

Una delle eventualità più temute dall'utente pc è quella di sospettare (magari erroneamente) che il proprio sistema sia stato colpito da un virus: un malfunzionamento dovuto ad altre cause, un comportamento anomalo di un'applicazione (impossibilità di eseguire alcune funzioni), rallentamenti improvvisi...ecco tutta una serie di situazioni che potrebbero portare a pensare alla presenza di un virus nel proprio sistema...

Ora che il "tarlo" è entrato nella mente dell'utente nulla lo può tranquillizzare, fino alla matematica certezza che la situazione presto sarà nuovamente sotto controllo: per questa ragione niente è meglio di un controllo rapido ed efficace.

Per esperienza personale mi è capitato di imbartermi in sistemi che, pur "infetti", ad una scansione approfondita effettuata con un antivirus aggiornato risultavano (incredibilmente) "puliti": probabilmente ciò dipende dal fatto che l'antivirus è stato installato in seguito ad un'avvenuta "infezione".

Altro evento frequente è l'impossibilità di avviare una scansione con il proprio antivirus proprio perché il virus ne ha compromesso la funzionalità.

Quindi, come comportarsi in caso di sospetta "infezione"?

Io consiglio di procedere seguendo i "10 passi" sotto riportati (grazie a "Spigolo", aka Paolo Angioni, per alcuni input davvero interessanti):

### **1 - scaricare un antivirus freeware per uso personale (e VirIt - vedi punto 9)**

# un elenco di antivirus gratuiti si trova [QUI](#) (elenco a fondo pagina) - io consiglio, in ordine di preferenza personale, AntiVir o AVG o Avast

# AntiVir appena scaricato non necessita di aggiornamento (sono comprese le ultime "firme" già nel file di installazione); AVG si può aggiornare appena installato direttamente da internet; per Avast basta scaricare il file "VpsUpd.exe" alla pagina <http://www.avast.com/.../>.

### **2- gli utenti 'Windows ME o XP' devono disattivare il ripristino della configurazione di sistema**

# funzione da riattivare solo a giochi fatti e sicuri che il proprio pc sia "pulito"

### **3 - scollegare il computer da internet (o, se si è collegati in rete, dalla rete stessa)**

# è sufficiente scollegare il cavo del modem o della scheda di rete (internet può essere vettore di virus)

### **4 - riavviare il pc in modalità provvisoria (premendo F8 in fase di avvio)**

# chi per qualche ragione non riuscisse a ripartire in modalità provvisoria può parzialmente supplire a questo disabilitando momentaneamente i programmi in esecuzione automatica (start-esegui-msconfig-ok-pannello Avvio o Esecuzione

automatica) - si tratta di un'operazione volta a neutralizzare eventuali programmi "maligni" in avvio automatico e, se c'è, l'antivirus residente (per evitare conflitti altrimenti probabili)

**5 - installare l'antivirus poco prima scaricato (e aggiornato!)**

**6 - effettuare una scansione approfondita del sistema e lasciar lavorare l'antivirus**

**7 - (terminata la scansione) riavviare normalmente il pc**

**8 - Effettuare un'ulteriore scansione di controllo: per questa io consiglio di usare "Vir.It eXplorer Lite International Edition"**

# si tratta di un antivirus/antimalware molto valido (ma non gratuito) disponibile alla sezione "Download" del sito [http://www.tgsoft.it/italy/index\\_ita.html](http://www.tgsoft.it/italy/index_ita.html) (alla stessa pagina è presente una descrizione delle caratteristiche del programma). Una volta installato va aggiornato e, riavviato il pc, effettuata la scansione, al termine della quale si può procedere alla sua disinstallazione.

**9 - disinstallare, se nel sistema sono ora presenti due antivirus, quello di cui ci si fida meno**

# se si decidesse di tenere quello che si usava in precedenza, assicurarsi che funzioni correttamente prima di disinstallare l'altro (ci sono virus che neutralizzano l'antivirus che trovano installato nel sistema)

**10 - riabilitare i programmi in esecuzione automatica**

# solo quelli necessari!!! => fare riferimento alla pagina

[www.3feetunder.com/.../startup/...](http://www.3feetunder.com/.../startup/...)

**NOTA:** il fatto che alcuni antivirus siano gratuiti per uso personale non significa questi siano meno efficienti rispetto a "colleghi" più famosi e costosi: la loro efficienza è almeno pari a questi ultimi, ed anzi sono da preferire in termini di risorse richieste al sistema, essendo molto più "leggeri" e meno "invasivi". Io uso con soddisfazione Antivir da qualche anno (molti tra i miei clienti ed amici usano con altrettanta soddisfazione Avast, preferendo l'utilizzo di un antivirus in italiano) e l'unico antivirus a pagamento che ho provato con cui lo scambierei è "Virt" (di cui si parla al punto 9) o "Nod32" - chi lo volesse provare può scaricare la demo funzionante 30 giorni dal sito web della società produttrice - <http://www.nod32.it>

-----

L'ideale per me sarebbe però effettuare una scansione approfondita del sistema ancor prima che il sistema operativo venga caricato.

Avira ha realizzato "Avira AntiVir Rescue System", un eseguibile che consente la creazione di un cd-antivirus bootable che permette la scansione del sistema senza dover prima caricare il sistema operativo (Avira fornisce un file .exe che eseguito procede alla creazione di un cd avviabile).

Un'altra valida alternativa è rappresentata dal Rescue Disk offerto da Kaspersky (a differenza del primo, quest'ultimo necessita poi di un aggiornamento prima di essere pienamente operativo).

I riferimenti di entrambi si trovano alla pagina [www.romanelmondo.it/programmi-gratuiti](http://www.romanelmondo.it/programmi-gratuiti).

## §

A tale scopo può anche essere utilizzata una suite come "UBCD4Win" (<http://www.ubcd4win.com>) nella quale, oltre all'antivirus, possono essere compresi molti altri strumenti diagnostici e di controllo.

Un'altra opzione potrebbe essere quella di usare un antivirus che non necessita di installazione: nella suite "WinPenPack" ([www.winpenpack.com](http://www.winpenpack.com)) è possibile, così come nei cd-live, trovare oltre all'antivirus anche altri tools per la rimozione di "ospiti sgraditi" (malware di vario genere), anche se in questo caso si lavora a sistema operativo già caricato (opzione inutilizzabile qualora ci siano dei problemi per cui è impossibile accedere a Windows).