visualizzata l'ultima voce del report. Per disabilitare questa modalità, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida e deselezionare la casella **Mostra ultima voce del report** oppure selezionare una voce nel report.

14.7.2. Esportazione e invio dei report

Kaspersky Anti-Virus® Personal permette di modificare l'elenco dei report creati in base ai risultati delle diverse attività. È possibile accedere alle opzioni di modifica disponibili dal menu contestuale (cfr. la Figura 34), accessibile facendo clic con il pulsante destro del mouse sulla finestra **Report** (cfr. la Figura 29).



Figura 34. Comandi di scelta rapida utilizzati per la gestione dei report

Il base al tipo di report specifico (i tipi sono Attenzione, Nota e Messaggio), alcune opzioni del menu di scelta rapida potrebbero non essere disponibili. Ciò è vero per l'opzione che permette di esportare un report in un file ed inviarlo a Kaspersky Lab, disponibile solo per i report *Attenzione* (relativi, per esempio, alle attività che sono terminate con un errore). Si noti inoltre che non è possibile eliminare un report mentre l'azione al quale si riferisce è in corso.

Inoltre, la funzione di esportazione di report dettagliati su file consente di visualizzare le informazioni come tabella di MS Excel.

Se una qualsiasi attività (per esempio la scansione del computer o l'aggiornamento del database antivirus) viene inspiegabilmente interrotta o provoca un errore di cui non si conosce l'origine, è possibile inviare un report di tale attività a Kaspersky Lab.

A tale proposito, aprire la finestra **Report**, selezionare il report che si desidera inviare facendo clic con il pulsante destro del mouse e scegliere l'opzione **Invia report a Kaspersky Lab** nel menu di scelta rapida. Si apre una nuova finestra del client di posta elettronica utilizzato (per esempio Microsoft Outlook Express)

con un messaggio a cui è allegato il file del report. Inviare questo messaggio e gli esperti di Kaspersky Lab cercheranno di fornire una risposta nel più breve tempo possibile.



I messaggi di posta elettronica vengono creati automaticamente solo se i client utilizzati sono Microsoft Outlook o Microsoft Outlook Express. Se si dispone di un programma diverso (per esempio The Bat!), la creazione automatica dei messaggi è supportata solo configurando il Simple MAPI del programma.

14.8. Impostazioni supplementari di Kaspersky Anti-Virus® Personal

Oltre a configurare le impostazioni per attività specifiche, Kaspersky Anti-Virus® Personal permette la configurazione di alcuni parametri generali e di assistenza (cfr. la Figura 35). A tal fine, è sufficiente selezionare il collegamento [Impostazioni supplementari](#) nella sezione sinistra della scheda **Impostazioni** (cfr. la Figura 4) e modificare le impostazioni come necessario:

- Visualizza messaggi a comparsa** – permette di visualizzare tutti i suggerimenti a comparsa che accompagnano le operazioni di Kaspersky Anti-Virus® Personal. Si raccomanda di non disabilitare questa funzione, poiché il programma opera spesso in una modalità interattiva che richiede una continua risposta dell'utente nel corso dell'elaborazione.
- Abilita avvisi acustici** – permette di accompagnare con effetti sonori la visualizzazione di messaggi durante l'uso di Kaspersky Anti-Virus® Personal. Per modificare il gruppo di file audio impiegato per tali avvisi, aprire **Avvio** → **Impostazioni** → **Pannello di controllo** → **Suoni e multimedia** → **Suoni**).
- Avvisa utente dell'annullamento della scansione** – visualizza la richiesta di conferma dell'annullamento della scansione manuale. Dopo l'annullamento della scansione, viene visualizzato un messaggio sull'icona del programma nella barra delle applicazioni, che spiega i motivi per cui la scansione è stata interrotta.
- Registra tutti i messaggi** – permette di registrare nei rapporti tutti i messaggi creati durante le operazioni del programma (messaggi di informazione, messaggi d'errore, ecc.). Per impostazione predefinita, questa funzione è disabilitata, e nel report figureranno solo i messaggi più importanti, come gli errori durante l'esecuzione di un'attività, le interruzioni di un'attività, ecc.
- Non memorizzare report più lunghi di ... giorno** – per impostazione predefinita, i report sono conservati per trenta giorni. È possibile modificare questo periodo inserendo un valore diverso nel campo a

destra, o rimuovere questa limitazione deselegionando la casella corrispondente. Durante il caricamento dell'antivirus viene eseguito un controllo dei report, in seguito al quale vengono eliminati quelli che risultano conservati per un periodo più lungo di quello specificato.



Lancia Kaspersky Anti-Virus Personal all'avvio del sistema – permette il caricamento automatico di Kaspersky Anti-Virus® Personal dopo aver riavviato il sistema operativo.



Si raccomanda vivamente di non disabilitare il caricamento automatico di Kaspersky Anti-Virus® Personal perché ciò aumenta il rischio di infezioni a carico del computer.

Non è possibile modificare quest'impostazione se non si dispone dei diritti di Amministratore per la macchina.



Avvisa utente del caricamento/scaricamento antivirus – visualizza una richiesta di conferma dell'avvio/uscita da Kaspersky Anti-Virus Personal.



Usa password per protezione applicazione – abilita la richiesta di password alla chiusura dell'applicazione principale e al tentativo di disabilitare la protezione in tempo reale. Si raccomanda di abilitare questa opzione quando il computer è accessibile ad altri utenti se non si desidera che essi modifichino le impostazioni dell'antivirus, svolgano attività con Kaspersky Anti-Virus® Personal o impieghino questo programma per qualsiasi altro scopo. Dopo aver abilitato questa opzione, inserire nell'apposito campo una **Password** alfanumerica di lunghezza compresa tra 1 e 32 caratteri, quindi digitarla nuovamente nel campo **Conferma password**.

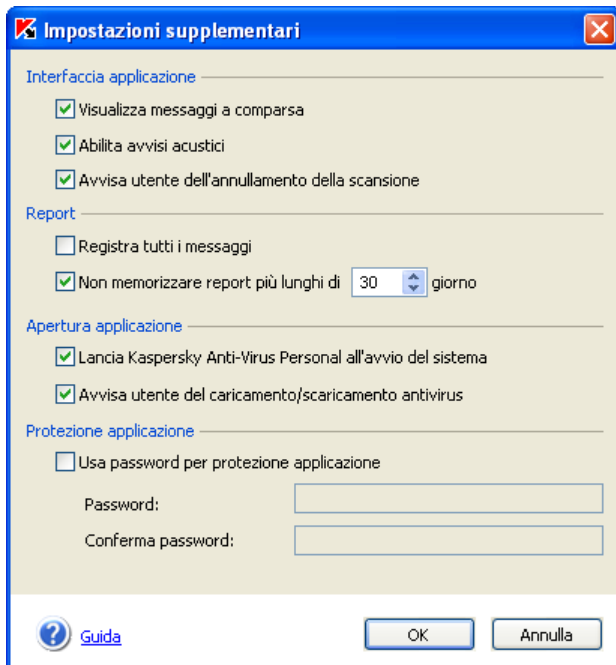


Figura 35. Impostazioni supplementari di Kaspersky Anti-Virus Personal

APPENDICE A. COME CONTATTARE L'ASSISTENZA TECNICA

Il servizio di assistenza tecnica di Kaspersky Lab è accessibile a tutti gli utenti registrati di Kaspersky Anti-Virus® Personal nei seguenti casi:

- Se il programma sembra lavorare in maniera impropria e si verificano frequenti errori.
- Se Kaspersky Anti-Virus® Personal individua un file, contenente dati critici, probabilmente infetto da un virus o da una sua variante, e il programma nega l'accesso a tale file. Se è necessario continuare a lavorare su tale file.



Per inviare un messaggio al servizio di assistenza tecnica di Kaspersky Lab relativo a qualsiasi problema riscontrato durante l'utilizzo del programma:

fare clic su [Invia domanda ad assistenza tecnica](#) nella sezione sinistra della scheda **Assistenza** (cfr. la Figura 5) della finestra principale dell'applicazione.

Il programma crea automaticamente un nuovo messaggio utilizzando il programma di posta elettronica presente sul computer, per esempio Microsoft Outlook. Tale messaggio conterrà in allegato un file di testo contenente una descrizione del sistema e tutti i dati necessari relativi alla copia di Kaspersky Anti-Virus® Personal installata. Fornire quindi una descrizione dettagliata dei problemi riscontrati nell'uso del programma e inviare il messaggio. I nostri consulenti tecnici cercheranno di rispondere a ogni domanda nel più breve tempo possibile.

Se Kaspersky Anti-Virus® Personal mette in quarantena un file probabilmente infetto, è consigliabile aggiornare il database antivirus e provare a riparare l'oggetti (per ulteriori informazioni cfr. la sezione 14.4, pag. 81). Se il tentativo non riesce e si ha urgente necessità di utilizzare tale file, l'utente può inviarlo a Kaspersky Lab per una analisi approfondita. Il file potrebbe essere stato infettato da un virus sconosciuto, o potrebbe trattarsi più semplicemente di un falso allarme.



Attenzione! È possibile inviare file ai Laboratori Kaspersky solamente dopo averne eseguito la scansione con il database aggiornato alla data della spedizione.



Per inviare un file a Kaspersky Lab per un'analisi approfondita:

Selezionare il file nella finestra **Quarantena** (cfr. la Figura 26) e fare clic sul pulsante [Invia](#).

Il programma creerà e aprirà automaticamente un nuovo messaggio utilizzando il programma di posta elettronica presente sul computer, per esempio Microsoft Outlook, con il file probabilmente infetto in allegato. Inviare questo messaggio. Gli esperti di Kaspersky Lab analizzeranno con attenzione il file ricevuto, cercando di recuperare tutti i dati in esso contenuti. In ogni caso, l'utente riceverà una risposta dettagliata con i risultati dell'analisi.



Ogni file inviato deve essere stato sottoposto a scansione con Kaspersky Anti-Virus® Personal al massimo un giorno prima della spedizione.

In alcuni casi possono esservi ragioni per considerare infetti uno o più file sul proprio sistema anche se Kaspersky Anti-Virus® Personal non ha rilevato la presenza di virus durante la scansione. Tali file possono essere inviati ai Laboratori Kaspersky per un'analisi.



Per inviare file sospetti a Kaspersky Lab per l'analisi:

fare clic su [Invia file per analisi](#) nella sezione sinistra della scheda **Assistenza** (cfr. la Figura 5). Selezionare i file sospetti utilizzando la finestra standard di selezione file di Windows.

I successivi passaggi necessari per inviare un messaggio a Kaspersky Lab sono identici a quelli relativi all'invio di oggetti probabilmente infetti dalla finestra **Quarantena**.

APPENDICE B. GLOSSARIO

Durante la lettura di questo Manuale d'uso è possibile imbattersi in termini specifici della protezione antivirus. Per chiarirne il significato abbiamo compilato questa Appendice, elencando i termini in ordine alfabetico per semplificarne la consultazione.

A

Aggiornamento del database antivirus – Una funzione di Kaspersky Anti-Virus® Personal che mantiene efficace la protezione antivirus del computer. Il processo di aggiornamento include la copia del *database antivirus* nel proprio computer dai *server di aggiornamento* di Kaspersky Lab, e l'integrazione automatica del nuovo database in Kaspersky Anti-Virus® Personal.

Alta velocità – Un livello di protezione che abilita la scansione dei soli *oggetti a rischio di infezione*, riducendo in maniera significativa il tempo di scansione.

Analizzatore euristico di codici – Una tecnologia efficientissima che consente a un programma antivirus di rilevare virus ignoti. Tutti gli oggetti sospetti di contenere un virus ignoto o una variante ignota di un virus vengono identificati grazie a questa tecnologia.

Archivi – File contenenti uno o più file che, a loro volta possono essere archivi.

B

Backup – La creazione di copie di sicurezza di un file nella cartella BACKUP prima di trattarlo (riparazione o eliminazione). Il file di backup potrà essere successivamente ripristinato, per esempio per sottoporlo a un'ulteriore scansione con una versione più aggiornata del database antivirus.

BACKUP – Una directory contenente copie di backup di oggetti eliminati o riparati.

C

Chiave di licenza – Un file con estensione *.key* che svolge la funzione di "chiave" personale per il corretto funzionamento di Kaspersky Anti-Virus® Personal. La chiave di licenza è inclusa nel kit di distribuzione se si acquista una copia di Kaspersky Anti-Virus® Personal da un rivenditore Kaspersky Lab. Se il prodotto viene acquistato online, la chiave di licenza viene inviata per posta elettronica. Senza la chiave di licenza Kaspersky Anti-Virus® Personal NON FUNZIONA.

D

Database antivirus – Un database creato dagli specialisti di Kaspersky

Lab, contenente una descrizione dettagliata dei virus noti e dei relativi metodi di rilevamento e riparazione. Il nostro database antivirus viene regolarmente aggiornato con le informazioni relative ai nuovi virus man mano che fanno la loro comparsa; pertanto, per garantire la protezione costante del computer è necessario *aggiornare* il proprio database installato con la maggior frequenza possibile.

Database di posta elettronica – Database di formato speciale contenenti i messaggi di posta elettronica memorizzati nel computer. Ogni messaggio in arrivo o in uscita viene salvato nel database subito dopo la ricezione o l'invio. Questi database vengono esaminati durante la scansione completa del computer. Nella modalità di protezione in tempo reale, Kaspersky Anti-Virus® Personal esamina tutti i messaggi di posta elettronica in arrivo e in uscita durante l'invio o la ricezione.

Disinfezione – Metodo di trattamento di un oggetto infetto. La procedura di disinfezione consente di rimuovere integralmente o in parte il codice maligno dai dati infetti, o di stabilire che la riparazione è impossibile. Gli oggetti vengono riparati per mezzo di record presenti nel database antivirus.

E

Eliminazione di un oggetto – Metodo di trattamento di un oggetto. Eliminare un oggetto significa rimuoverlo fisicamente dal computer. È il metodo raccomandato per gli oggetti la cui riparazione, per varie ragioni, risulta impossibile.

Esclusioni – Impostazioni definite dall'utente volte ad escludere determinati oggetti dalla scansione. È possibile personalizzare le regole di esclusione relative alla *protezione in tempo reale* e alla *scansione manuale*. Per esempio, è possibile escludere gli archivi dalla scansione completa del computer oppure specificare mediante l'uso di maschere determinati tipi di file che non si desidera esaminare.

F

Falso allarme – Situazione in cui il programma antivirus indica come infetto un oggetto pulito in quanto il codice in esso contenuto somiglia a un codice virale.

File compressi – File contenenti un programma e le istruzioni per la sua esecuzione da parte del sistema operativo.

I

Ignora – Metodo di trattamento in cui viene negato l'accesso all'oggetto (solo in modalità di protezione in tempo reale), e vengono registrate nel report del funzionamento del programma le informazioni relative all'oggetto, ma non vengono eseguite altre operazioni su di esso.

Isolamento (spostamento degli oggetti nella cartella della quarantena)

– Un metodo di trattamento degli *oggetti probabilmente infetti* che consiste nel negare l'accesso a tali oggetti e nel trasferirli nella cartella della quarantena per un successivo trattamento.

L

Livello raccomandato – Un livello di protezione antivirus basato sulle impostazioni raccomandate dagli esperti di Kaspersky Lab, che garantisce la protezione ottimale del computer. È il livello predefinito.

M

Memoria del computer – La RAM installata sul computer.

Moduli di Kaspersky Anti-Virus® Personal – File inclusi nella copia in distribuzione di Kaspersky Anti-Virus® Personal. Ciascuno di questi moduli corrisponde a una funzione specifica di Kaspersky Anti-Virus® Personal, per esempio la *protezione in tempo reale*, la *scansione manuale*, l'*aggiornamento*. Avviando la scansione manuale dalla finestra principale dell'applicazione, si esegue il modulo corrispondente a questa attività.

Massima protezione – Livello di protezione che garantisce la massima sicurezza offerta da Kaspersky Anti-Virus® Personal. In questa modalità di protezione vengono sottoposti alla scansione antivirus tutti i file memorizzati nel disco fisso, supporti rimovibili e unità di rete (se presenti).

O

Oggetti eseguiti all'avvio del sistema operativo – Un insieme di programmi necessari per l'esecuzione e il corretto funzionamento del sistema operativo e di altri programmi installati sul computer. Il sistema operativo li esegue ad ogni avvio. Alcuni virus infettano gli oggetti d'avvio e possono provocare un errore del sistema operativo.

Oggetto infetto – Un oggetto contenente un virus. Si raccomanda di non accedere a tali oggetti perché possono diffondere l'infezione nel computer. In presenza di un oggetto infetto, se ne raccomanda la *disinfezione* per mezzo di Kaspersky Anti-Virus® Personal, o l'eliminazione qualora la disinfezione non sia possibile.

Oggetto OLE – Un oggetto collegato a un altro file o incorporato in esso. Kaspersky Anti-Virus® Personal li sottopone a scansione per escludere la presenza di virus. Per esempio, un foglio di calcolo di Microsoft Excel incorporato in un documento Word sarà analizzato da Kaspersky Anti-Virus® Personal come oggetto OLE.

Oggetto potenzialmente infettabile – Un oggetto a rischio di infezione. Gli oggetti potenzialmente infettabili sono in genere file eseguibili, vale a dire file con estensione *com*, *exe* o di altro tipo.

Oggetto probabilmente infetto – Un oggetto contenente un codice di un virus noto o simile a quello di un virus attualmente ignoto a Kaspersky Lab. Gli oggetti probabilmente infetti vengono rilevati per mezzo dell'*analizzatore euristico di codici*.

P

Patch – Un pacchetto di file utilizzati per l'aggiornamento dei programmi. Le patch possono essere scaricate da Internet e installate sul computer.

Periodo di validità della licenza – Il periodo nel quale l'utente ha il diritto di utilizzare Kaspersky Anti-Virus® Personal. Il periodo di validità della licenza è definito da una chiave di licenza valida e dura generalmente un anno dalla data dell'acquisto. Dopo la scadenza della licenza, il prodotto conserva la funzionalità ma non consente di usufruire del servizio di *aggiornamento del database antivirus*.

Prevenzione – Una serie di misure precauzionali da adottare per impedire la penetrazione di virus nel computer. La prevenzione antivirus del computer prevede la protezione antivirus completa e la possibilità di scaricare aggiornamenti del programma.

Protezione in tempo reale – Una modalità di Kaspersky Anti-Virus® Personal eseguita automaticamente all'avvio del sistema. In modalità di protezione in tempo reale, il programma effettua la scansione antivirus di ogni oggetto aperto a fini di lettura, scrittura o esecuzione. Se un oggetto viene identificato come infetto o sospetto, Kaspersky Anti-Virus® impedisce di accedervi e cerca di trattarlo (riparazione, isolamento, eliminazione, ecc.) oppure richiede l'intervento dell'utente.

Q

Quarantena – Una cartella in cui Kaspersky Anti-Virus® Personal trasferisce tutti gli *oggetti probabilmente infetti* rilevati durante una *scansione completa del computer* o in modalità di *protezione in tempo reale*.

R

Recupero, ripristino – Il trasferimento di un file dalla *Quarantena* alla cartella originaria in cui si trovava prima di essere isolato, riparato o eliminato.

S

Scansione manuale – Una modalità operativa avviata dall'utente, che esegue la scansione di tutti i tipi di file residenti nel computer.

Script – Un insieme di azioni eseguite durante l'uso di Microsoft Internet Explorer; per esempio per la visita a un sito web. Nella modalità di protezione in tempo reale, Kaspersky Anti-Virus® Personal tiene sotto controllo l'esecuzione degli script, li disabilita e li sottopone a scansione antivirus. In base ai risultati della scansione, è possibile eseguire determinate azioni sullo script, per esempio consentirne o proibirne

l'esecuzione.

Server di aggiornamento di Kaspersky Lab – Un elenco di server http e ftp di Kaspersky Lab da cui Kaspersky Anti-Virus® Personal copia il database antivirus nel computer.

Settore di boot – Una particolare area del disco contenente il programma di caricamento del sistema operativo.

Settore di boot del disco – Un'area del disco fisso o di qualsiasi altro supporto rimovibile (per esempio un floppy disk o CD-ROM). Esistono *virus d'avvio* che infettano specificamente i settori di boot. Kaspersky Anti-Virus® Personal esegue la scansione antivirus dei settori di boot e li *ripara* in caso di virus.

Solo report – In questa modalità, il programma non esegue alcuna azione ma si limita a bloccare l'accesso a un file infetto o sospetto (solo in modalità di protezione in tempo reale) e a registrarne il rilevamento nell'apposito report.

Status della protezione antivirus – Lo status corrente della protezione antivirus che definisce il livello di sicurezza del computer.

V

Virus d'avvio – Un virus che infetta i *settori di boot* dei dischi e del sistema operativo del computer. Durante la fase di avvio, il virus obbliga il sistema a leggere la memoria e a trasferire il controllo al codice del virus invece che al caricatore originale.

Virus ignoto – Un nuovo virus non ancora registrato nel *database antivirus*. Di regola, Kaspersky Anti-Virus® rileva i virus ignoti per mezzo dell'*analizzatore euristico di codici* e indica come *probabilmente infetti* gli oggetti che li contengono.

APPENDICE C. 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 applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e filiali nel Regno Unito, Francia, Germania, Giappone, USA (CA), Benelux, Cina e Polonia. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 300 esperti, tutti specializzati in tecnologie antivirus, 9 dei quali in possesso di laurea in amministrazione aziendale, 15 di specializzazione postlaurea, e due appartenenti alla Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus consente all'azienda di offrire una protezione completa contro minacce presenti e perfino future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e commerciali.

Anni di duro lavoro ne hanno fatto un'azienda leader tra i principali produttori di software per la sicurezza informatica. 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 Anti-Virus[®], offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, gateway di posta elettronica, firewall e portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Anti-Virus[®], per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada), ecc.

C.1. Altri prodotti Kaspersky Lab

Kaspersky Anti-Virus® Personal Pro

Pacchetto progettato per offrire una protezione antivirus completa ai computer domestici con sistema operativo Windows 98/ME, Windows 2000/NT e Windows XP oltre alle applicazioni di MS Office 2000. Kaspersky Anti-Virus® Personal Pro include un'applicazione di facile utilizzo per il prelievo quotidiano automatico degli aggiornamenti del database antivirus e dei moduli del programma. L'esclusivo sistema di analisi euristica di seconda generazione rileva con efficacia perfino i virus ignoti. Kaspersky Anti-Virus® Personal Pro presenta un'interfaccia migliorato sotto molti aspetti, agevolando più che mai l'uso del programma.

Kaspersky Anti-Virus® Personal Pro presenta le seguenti funzioni:

- **scansione manuale** di dischi locali per rilevare ogni tipo di virus;
- **protezione in tempo reale** di tutti i file dai virus;
- **un filtro di posta** che esamina in background tutti i messaggi in entrata e in uscita;
- **behavior blocker** che garantisce la protezione totale dai macrovirus.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker è una firewall personale, progettata cioè per garantire la protezione di computer con sistema operativo Windows da qualsiasi accesso non autorizzato ai dati e dagli attacchi esterni da Internet o reti locali adiacenti.

Kaspersky® Anti-Hacker controlla l'attività di rete TCP/IP di tutte le applicazioni eseguite sul computer. In caso di rilevazione di azioni sospette, il programma blocca l'accesso alla rete da parte di tali applicazioni. Questa misura consente all'utente di conservare con sicurezza dati confidenziali nel proprio computer.

Grazie alla tecnologia SmartStealth™ la rilevazione del computer dall'esterno è oggi più difficoltosa. Questa modalità tuttavia non influisce minimamente sulla fluidità della navigazione in rete: il programma garantisce infatti la consueta trasparenza e accessibilità dei dati.

- Kaspersky® Anti-Hacker blocca i più comuni attacchi di pirateria informatica ed effettua un monitoraggio costante dei tentativi di scansione delle porte del computer.
- Il software supporta una gestione semplificata offrendo la scelta tra cinque livelli di sicurezza. Per impostazione predefinita, il programma si apre sulla modalità di autoapprendimento che configura automaticamente il sistema di sicurezza in base alle risposte dell'utente a eventi di vario tipo. Questa caratteristica consente di

personalizzare il programma in base alle preferenze ed esigenze specifiche dell'utente.

Kaspersky® Security for PDA

Kaspersky® offre un'affidabile protezione antivirus dei dati memorizzati su PDA con Palm OS o Windows CE, e di qualsiasi informazione trasferita da un PC o scheda di estensione, file ROM e database. Il software contiene una combinazione di strumenti antivirus mirati:

- uno **scanner antivirus**, usato per la scansione manuale di tutti i dati memorizzati (sia sul PDA stesso che su qualsiasi scheda di estensione) e
- un **monitor antivirus** che intercetta i virus durante il trasferimento di dati con l'utility HotSync™ o prelevati da dispositivi portatili.

Esso offre l'accesso criptato al dispositivo e codifica tutti i dati memorizzati nel dispositivo e nelle schede di memoria.

Kaspersky Anti-Virus® Business Optimal

Il pacchetto è stato sviluppato per garantire una protezione completa dei dati per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal include la protezione antivirus completa⁸ per:

- *workstation* con Windows 95/98/ME, Windows NT/2000/XP Workstation e Linux;
- *file server e application server* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell NetWare, FreeBSD, BSDi e OpenBSD, e Linux;
- *Sistemi di posta*: Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; MS ISA Server.

Il kit di distribuzione di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di programmi antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

⁸ In base al tipo di kit di distribuzione.

Kaspersky® Corporate Suite

Questo pacchetto è stato sviluppato al fine di offrire una protezione totale dei dati di reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i nodi di una rete aziendale, anche in ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una console mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

- *Workstation* con Windows 98/ME, Windows NT/2000/XP e Linux;
- *file server e application server* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell NetWare, FreeBSD, OpenBSD, e Linux;
- *Sistemi di posta*, inclusi Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; MS ISA Server.
- *Computer portatili* (PDA).

Il kit di distribuzione di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, tutti i moderni metodi di filtraggio della posta elettronica (inclusi gli elenchi RBL e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam funziona come filtro controllando tutta la posta in entrata alla ricerca di oggetti identificati come spam. Il software è compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal è studiato per garantire la protezione di Microsoft Outlook e Microsoft Outlook Express dai messaggi di posta elettronica indesiderati (spam).

Il pacchetto Kaspersky® Anti-Spam Personal è un potente strumento che garantisce l'intercettazione dello spam nel flusso di messaggi in arrivo mediante i protocolli POP3 e IMAP4 (solo per Microsoft Outlook).

Il processo di filtraggio comporta l'analisi di tutti gli attributi della lettera (indirizzi e intestazioni del mittente e del destinatario), il filtraggio dei contenuti (analisi dei contenuti della lettera, compresi oggetto e allegati), nonché una serie di esclusivi algoritmi linguistici ed euristici.

L'elevato grado di efficacia del programma è garantito anche grazie all'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico.

C.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab.

Supporto tecnico	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina http://www.kaspersky.com/supportinter.html
Informazioni di carattere generale	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com

APPENDICE D. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALMENTE VINCOLANTE ("CONTRATTO") RELATIVO AL SOFTWARE SPECIFICATO ("SOFTWARE") PRODOTTO DA KASPERSKY LAB ("KASPERSKY LAB").

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC 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, FACENDO CLIC 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. QUESTO SOFTWARE PUÒ ESSERE RESTITUITO PER OTTENERE IL RIMBORSO COMPLETO. IL DIRITTO DELL'UTENTE ALLA RESTITUZIONE E AL RIMBORSO SCADE 30 GIORNI DOPO L'ACQUISTO PRESSO UN DISTRIBUTORE O RIVENDITORE KASPERSKY LAB AUTORIZZATO. IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Tutti i riferimenti al termine "Software" contenuti nel presente includeranno la chiave di attivazione software ("File di identificazione chiave") che sarà fornita all'utente da Kaspersky Lab come parte integrante del Software.

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. La copia del software può essere installata su computer, workstation, palmare o altro dispositivo elettronico per cui è stato progettato il Software (ciascuno dei quali denominato "Dispositivo client").

Se il Software è concesso su licenza come suite o pacchetto contenente più di un prodotto Software specificato, tale licenza si applica a tutti i prodotti software specificati, ed è soggetta alle restrizioni o alle condizioni d'uso specificate sul listino prezzi applicabile o sull'imballo di ciascun singolo prodotto Software.

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

1.1.1 Il Software è "in uso" su un Dispositivo client 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 dispositivo client. 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 archivio, 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 Qualora l'utente venda il Dispositivo client su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.3 All'utente è fatto divieto di decompilare, reverse engineer, 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'interoperabilità del Software con programmi informatici creati autonomamente saranno fornite da Kaspersky Lab su richiesta, previo pagamento dei costi e delle spese ragionevolmente sostenuti per ottenere e fornire tali informazioni. Nel caso in cui Kaspersky Lab informi l'utente di non avere intenzione di mettere a disposizione tali informazioni per qualsiasi ragione, inclusi (senza limitazione) i costi, l'utente sarà autorizzato ad adottare le misure necessarie per ottenere l'interoperabilità, a condizione di poter soltanto decodificare o decompilare nella misura concessa per legge.

1.1.4 L'utente non deve, né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.5 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.

1.1.6 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.

1.2 Utilizzo in modalità Server. L'utente può utilizzare il Software su un Dispositivo Client o su un server o un dispositivo che operi come tale ("Server") nell'ambito di un ambiente multiutente o collegato in rete ("Modalità Server") solo

se tale uso è consentito dal listino prezzi applicabile o sull'imballo del Software. È richiesta una licenza separata per ogni Dispositivo Client o postazione dalla quale ci si connette al Server, indipendentemente dal fatto che tali dispositivi Client o postazioni concesse in licenza si connettano contemporaneamente o stiano effettivamente accedendo al Software o utilizzando lo stesso. L'utilizzo di software o hardware che riduce il numero di Dispositivi Client o postazioni con utilizzo o accesso diretto al Software (per esempio software o hardware di "multiplexing" o "pooling") non riduce il numero di licenze richieste (in quanto il numero richiesto di licenze sarebbe pari al numero di ingressi distinti al software o hardware di multiplexing o pooling "front end"). Se il numero di Dispositivi Client o di postazioni che possono connettersi al Software è maggiore del numero di licenze ottenute, l'utente deve disporre di un meccanismo ragionevole che garantisca che l'uso del Software non supera i limiti di utilizzo specificati per la licenza ottenuta. La presente licenza autorizza l'utente a effettuare o scaricare il numero di copie della Documentazione per ogni Dispositivo Client o postazione concessi in licenza necessario per il suo utilizzo ai termini di legge, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

1.3 Licenze per volume. Se il Software è concesso dietro una licenza per volume le cui condizioni sono specificate nella fattura applicabile del prodotto o sull'imballo del Software, l'utente può effettuare, utilizzare o installare tante copie supplementari del software sul numero di Dispositivi Client quante sono specificate nelle condizioni della licenza per volume. L'utente deve applicare meccanismi ragionevoli per garantire che il numero di Dispositivi Client su cui è stato installato il Software non superi il numero di licenze ottenute. La presente licenza autorizza l'utente a effettuare o scaricare una copia della Documentazione per ogni copia supplementare autorizzata dalla licenza per volume, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

2. Periodo di validità. Il presente Contratto è valido per un (1) anno, salvo e fino a rescissione anticipata come stabilito nel presente. Il presente Contratto terminerà automaticamente in caso di mancata osservanza da parte dell'utente di una delle condizioni, limitazioni o altri requisiti descritti nel presente. Al momento della rescissione o alla scadenza del presente Contratto, l'utente è tenuto a distruggere immediatamente tutte le copie del Software e della Documentazione. È possibile rescindere dal presente Contratto in qualsiasi momento distruggendo tutte le copie del Software e della Documentazione.

3. Assistenza.

(i) Kaspersky Lab fornirà al cliente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per un periodo di un anno dietro:

(a) pagamento della tariffa di assistenza corrente;

(b) soddisfacente compilazione del Modulo di sottoscrizione ai servizi di assistenza fornito all'utente unitamente al presente Contratto o disponibile sul

sito web di Kaspersky Lab, che richiede all'utente di produrre il File di identificazione chiave 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.

(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) Con la compilazione del Modulo di richiesta dei Servizi di assistenza, l'utente accetta le condizioni esposte nell'Informativa sulla tutela della privacy applicata da Kaspersky Lab e allegata al presente Contratto, e acconsente esplicitamente al trasferimento dei propri dati all'esterno dei propri confini nazionali, come specificato nell'Informativa sulla tutela della privacy.

(iv) Per "Servizi di assistenza" si intende

(a) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(b) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(c) Assistenza tecnica estesa tramite posta elettronica o linea telefonica dedicata forniti dal distributore o dal rivenditore;

(d) Rilevamento virus e aggiornamenti per l'eliminazione entro 24 ore.

4. Diritti di proprietà. Il Software è protetto dalle leggi sul copyright. Tutti i diritti, titoli e interessi in e sul Software, compresi tutti i diritti d'autore, brevetti, marchi e altri diritti sulla proprietà intellettuale sono proprietà e possesso di Kaspersky Lab e dei suoi fornitori. 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.

5. Riservatezza. L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi e il File di identificazione chiave 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 File di identificazione chiave.

6. Garanzia limitata

(i) Kaspersky Lab garantisce che per un periodo di 90 giorni a decorrere dal primo caricamento o installazione il Software opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(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 relativa Documentazione saranno idonei a soddisfare tali esigenze, né che l'uso sarà privo di interruzioni e di errori;

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'unico rimedio per l'utente e l'unica responsabilità a carico di Kaspersky Lab in caso di violazione della garanzia come da paragrafo (i) consiste, a discrezione di Kaspersky Lab, nella riparazione, sostituzione o rimborso del Software qualora tale violazione venga riferita a Kaspersky Lab o a chi in sua vece durante il periodo di validità della 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 stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (v) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

7. Responsabilità limitata

(i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente a (i) responsabilità civile per frode, (ii) 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, (iii) eventuali violazioni degli obblighi stabiliti dalla sezione 12 del Sale of Goods Act del 1979 o della sezione 2 del Supply of Goods and Services Act del 1982 o (iv) eventuali responsabilità che non possono essere escluse ai termini di legge.

(ii) Ai sensi del paragrafo (i), il Fornitore 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 affari;
- (f) perdita di opportunità;
- (g) perdita di avviamento;
- (h) danni alla reputazione;
- (i) perdita, danni o corruzione di dati;
- (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 nel paragrafo (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), 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.

8. La costituzione e l'interpretazione del presente Contratto devono essere effettuate in conformità alle leggi dell'Inghilterra e del Galles. Le parti si sottopongono alla giurisdizione delle corti di Inghilterra e Galles, salvo il diritto di Kaspersky Lab in qualità di parte ricorrente, di avviare il ricorso in qualsiasi corte della giurisdizione competente.

9. 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. Fatto salvo quanto stabilito ai paragrafi (ii) - (iii), l'utente non sarà in alcun modo risarcito per eventuali false dichiarazioni ricevute sulle quali aveva fatto affidamento nella stipula del presente Contratto ("Falsa dichiarazione") e Kaspersky Lab non sarà vincolata da altre responsabilità oltre a quelle relative alle espresse condizioni del presente Contratto.

Nessun elemento nel presente Contratto esclude o limita la responsabilità di Kaspersky Lab per eventuali false dichiarazioni rilasciate intenzionalmente.

(iii) La responsabilità di Kaspersky Lab per Dichiarazioni erronee in merito a questioni fondamentali, incluse le questioni fondamentali ai fini della capacità del produttore di adempiere agli obblighi previsti dal presente Contratto, sarà soggetta alle limitazioni di responsabilità esposte nel paragrafo 7 (iii).