

Il decalogo McAfee per la Protezione in internet per la tua famiglia

Come parlare a bambini,
preadolescenti, adolescenti
e principianti d'ogni età della
sicurezza on-line

10

Indice dei contenuti

- 3 Introduzione
- 4 Internet oggi:
la prudenza non è mai troppa
- 5 Il decalogo della protezione per aiutarti
a tutelare tutta la famiglia
- 17 L'ABC della protezione on-line:
 - 17 Per i bambini (da 3 a 7 anni)
 - 21 Per i preadolescenti (da 8 a 12 anni)
 - 26 Per gli adolescenti (da 13 a 19 anni)
 - 30 Per i principianti d'ogni età
- 33 Informazioni su McAfee

10





Introduzione

Nel mondo, milioni di famiglie si servono quotidianamente di Internet come strumento didattico e di ricerca, per fare spese, acquisti importanti e operazioni bancarie, per investire, condividere foto, divertirsi con i videogiochi, scaricare film e musica, comunicare con amici, fare nuovi incontri e per tutta una serie di altre attività. Tuttavia, se è vero che il ciber spazio offre molti vantaggi, opportunità e comodità, è anche vero che presenta rischi crescenti, con **nuove minacce che emergono numerose ogni giorno**.

Non c'è quindi da stupirsi se la criminalità informatica continua a diffondersi moltiplicando gli abusi a danno di Internet e di coloro che lo utilizzano. Ecco perché la prudenza è d'obbligo ad ogni connessione on-line. Oltre ad installare un efficace software di protezione prodotto da un'azienda affidabile per difendere la tua famiglia da pirateria, furti di identità, truffe perpetrate via e-mail e molestie on-line, devi **seguire alcune regole di sicurezza basilari** e agire con lo stesso buon senso che ti guida nel mondo reale. In sintesi, devi pianificare la protezione in Internet della tua famiglia.

Non appena un tuo familiare diventa un utente attivo di Internet—indipendentemente dalla sua età—devi sensibilizzarlo al tema della sicurezza. **Devi tenere presente** che anche se non hai installato un computer a casa, i PC sono disponibili praticamente ovunque: a scuola, in biblioteca, dagli amici e perfino negli oratori delle chiese. È essenziale che ognuno conosca i principi fondamentali dell'autoprotezione nel cyberspazio.



Internet oggi: la prudenza non è mai troppa

- Il 50% degli adolescenti on-line ha fornito informazioni personali¹
- Gli hacker attaccano i PC dotati di accesso Internet ogni 39 secondi²
- Secondo i McAfee® Avert Labs®, esistono oggi 222.000 virus informatici conosciuti in circolazione e il numero di minacce cresce di giorno in giorno
- Il 30% degli adolescenti ha subito atti di "cyberbullismo" una o più volte durante il periodo scolastico³
- Nel 2008 i crimini in Internet sono cresciuti del 33% rispetto all'anno precedente⁴
- Il 31% dei bambini è stato esposto a contenuti pericolosi¹
- Ogni anno 3,2 million di persone in tutto il mondo sono vittime di frodi di identità⁵

1 EU Kids Online, Comparing children's online opportunities and risks across Europe (Preadolescenti ed adolescenti dell'UE on-line, Relazione su rischi ed opportunità on-line in Europa) (2006-2009)

2 Hackers Attack Every 39 Seconds (I pirati attaccano ogni 39 secondi) – James Clark School of Engineering Università del Maryland (U.S.A.)

3 theage.com.au

4 2008 Internet Crime Report (Rapporto 2008 sui crimini in Internet), IC3

5 National Fraud Strategic Authority (Agenzia Americana per le Frodi di Identità)



Il decalogo della
protezione per
aiutarti a tutelare
tutta la famiglia



Punto 1

Il posto giusto per il PC

Se hai dei figli, scegliere dove installare il computer domestico è una delle decisioni più importanti da prendere. Ti consigliamo di installarlo in una **zona molto frequentata della casa** e di limitare a poche ore il tempo che i tuoi figli passano davanti allo schermo. Accertati di avere sul computer un **software di protezione** con controlli parentali analoghi a quelli disponibili con i prodotti McAfee oppure utilizza software specifico progettato per tutelare i bambini on-line, come McAfee Family Protection.

Punto 1



Punto 2

Punto 2

Decidere insieme i limiti da rispettare

Stabilire esattamente cosa è ammissibile e cosa è inaccettabile riguardo a:

- Il tipo di siti web che si possono visitare
- Le chat e i forum ai quali è consentito partecipare:
 - Scegliere soltanto chat controllate
 - Accertarsi di rendere inaccessibili le chat “.alt”, dedicate a tematiche che possono non essere adatte ai più giovani
- Il genere di argomenti di cui è lecito discutere on-line e il linguaggio considerato sconveniente



Punto 3

Stabilire insieme le regole d'uso del PC

Ti consigliamo di rispettare i seguenti criteri:

- Non collegarsi mai con nomi utente che rivelano la vera identità personale o che possono risultare provocanti
- Non rivelare mai le proprie password
- Non rivelare mai numeri di telefono o indirizzi
- Non divulgare mai informazioni che rivelano l'identità personale
- Non divulgare mai fotografie sconvenienti o che possono rivelare l'identità personale (ad esempio: con nomi di città o scuole sulle magliette)
- Non condividere mai informazioni con estranei conosciuti on-line
- Non incontrare mai di persona estranei conosciuti on-line
- Non aprire mai allegati inviati da estranei

Una volta stabilite le regole da rispettare, stilarne un elenco e apporlo accanto al computer.

Punto 3



Punto 4

Un codice di condotta per comportarsi correttamente on-line

Elaborare un codice di condotta o **utilizzare il modello alla pagina seguente**, per chiarire e pattuire ciò che in famiglia si intende per uso lecito del computer e **comportamento corretto on-line**.

Punto 4

A young boy with short brown hair, wearing a white and blue striped shirt, is looking down at a screen. A man with dark hair is leaning over him, also looking at the screen. The background is a warm, indoor setting.

I miei impegni per la sicurezza on-line

Poiché la possibilità di usare il computer e di collegarmi a Internet è un privilegio che non voglio perdere,

- Mi impegno a navigare, eseguire ricerche, giocare e **chattare in tutta sicurezza ogni volta che sono on-line**
- Mi impegno a **rispettare tutte le regole** che abbiamo stabilito di comune accordo
- Mi impegno a non rivelare** il mio vero nome, il mio numero di telefono, il mio indirizzo o le mie password agli "amici" on-line
- Mi impegno a **non incontrare mai di persona** le persone conosciute on-line
- Se quando sono on-line mi trovo in una situazione che mi fa sentire in pericolo o a disagio, **prometto di dirlo a (genitore/tutore/insegnante)** per farmi aiutare
- Prometto di rispettare i miei impegni** e dichiaro di essere consapevole delle conseguenze che può avere ogni mia decisione

Firma del bambino/ragazzo _____

- In qualità di genitore/tutore/insegnante, prometto di rendermi disponibile per ogni tua richiesta di assistenza e di aiutarti a risolvere qualsiasi problema che puoi incontrare al meglio delle mie possibilità.

Firma del genitore/tutore/insegnante _____



Punto 5

Il software di protezione

Accertati che il tuo PC sia protetto da un software di protezione efficace, capace di neutralizzare virus, hacker e spyware e di filtrare i contenuti, le immagini e i siti web offensivi. Il software **deve essere aggiornato regolarmente**, per far fronte alle nuove minacce che emergono quotidianamente. Uno strumento di protezione ad aggiornamento automatico—come il software McAfee **che si gestisce in maniera totalmente autonoma**—è la scelta ideale.

Punto 5



Punto 6

Controlli parentali

Tutti i principali fornitori di software di protezione propongono i controlli parentali. Non dimenticare di attivarli. Se usi un freeware o un software privo di controlli parentali, valuta l'opportunità di acquistare un prodotto che ne è dotato. È importante conoscerne il funzionamento e imparare a utilizzare le opzioni che filtrano e bloccano i contenuti impropri.

Per tutelare completamente i tuoi bambini nelle loro attività on-line, utilizza il software McAfee Family Protection in aggiunta al controllo parentale già presente all'interno del tuo software di protezione. Il software McAfee Family Protection tutela i bambini di ogni età dall'esposizione a contenuti non adatti, rischi connessi ai social network, estranei ed altre tipologie di minaccia on-line.

Naturalmente, anche questi strumenti hanno i loro limiti. Niente e nessuno può sorvegliare bambini e ragazzi on-line con la stessa attenzione e reattività dei genitori.

Punto 6



Punto 7

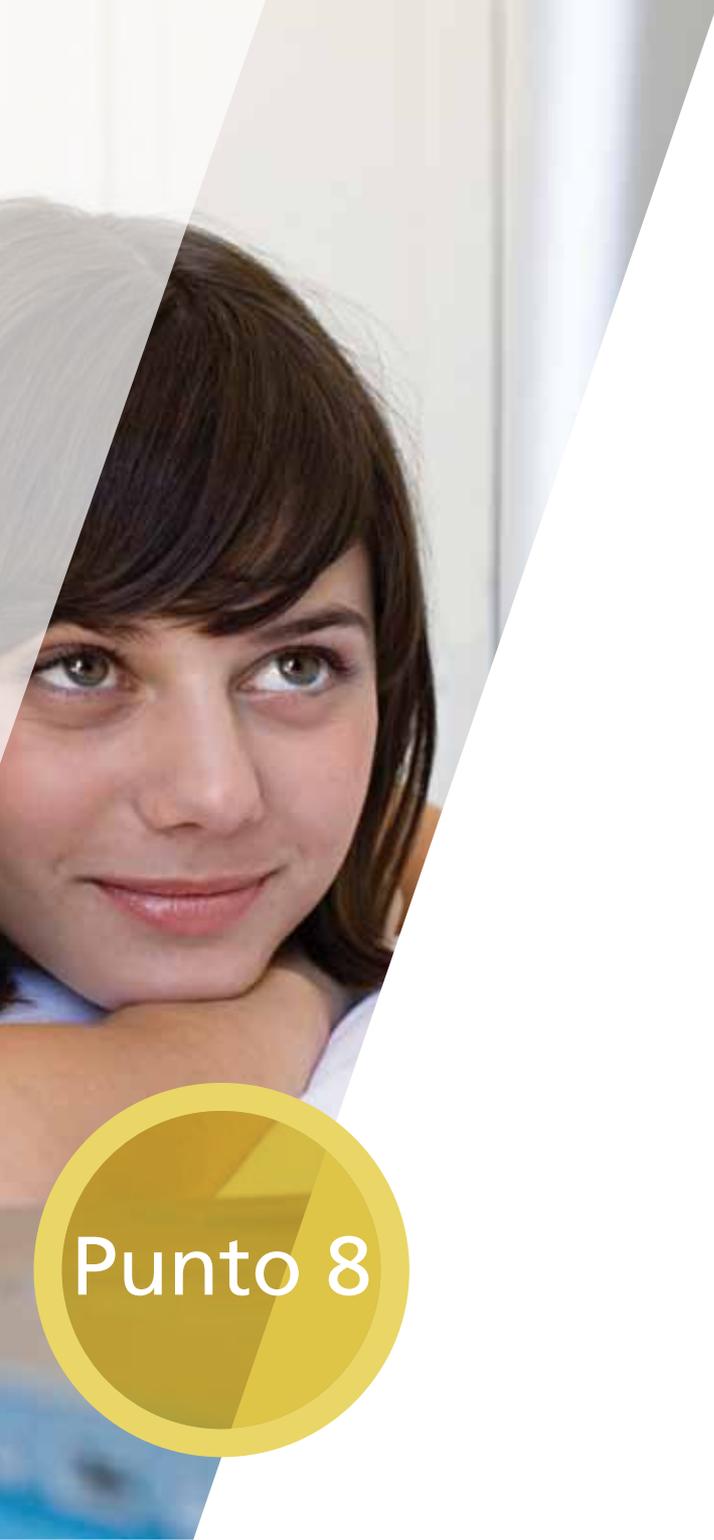
Punto 7

Ricordare a tutta la famiglia che le persone incontrate on-line sono degli estranei

Tutti coloro che si collegano on-line devono rendersi conto che:

Per quanto frequenti siano le chat con gli “amici” on-line, per quanto questi “amici” virtuali siano di vecchia data e malgrado la convinzione di conoscerli ormai bene, le persone incontrate on-line sono e rimangono degli estranei. **Quando si chiacchiera on-line è molto facile mentire e fingere di essere qualcun altro.** I bambini, in particolare, devono sapere che dietro un nuovo “amichetto” può in realtà nascondersi un uomo di 40 anni anziché un loro coetaneo.

I **social network** quali ad esempio Bebo, Orkut, MySpace e Facebook sono nati per favorire nuovi incontri on-line. Pertanto, i genitori devono visitare questi siti e **verificare il profilo dei propri figli** per accertarsi che non frequentino luoghi di conversazioni sconvenienti e di diffusione di fotografie disdicevoli. I genitori devono inoltre controllare i messaggi immediati scambiati dai loro figli per accertarsi che non siano preda di molestatore on-line.



Punto 8

Creare password efficaci

Per creare password difficilmente decifrabili, è consigliabile usare almeno 8 caratteri che comprendano una combinazione di lettere, numeri e simboli. **Le password dovrebbero essere cambiate regolarmente** per ridurre le probabilità di violazione con il passare del tempo.

Tecniche per creare password sicure:

- Utilizzare una finta targa "personalizzata": "GR8way2B"
- Utilizzare più parole di poche lettere con segni di punteggiatura: "Bindi#the^jungle@girl"
- Inserire la punteggiatura o un simbolo al centro della parola: "Beck%ham"
- Utilizzare una parola con contrazione insolita: "ftblplyr"
- Utilizzare la prima lettera di ogni parola di una frase, con un numero a caso: "provate a decifrarla, questa password" = "pad5qp"
- Non rivelare mai le proprie password!

Punto 8



Punto 9

Verifica il software di protezione

Apri il tuo software di protezione e verifica che il tuo computer sia al sicuro grazie alle **tre protezioni cruciali: antivirus, antispyware e firewalll**.

Queste tre protezioni di base dovrebbero essere potenziate da un antispam e da un software per ricerche sicure come McAfee SiteAdvisor® che offre funzioni anti-phishing e segnala il grado di affidabilità dei siti web. È inoltre utile per le famiglie avere sul PC di casa una soluzione di protezione completa, che includa controlli parentali e strumenti di prevenzione dei furti di identità.

Punto 9



Punto 10

Tenersi informati

Chi conosce i rischi, riesce a proteggersi meglio. Ti invitiamo a visitare il nostro McAfee Security Advice Center, un sito dove puoi consultare materiali divulgativi sulla protezione dei computer e in Internet, all'indirizzo: www.mcafee.com/advice.

Punto 10



L'ABC della protezione on-line

per i bambini da 3 a 7 anni

A photograph showing a man and a young boy sitting together, looking at a computer monitor. The man is on the left, leaning in, and the boy is on the right, facing the screen. The background is a warm, yellowish wall. The image is partially obscured by a large, diagonal, semi-transparent graphic element that separates it from the text on the right.

A

Il dialogo con i bambini

Quando parli di protezione in Internet con bambini piccoli, fallo a computer spento, così ti presteranno tutta la loro attenzione. Per cominciare, spiega che il computer è solo uno strumento e che Internet è come una gigantesca biblioteca elettronica piena di informazioni.

Spiega perché è importante proteggersi on-line, in che modo gli intrusi possono andare a curiosare tra i tuoi dati personali importanti attraverso il computer. Parla dei malintenzionati capaci di prendere il controllo del PC e danneggiarlo, tanto da costringerti a comprarne un altro.

Spiega perché è fondamentale non comunicare informazioni personali ad altri on-line. Devi fare in modo che capiscano che non devono usare il loro vero nome, che non devono dire dove vivono o quale scuola frequentano.



B

Crea un elenco di regole d'uso del computer per i bambini piccoli

Queste sono alcune delle regole da non dimenticare:

- Non scaricare musica o programmi dai siti web senza il consenso dei genitori
- Partecipa soltanto a chat controllate dove la chat è effettivamente controllata da un adulto
- Non inviare mai una tua fotografia senza parlarne prima ai tuoi genitori
- Non usare un linguaggio scorretto
- Non visitare i siti per adulti
- Comunica informazioni soltanto a chi conosci davvero, come compagni di scuola, amici e familiari
- Non compilare moduli o questionari elettronici senza l'aiuto dei genitori
- Utilizza solo motori di ricerca per bambini, come Ask for Kids e Yahoo! Kids



C

Utilizza browser e motori di ricerca pensati per i bambini

Accertati che i bambini usino browser e motori di ricerca che non visualizzano parole o immagini sconvenienti. Verifica che siano dotati di funzioni per ricerche sicure e di filtri linguistici con parole preimpostate. È sufficiente verificare e approvare le parole e i siti web impostati come valori predefiniti.

Se i tuoi figli utilizzano un motore di ricerca standard, assicurati di attivare il controllo parentale integrato per bloccare la visualizzazione nei risultati di immagini e contenuti sconvenienti.



L'ABC della protezione on-line

per i preadolescenti da
8 a 12 anni



A

Il dialogo con i preadolescenti

I giovanissimi tra gli otto e i dodici anni sono molto più smaliziati rispetto ai loro coetanei delle precedenti generazioni. Il termine “preadolescente” è stato coniato per definire precisamente questa fascia d’età composta da ragazzi non più considerati “bambini” ma che non sono ancora entrati nell’adolescenza. Va segnalato che i preadolescenti si sentono a loro agio davanti a un computer: ne hanno sempre visto uno a casa e/o a scuola.

Prima di intavolare il dialogo, è necessario prendere alcune decisioni preliminari per limitare il loro accesso ad Internet. Perché le regole siano chiare, occorre innanzitutto definirle. Per tutelare la loro sicurezza, devi conoscere le risposte alle seguenti domande:

- Il computer è installato in una zona liberamente accessibile della casa?
- Quali sono i siti web sicuri per i preadolescenti?
- Quanto dovrebbe durare una loro sessione on-line?
- Cosa possono fare mentre sono on-line?
- Con chi hanno il permesso di interagire?
- Se decidi di non sorvegliarli di persona, quando dovrebbero chiedere il tuo aiuto o la tua approvazione?



Una volta definite le risposte a queste domande, puoi procedere con il dialogo vero e proprio. A computer spento per evitare distrazioni, dovresti cominciare spiegando che il computer è uno strumento utile ma che è essenziale proteggersi on-line.

Assicurati di discutere dei seguenti argomenti:

- Le minacce costituite da virus, spyware e hacker
- L'abilità dei molestatori nell'indurre i ragazzi a parlare di se stessi
- Perché è importante proteggersi on-line e in che modo gli intrusi possono andare a curiosare tra i tuoi dati personali importanti attraverso il computer
- Il furto di identità e come viene perpetrato
- La possibilità che tu, o un esperto (se l'informatica non è la tua specialità), scopra ogni singola operazione eseguita sul tuo computer
- Parla dei malintenzionati che possono prendere il controllo del PC e danneggiarlo, tanto da costringerti a comprarne un altro



B

Ricorda ai tuoi figli di rivolgersi a te se succede qualcosa di sgradevole on-line

Insisti bene sul fatto che i tuoi ragazzi devono dirti se ricevono messaggi strani o sgradevoli durante una chat e che non ti arrabbierai con loro per questo né li punirai privandoli dell'accesso a Internet. Chiarisci che sei consapevole del fatto che non possono controllare quello che gli altri dicono e che non sono responsabili di questi episodi.

È bene inoltre controllare che i preadolescenti non subiscano o compiano atti di bullismo on-line. All'uscita di scuola, i ragazzi non si lasciano necessariamente anche i compagni e i conflitti di classe alle spalle. E-mail, SMS e telefoni cellulari consentono agli studenti di rimanere sempre in contatto e non è da escludere che abusino della tecnologia per assillare, tiranneggiare e fare del male.



C

Come bloccare gli utenti e segnalare i problemi

In caso tuo figlio sia vittima di comportamenti sgradevoli o dannosi durante una sessione di chat, è possibile segnalare il problema e bloccare l'utente. Innanzitutto, salva, copia e incolla i messaggi testuali relativi alla sessione in un programma di elaborazione testi. Invia poi la copia dei messaggi al moderatore o all'amministratore della chat. Le informazioni di contatto sono generalmente reperibili nella sezione dedicata alla guida o alla segnalazione dei problemi. La maggior parte dei programmi di chat consentono di bloccare un utente facendo clic sul suo nome nella lista dei contatti e selezionando il comando "Blocca" o "Ignora".



L'ABC della protezione on-line

per gli adolescenti
da 13 a 19 anni



A

Il dialogo con gli adolescenti

Analogamente alle norme di sicurezza stradale che bisogna conoscere prima di mettersi al volante, gli adolescenti devono apprendere le regole della navigazione sicura prima di esplorare il web in totale autonomia.

Ma a differenza della circolazione automobilistica, il traffico su Internet non è disciplinato da un "codice della strada". Ciò rende Internet un ambiente allo stesso tempo molto dinamico e molto pericoloso. Di conseguenza, per evitare blocchi di sistema o danni peggiori, bisogna stabilire delle regole e farle rispettare. L'obiettivo è insegnare agli adolescenti come agire con buonsenso per evitare i pericoli on-line.



È essenziale spiegare bene perché è importante proteggersi on-line.

Assicurati di discutere dei seguenti argomenti:

- Le minacce costituite da virus, spyware e hacker e il loro modo di agire
- L'abilità dei molestatori nell'indurre i giovani più vulnerabili a parlare di se stessi
- Perché è importante proteggersi on-line e in che modo gli intrusi possono andare a curiosare tra i tuoi dati personali importanti attraverso il computer
- Il furto di identità e come viene perpetrato
- La possibilità che tu, o un esperto (se l'informatica non è la tua specialità) scopra ogni singola operazione eseguita sul tuo computer
- Parla dei malintenzionati che possono prendere il controllo del PC e danneggiarlo, tanto da costringerti a comprarne un altro



B

Sottolinea bene che le persone incontrate on-line sono pur sempre degli sconosciuti

Malgrado la frequenza delle conversazioni on-line e malgrado la convinzione di conoscerli ormai bene, gli interlocutori virtuali sono e rimangono degli estranei. Su Internet si può mentire sulla propria identità e il nuovo "amico" di un adolescente può non essere affatto un giovane coetaneo, ma un uomo di 40 anni.

C

Verifica il profilo dei tuoi ragazzi sui siti di social network

Assicurati che non divulghino troppe informazioni personali su Bebo, Orkut, MySpace o Facebook. Accertati che non condividano fotografie che possono risultare provocanti. Insisti sul fatto che possono involontariamente attirare l'attenzione di molestatori on-line, mettere a disagio amici e familiari, mandare in fumo la possibile ammissione all'università o suscitare una cattiva impressione in un futuro datore di lavoro.



L'ABC della protezione on-line

per principianti di tutte le età



Tua moglie, o tuo marito, il tuo o la tua compagna, i tuoi genitori, i suoceri o i nonni possono essere utenti di computer e di Internet alle prime armi. E possono rivelarsi meno scaltri di quanto pensi, facili vittime di truffatori on-line e attacchi di pirati informatici. Pertanto, avranno bisogno di un piccolo aiuto da parte tua. La discussione sulla protezione in Internet dovrebbe toccare i seguenti argomenti:

A

Virus, spyware e hacker

Se necessario, puoi trovare facilmente una definizione di questi termini con una ricerca on-line o consultando in nostro glossario all'indirizzo www.mcafee.com/advice.

**B**

I rischi insiti nel furto d'identità e nel phishing

Il phishing avviene quando i criminali informatici simulano il sito web e le comunicazioni e-mail di un'organizzazione legittima con l'intento di carpire le password e i numeri di carta di credito degli utenti. Assicurati di verificare regolarmente gli estratti del conto corrente e della carta di credito.

C

L'importanza di prestare attenzione quando si scaricano contenuti "gratuiti"

Ricorda ai tuoi familiari che nessuno regala niente, è risaputo, neanche gli omaggi! Avvertili inoltre che se scaricano programmi software, è possibile che l'applicazione sia contaminata da adware e spyware.

Altri consigli sulla protezione del PC e in Internet

Per maggiori informazioni e consigli sulla protezione del PC e in Internet, visita il McAfee Security Advice Center all'indirizzo www.mcafee.com/advice.

Informazioni su McAfee

Con sede principale a Santa Clara, in California, McAfee, Inc. è la principale azienda focalizzata sulle tecnologie di sicurezza. McAfee è costantemente impegnata nella lotta contro le più pericolose minacce alla sicurezza. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi e reti in tutto il mondo, consentendo agli utenti di navigare ed effettuare acquisti sul web in modo sicuro. Grazie a un riconosciuto team di ricerca, McAfee crea soluzioni innovative che proteggono gli utenti consumer, aziende, pubblica amministrazione e service provider consentendo loro di essere conformi alle normative, proteggere i dati, evitare interruzioni delle attività, identificare le vulnerabilità e monitorare e migliorare costantemente la loro sicurezza.

<http://www.mcafee.com>

McAfee, Srl. Via Gaudenzio Fantoli, 7 20138 Milano, Italy 1.888.847.8766 www.mcafee.com

McAfee, SiteAdvisor e/o altri marchi citati nel presente documento sono marchi o marchi registrati di McAfee, Inc. e/o di consociate negli USA e/o in altri Paesi. Il Rosso McAfee utilizzato con riferimento alla protezione è una caratteristica distintiva dei prodotti a marchio McAfee. Tutti i marchi registrati e non registrati citati nel presente documento sono di proprietà esclusiva dei rispettivi titolari.
© 2009 McAfee, Inc. Tutti i diritti riservati.