

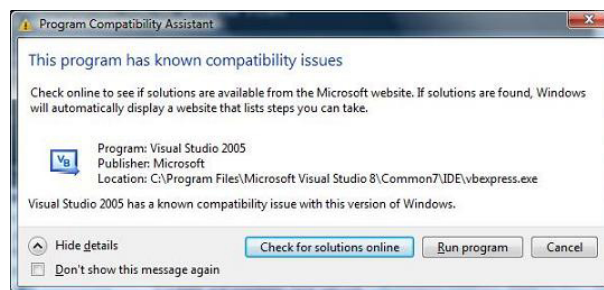
A cura di **Gianluca Marcoccia**

Installare Visual Basic 6 sui nuovi sistemi operativi

Se dovessi abbandonare Windows XP SP3 per passare a un sistema operativo successivo - probabilmente Windows 8 - potresti continuare a utilizzare Visual Basic 6 SP6? In alternativa, che livello di compatibilità potresti aspettarmi con il precedente Windows 7? So che dovrei passare a Visual Basic 2010, ma a ottant'anni ricominciare da zero non è così facile!

G. Aponte

L'installazione dell'ambiente di sviluppo Visual Basic 6 nelle ultime versioni dei sistemi operativi Windows non è ufficialmente supportata da Microsoft. Nonostante l'utilizzo con Vista non presenti particolari difficoltà, l'interoperabilità di VB 6 è gradualmente peggiorata con Windows 7 fino ad avere gravi problemi di compatibilità con Windows 8. Lanciando il setup, la procedura guidata d'installazione si blocca senza lasciare altre possibilità all'utente. Secondo le informazioni riportate nella pagina di supporto tecnico, Microsoft assicurerà la compatibilità del pacchetto Runtime di Visual Basic 6 anche sui nuovi sistemi operativi, compreso Windows 8, per consentire l'esecuzione dei software sviluppati con questo ambiente di sviluppo, ma oltre a questo non sono previsti aggiornamenti per il compilatore né per l'interfaccia utente. Sebbene sia



concettualmente possibile trasferire i propri progetti sulle versioni successive dell'ambiente di sviluppo, questa scelta pone non pochi problemi per il supporto delle applicazioni e potrebbe rendere necessaria la riscrittura di intere porzioni di codice sorgente per renderle compatibili con le librerie aggiornate. Allo stesso tempo, modifiche così estese richiederebbero di certificare nuovamente il corretto funzionamento dell'applicazione eseguendo batterie di test e il successivo debugging. È facile immaginare che per molti software ormai obsoleti e per aziende dotate di un budget limitato questa soluzione non sia praticabile. Un'alternativa più accettabile può essere l'utilizzo di un software di virtualizzazione. Allestendo una macchina virtuale per l'esecuzione di Windows XP si potrà continuare a utilizzare questo ambiente di sviluppo anche sui computer basati su Windows 8. Con questo sistema operativo l'operazione è più laboriosa perché Microsoft

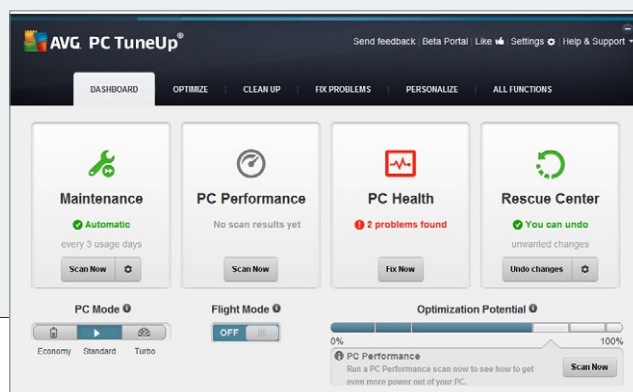
ha dismesso l'XP Mode, prima fornito a corredo. È comunque possibile sopperire alla mancanza procedendo personalmente alla creazione della VM. Se si ha a disposizione Windows 8 Professional, questa versione del sistema operativo include il software di virtualizzazione Hyper-V, in caso contrario se ne potrà comunque installare e utilizzare un altro, per esempio uno dei prodotti di VMWare. Un altro fattore da tenere in considerazione è che, in assenza dell'XP Mode, sarà necessario procedere all'installazione di Windows XP e per tale scopo si dovrà riciclare un codice d'attivazione da un vecchio computer. C'è, però, un'altra possibilità per evitare le complicazioni relative alla creazione di una macchina virtuale ad hoc. Sebbene la procedura d'installazione non sia in grado di funzionare in Windows 8, è possibile eseguire manualmente il caricamento degli eseguibili e delle librerie necessarie al funzionamento di Visual Basic 6 in questo modo:

Visual Basic 6 presenta incompatibilità con Windows 7 e 8, ma con alcuni accorgimenti è comunque possibile portarne a termine l'installazione. In alternativa, si può utilizzare questo ambiente di sviluppo mediante tecniche di virtualizzazione.

Antivirus Avg e dischi allo stato solido

Ho acquistato e installato l'antivirus Avg Internet Security 2014 sul mio computer. Nei giorni precedenti avevo sostituito il disco fisso principale con un Ssd Samsung 840 Evo da 250 Gbyte. Dopo dieci giorni, durante i quali il Pc non ha mai mostrato problemi e ha mantenuto l'auspicata rapidità d'avvio e spegnimento, improvvisamente i tempi si sono allungati a dismisura, rasentando il blocco totale. Dopo aver effettuato le consuete prove sull'Ssd, risultate regolari, ho scoperto in Rete che il mio antivirus avrebbe alcune incompatibilità con gli Ssd. E, in effetti, quando ho rimosso il software tutto è tornato alla normalità. Vorrei sapere a cosa sia dovuto il problema e perché non si presenti subito, ma solo dopo alcuni giorni.

Attilio D.P.



In passato, alcuni utenti della suite Avg hanno segnalato rallentamenti su computer in cui era presente un Ssd. Gli sviluppatori del software hanno attribuito la causa all'utilità TuneUp, un software a corredo di Internet Security che ottimizza l'efficienza delle memorie di massa. Il problema si verificava perché TuneUp non era sempre in grado di identificare i dischi Ssd e quindi applicava anche su questi le strategie di gestione riservate ai dischi magnetici tradizionali. A questo proposito, ricordiamo che la deframmentazione, fondamentale per gli hard disk magnetici, è sconsigliabile per gli Ssd perché usura le celle di memoria flash con ripetute operazioni di lettura/scrittura e non migliora le prestazioni. Le segnalazioni di malfunzionamento delle funzioni di ottimizzazione riguardavano, però, le versioni precedenti della suite e sembravano essere state risolte con un apposito aggiornamento. È perciò strano che il problema si sia ripresentato con la versione più recente. Sugeriamo di verificare se l'inconveniente sia riconducibile alla stessa causa reinstallando la suite ed escludendo, dal suo pannello di controllo, l'esecuzione di TuneUp. Se il sistema funzionasse in modo corretto si potrà lasciare disattivata questa funzione (in attesa di un aggiornamento risolutivo) mantenendo però il computer protetto.

Alcune versioni dell'utility TuneUp a corredo dell'antivirus Avg hanno problemi di rilevazione delle unità Ssd e possono causare pesanti rallentamenti del sistema operativo.

1. Copiare i file d'installazione dal Cd-Rom del software. Entrare nella cartella e creare due copie del file *Vb98pro.stf*.

2. Alla prima copia assegnare il nome *Acost.exe*, alla seconda copia il nome *Acmsetup.exe*.

3. Creare una copia del contenuto della directory Setup nella cartella in cui avete archiviato il contenuto del Cd-Rom.

5. Fare clic con il tasto destro del mouse sul file *Acmsetup.exe*, selezionare *Proprietà* e impostare l'esecuzione in modalità compatibile con Windows XP SP3.

6. Eseguire la stessa impostazione per i file *Acmboot.exe* e *Setup.exe*.

7. Lanciare *Setup.exe* con i diritti d'Amministratore.

8. Quando apparirà un avviso relativo a potenziali incompatibilità, confermare e proseguire con la procedura guidata.

9. Selezionare l'opzione d'installazione personalizzata e rimuovere il segno di spunta da *Data Access* (requisito per la successiva installazione del Service Pack).

10. Al completamento dell'installazione, la procedura guidata si bloccherà a causa dell'incompatibilità con il nuovo sistema operativo, ma a questo punto tutto il materiale necessario al funzionamento dell'ambiente di sviluppo è già stato installato.

11. Riavviare il computer e confermare eventuali richieste di chiusura delle applicazioni in esecuzione.

Completata l'installazione di Visual Basic 6, si dovrà procedere al caricamento del Service Pack 6. Come spiegato in precedenza, ciò non potrà andare a buon fine se non si deseleziona *Data Access* al punto 9 della procedura precedente. Procedere in questo modo:

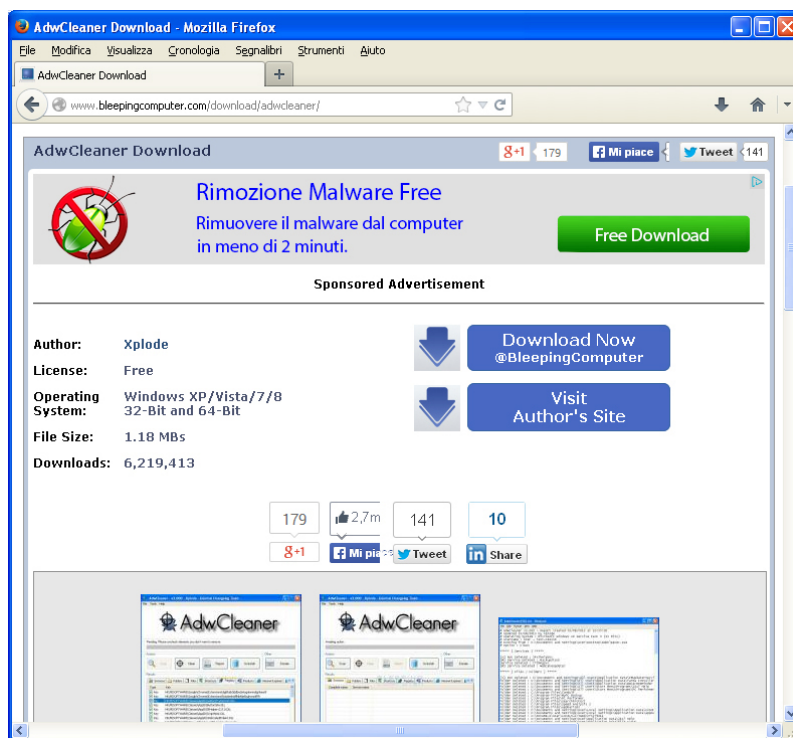
1. Copiare il Service Pack 6 in una cartella del disco fisso.

2. Nella stessa cartella, creare due copie del file *Sp698vbo.stf*, assegnando alla prima il nome *Acost.exe*, alla seconda il nome *Acmsetup.exe*.

3. Eseguire il file *Acmsetup.exe*.

4. Al completamento dell'operazione potrebbe essere richiesto il riavvio del computer.

L'ambiente di sviluppo dovrebbe ora essere utilizzabile anche in Windows 8. Facciamo presente che, nonostante



I concessionari di pubblicità sui siti web dovrebbero controllare di più i banner dei propri inserzionisti. Sta aumentando la presenza di pulsanti per il download di greyware.

quest'ultima soluzione offra un'efficienza superiore e un ambiente di lavoro più diretto, l'utilizzo di un software di virtualizzazione ha il vantaggio di permettere l'esecuzione di Visual Basic 6 nel sistema operativo per il quale è stato progettato e quindi può contribuire a eliminare eventuali problemi.

AdwCleaner e il cavallo di Troia

Ho letto l'articolo di Dario Orlandi pubblicato a pag. 33 di *PC Professionale* di Gennaio 2014 e condivido le sue opinioni sul "crapware" che infesta i nostri computer. Sono stato quindi entusiasta nell'apprendere l'esistenza di un software che potesse se non risolvere almeno mitigare il problema, ma i risultati sono stati molto deludenti. Dopo aver scaricato dal sito ufficiale e aver installato AdwCleaner, la prima cosa che l'utility ha fatto è stata installare la barra strumenti Iminent, con la conseguente modifica della pagina iniziale di Firefox. Mi spiace constatare che anche professionisti come voi possano cadere in queste trappole.

Francesco Murolo

Il software segnalato sulle pagine di *PC Professionale* è sottoposto a verifiche

accurate e vengono prese tutte le precauzioni per garantirne l'affidabilità. Analizzando la segnalazione del nostro lettore abbiamo constatato che sul sito ufficiale di AdwCleaner talvolta sono presenti banner fuorvianti: nei riquadri pubblicitari vengono visualizzate immagini che riproducono un pulsante di download e che possono quindi trarre in inganno l'utente. Facendo clic sull'immagine si viene rimandati a una pagina gestita dallo sponsor pubblicitario e che contiene materiale non collegato con il sito d'origine. Queste situazioni, che si stanno sempre più diffondendo, non sono colpa del sito che ospita il banner pubblicitario, in quanto il materiale visualizzato è gestito dalla concessionaria di pubblicità in maniera del tutto indipendente. Il proprietario delle pagine web non ha alcun modo di verificare la liceità del materiale o di escludere eventuali indicazioni malevole. Come segnalato dal lettore, i siti che offrono utilità gratuite per la sicurezza informatica sono presi di mira proprio dai produttori di malware, adware e greyware e sempre più spesso sono utilizzati per la diffusione delle minacce che dovrebbero contribuire a eliminare. In passato anche su

siti che distribuivano Spybot Search & Destroy e Malwarebytes Anti-Malware si erano verificate situazioni analoghe a quella descritta. Contro i problemi di questo tipo non esistono strategie che garantiscano la totale sicurezza. L'unico accorgimento che possiamo consigliare consiste, prima di cliccare, nel passare il puntatore del mouse sull'icona che raffigura il pulsante di download e leggere, nell'ultima riga in basso della finestra del browser, l'indirizzo cui si verrà rinviati: se il link fa riferimento a un file contenuto nello stesso sito si avrà una buona probabilità che il materiale sarà affidabile. Se invece rimanda a siti diversi o a indirizzi Ip numerici sarà preferibile eseguire verifiche aggiuntive, per esempio una scansione antivirus del file scaricato, prima di passare alla sua installazione. Purtroppo, anche questo suggerimento non è risolutivo perché, al fine di garantire una velocità di trasferimento più elevata, molti siti preferiscono appoggiare i file da scaricare su servizi esterni di download a elevata disponibilità e quindi è possibile che anche materiale affidabile non provenga direttamente dal sito ufficiale dei produttori.

Office 2013 e la visualizzazione dei file recenti



Per motivi di sicurezza e privacy ho necessità di rendere invisibili tutti i file recenti di Office 2013. Per esempio, in Excel tramite l'opzione File/Opzioni/Impostazioni avanzate/Mostra questo numero di cartelle di lavoro recenti posso impostare a zero il numero di file visualizzati, ma è sufficiente modificare questo valore per far riapparire tutte le informazioni. La funzione File/Apri/Files Recenti/Cancela cartelle di lavoro escluse fornisce anch'essa una soluzione temporanea, ma le informazioni future continueranno a essere disponibili. Ho verificato anche che fossero impostate a 0 le chiavi del Registro di sistema

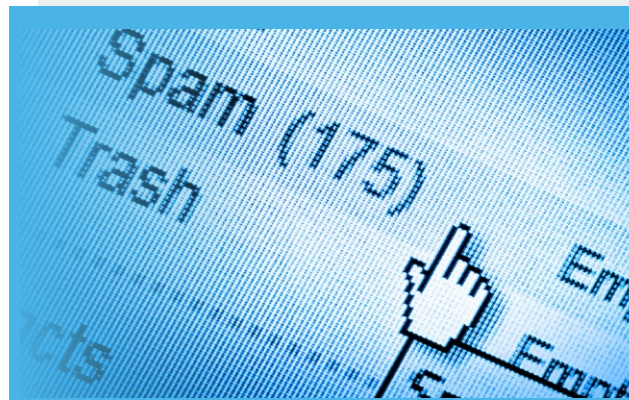
```
Hkey_Current User/Software/
Microsoft/Office/14.0/Excel/File
MRU/Max Display
Hkey_Current User/Software/
Microsoft/Office/14.0/Excel/Place
MRU/Max Display.
```

Questa soluzione ha funzionato perfettamente fino a Office 2010, ma non sembra

Notifica di ricezione di email mai spedite

Ho un computer basato su Windows XP e uso Microsoft Outlook come client di posta elettronica. La protezione del computer è garantita dall'antivirus incluso nella System Suite Professional di Avanquest. Outlook è configurato per la ricezione automatica della notifica di consegna delle email. Da qualche tempo sto ricevendo diversi avvisi di messaggi non consegnati, inviati a indirizzi sconosciuti e quindi relativi a mail non inviate da me. Si va da 2 a 20 notifiche al giorno. Ho pensato a un'infezione virale, ma scansioni effettuate anche con diversi antivirus online, compreso Kaspersky, non hanno rilevato nulla. Credo che se ci fosse un qualche cavallo di Troia che invia spam dovrei ricevere le notifiche di consegna anche dei messaggi regolarmente pervenuti e non solo di quelli rifiutati. Potete darmi un'idea circa l'origine del problema?

Maurizio Bortolin



Gli hacker utilizzano metodi sofisticati per diffondere lo spam. Le mail indesiderate possono provenire direttamente da computer infetti o essere inviate con tecniche di spoofing che mascherano il vero mittente.

Per anomalie del genere, la prima operazione consiste nell'accertarsi che l'origine non sia virale e che il computer non sia utilizzato per inviare email indesiderate per conto terzi. Le ripetute scansioni eseguite dal lettore sembrano escludere questa possibilità, anche perché gli indirizzi email presenti nelle notifiche non appartengono alla rubrica dei contatti del client di posta elettronica. Un comportamento tipico dei virus postali è di utilizzare l'elenco degli indirizzi per i propri invii, per fare in modo che il destinatario legga il messaggio in quanto proveniente da un mittente conosciuto.

Escludendo la presenza di software indesiderato, in base alle modalità operative descritte restano due possibilità: un hacker potrebbe essersi impossessato della password dell'account di posta elettronica e lo starebbe utilizzando per l'invio di spam. Avendo a disposizione i dati di accesso, il malintenzionato può inviare le email "pirata" direttamente dal proprio computer. Il vero proprietario dell'account di posta elettronica, però, riceve gli errori di recapito relativi a eventuali indirizzi inesistenti oppure le notifiche di ricezione. In questo caso, per risolvere il problema è sufficiente cambiare la password avendo cura di sceglierne una complessa, difficile da individuare.

Se anche dopo il cambiamento della password si continuasse a ricevere le notifiche, è probabile che l'hacker stia utilizzando una tecnica chiamata spoofing. Questo metodo consiste nel fare sì che le email risultino inviate da altri utenti, in modo che questi si prendano la colpa di aver prodotto spam o altri disservizi collegati alle spedizioni massive. Purtroppo, in questo caso non c'è niente che si possa fare, lo spoofing ha origine sul computer dell'hacker e passa per altri host sparsi in giro per il mondo, rendendo impossibile ogni contromisura. Anche la chiusura dell'account utilizzato dall'hacker per gli invii non avrebbe esiti pratici, in quanto l'indirizzo continuerà a essere utilizzato ed eventualmente ricondotto al precedente proprietario. In casi come questo non rimane altro da fare che ignorare le notifiche e sperare che l'accesso alla Rete utilizzato dal pirata informatico sia bloccato dal suo provider o dai gestori dei server postali.

valida con l'ultima versione della suite di Microsoft. C'è un'altra soluzione?

Lettera firmata

Nella suite Office 2013 le chiavi di registro che regolano la visualizzazione dei file recenti si trovano alla posizione:

```
Hkey_Current_User \Software\
Policies\Microsoft\Office\15.0\
Excel \Place Mru!Max Display
Hkey_Current_User \Software\
Policies\Microsoft\Office\15.0\
Excel \File Mru!Max Display
```

Anche in questo caso, l'impostazione a 0 di questi valori non esclude la creazione della cronologia di utilizzo dei file, ma serve solo a impedire la visualizzazione. L'accesso ai file, infatti, è gestito da parametri più generali, a livello del sistema operativo. In Windows 7, il modo più sicuro per ottenere il risultato prefissato è di modificare le politiche di gestione della cronologia con la seguente procedura:

1. Eseguire l'editor dei Criteri di gruppo locali (*Gpedit.msc*).
2. Nel riquadro a sinistra, espandere il ramo *Configurazione utente*.
3. Espandere la sezione *Modelli amministrativi*.
4. Selezionare la voce *Menu Start e barra delle applicazioni*.
5. Nel riquadro a destra, fare doppio clic su *Non mantenere la cronologia dei documenti aperti recentemente*.
6. Nella successiva finestra di dialogo, selezionare l'impostazione *Attivata*.

In Windows 8, è stato segnalato che le impostazioni precedenti non ottengono il risultato sperato. Perciò, è necessario modificare il Registro di configurazione aggiungendo la chiave *NoRecentDocsHistory* nella posizione

```
Hkey_Current_User\Software\
Microsoft\Windows\
CurrentVersion\Policies\Explorer
```

e assegnarle il valore *Dword 0x01*. Allo stesso modo è necessario creare la chiave *ClearRecentDocsOnExit* nella posizione

```
Hkey_Current_User\Software\
Microsoft\Windows\
CurrentVersion\Policies\Explorer
```

Anche in questo caso si dovrà assegnare un valore *Dword 0x01*. Con queste impostazioni si dovrebbe riuscire a tutelare la propria privacy durante l'utilizzo delle applicazioni di Office 2013.

Firefox e la cronologia di navigazione

Da qualche tempo ho un problema che si presenta durante le ricerche su Google con Firefox. Se dalla pagina dei risultati visito un link e poi premo il pulsante *Indietro* per tornare alla pagina precedente, si apre una finestra vuota del search engine.

Attraverso la cronologia riesco a risalire alla pagina di ricerca, ma, dato il numero molto elevato di interrogazioni sul web, procedere in questo modo è molto fastidioso e mi costringe a cambiare browser. Ho cercato in diversi modi di risolvere il problema, ma non sono ancora riuscito a venirne a capo.

Paolo Gaspari

L'inconveniente descritto dal lettore è stato segnalato più e più volte nei forum dedicati allo sviluppo del browser di Mozilla. L'anomalia sembra essere collegata ad alcune impostazioni del motore di rendering, tra cui lo zoom di visualizzazione, che può essere regolato con la pressione contemporanea dei tasti *Ctrl +*, per aumentare la

dimensione, e *Ctrl -*, per diminuirla. Nonostante il problema sia già stato comunicato da diversi utenti, il team di programmatori non ha ancora sviluppato una soluzione specifica. Tuttavia, alcune procedure permettono almeno di aggirarlo.

Quella più semplice consiste nell'impostare Firefox in modo che utilizzi come valore predefinito un livello di zoom più basso rispetto a quello che provoca il malfunzionamento. Purtroppo, questa soluzione non è adeguata per tutti gli utenti.

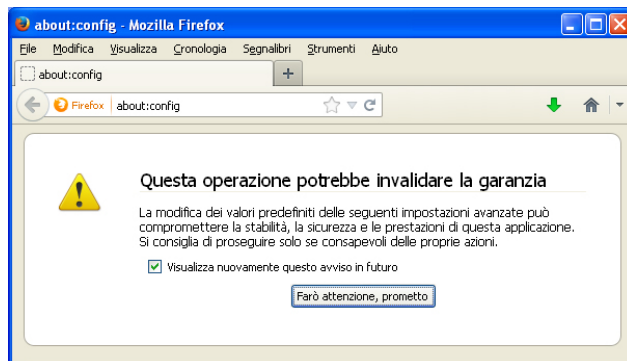
Un'alternativa che sembra avere maggior probabilità di successo è la seguente:

1. Aprire una nuova finestra di Firefox.
2. Nella barra degli indirizzi, digitare *about:config* e premere *Invio*.
3. Premere il pulsante *Farò attenzione, prometto*.
4. Nella barra di ricerca digitare "sessionhistory", che individuerà il parametro etichettato *browser.sessionhistory.max_total_viewers*.
5. Impostarlo al valore 0.
6. Confermare la scelta e chiudere tutte le finestre di Firefox.

Altri utenti hanno segnalato di aver risolto il malfunzionamento disabilitando la funzione di completamento automatico di Google:

1. Nella pagina iniziale del motore di ricerca fare clic sulla voce *Impostazioni* in basso a destra.
2. Nel menu contestuale, selezionare *Impostazioni di Ricerca*.
3. Nella sezione *Previsioni Google Instant*, spuntare la voce *Non mostrare mai i risultati di Instant*.
4. Premere il pulsante *Salva* in basso.
5. Chiudere la finestra e aprire di nuovo il motore di ricerca.

Nei computer condivisi tra più utenti, le liste dei documenti recenti possono creare problemi di riservatezza.



About:config è la pagina di Firefox che consente di modificare i parametri operativi del browser. Un chiaro ammonimento mette in guardia l'utente sui rischi dell'operazione.