Guida - Come NON Cadere nella Rete

Ovvero come difendersi dalle insidie di internet per “navigare” sicuri nella “grande rete”

RELEASE 3 – Maggio 2009
per scaricare una copia della guida in formato .pdf cliccate qui

Indice:

PREMESSE
Su consiglio di alcuni utenti del News Group Microsoft, visti alcuni errori, ho deciso di fare un nuovo “aggiornamento” e sopratutto di inserire a fondo guida le spiegazioni di come tentare l'eliminazione di uno o più files infetto/i.

Bene.. iniziamo....

Molti utenti “neofiti” - a cui è dedicata la guida - pensano che un pc protetto da un qualsiasi antivirus (magari un Norton non aggiornato e scaduto essendo una versione trial venduta assieme al pc) possa proteggerli da tutto senza considerare che, la “grande” rete, è un luogo a dir poco “ pericoloso” nel quale, per poter vivere “tranquilli”, bisogna sapere certe norme di “sopravvivenza” basilari.
Questo è quello che spero di riuscire a spiegare soprattutto agli "avventurosi" di internet i quali si accorgono sempre troppo tardi che un dialer ha composto decine e decine di chiamate verso numeri internazionali (= parecchie centinaia di Euro sulla bolletta).
Chi acquista il suo primo pc è affascinato dalle stupefacenti possibilità di Internet e, più o meno coscientemente, lo collega in rete senza nessun accorgimento ritrovandosi presto il pc infetto con relativo “rientro forzato” in assistenza che, oltre a rappresentare una scocciatura, può essere anche costoso.
Proprio per questo in questa guida cercherò di indicarvi una via per rendere il pc “sicuro” ma in maniera totalmente gratuita !!!!
Come?
Scegliendo software free e,ove possibile, in Italiano.
COSA E' UN “VIRUS” INFORMATICO?
Senza entrare nello specifico prima di tutto vediamo di capire cosa sono quei particolari software (programmi) creati per “infettare” altri programmi e chiamati in maniera “generica” virus;
a prescindere a quale tipologia appartiene (dopo cercherò di fare una breve panoramica su quelle più comuni) TUTTI questi software nascono con l'intento più o meno serio di recare “danni” all'ignaro utente del pc (che possono variare dall'apparizione di fastidiose schermate pubblicitarie al tentativo di furto dei vostri dati bancari per “ripulirvi” il conto corrente....)

Spero abbiate capito che difendersi è vitale non un semplice “optional”!!!

Un virus come si diffonde?

La diffusione dei primissimi virus (anni 1980 circa) avveniva tramite floppy disk quindi inserendo nel proprio pc il floppy (i cd-rom all'epoca erano ancora fantascienza) dell'amico/collega si rischiava di venire infettati..... con una diffusione piuttosto limitata.....

Oggi sfruttano la “grande rete” internet e le connessioni presenti su tutta la terra.... i rischi sono divenuti molto più elevati con la concreta possibilità di una infezione mondiale come accaduto per certi virus i quali hanno fatto impazzire mezzo mondo infettando pc in ogni angolo del globo.

Ma cosa è e cosa fa un virus?

Il “virus” non è altro che un piccolo programma scritto per alterare il funzionamento del computer o di un determinato programma logicamente senza il consenso o la consapevolezza dell'utente.

Come per tutti i “programmi” necessita di essere eseguito (= avviato) per proseguire nel suo “effetto” e per fare questo ha bisogno di:

- camuffarsi in maniera che sia l'utente stesso ad avviarlo
- Inserendo il proprio codice assieme ad un altro programma “innocuo” avviandosi insieme ad esso

Questo, chiaramente, è molto ma molto indicativamente quello che un “virus” ha bisogno per tentare la sua azione più o meno distruttiva....

QUALI SONO I RISCHI PIU' COMUNI?
Qui di seguito, prima di approfondire il discorso su quali software installare e perché, riporto le categorie principali delle minacce più comuni.
Ricordo che, anche se chiamati comunemente “virus”, non tutte le minacce sono “virus” ma a seconda del loro “atteggiamento” vengono catalogati in diverse “famiglie”.
Vediamole assieme:

Worm
Questa categoria si diffonde sfruttando le vulnerabilità del S.O.. (per questo è importante scaricare ed installare SEMPRE gli aggiornamenti del proprio S.o.)
Una volta penetrati in un computer , attraverso reti,posta elettronica e simili canali, cercano altri pc connessi nella stessa rete e tentano di inviare repliche di se stessi. Molte volte vengono utilizzati i dati contenuti in rubrica o nel client di posta elettronica. Queste caratteristiche consentono ai worm una rapida velocità di diffusione.

Virus
Programmi che infettano altri programmi aggiungendo il proprio codice maligno in maniera da “scatenare” la loro procedura distruttiva nel momento in cui si avvia il programma infettato.
Oltretutto molti di essi si “moltiplicano” come i virus biologici!
Alcuni hanno anche la capacità di modificarsi (parzialmente o completamente) autonomamente ad

ogni infezione rendendone più difficile il riconoscimento e la rimozione. (prendendo il nome di Virus polimorfici e Virus metamorfici)

Trojan
Programmi che eseguono azioni non autorizzate e che fanno da "cavallo di troia" tentando di scaricare, una volta penetrati nel pc, altri software maligni o tentando di "aprire la strada" a qualche craker (persone fisiche che tentano di prendere il controllo in remoto di un altro pc) con lo scopo di trafugare dati personali, documenti, indirizzi di posta o peggio dati bancari, ecc.

Adware
Codice di programma incluso in software, generalmente free, progettato per far visualizzare finestre e messaggi pubblicitari indesiderati (pop-up ed affini). Spesso raccolgono anche informazioni personali e modificano le impostazioni di sicurezza del browser (home page, motore di ricerca predefinito, livello di sicurezza, ecc.).

Spyware
Software che raccolgono informazioni sull'utente a sua insaputa tentando di inviare allo sviluppatore informazioni riservate come:

- Azioni dell'utente sul pc
- Quali programmi sono installati
- Raccogliere informazioni sul tipo di connessione, siti visitati ecc,

Rootkit
Utilità (si fa per dire !!!) che tentano di nascondere all'utente attività nocive nell'intento di impedire all'antivirus di riconoscere o individuare il/i file infetto/i.
Sono molto pericolosi e generalmente complessi da rimuovere perché in molti casi intaccano il registro del S.O.

Dialer
Virus concepiti allo scopo di creare una nuova connessione di tipo analogico sul proprio pc: il modem avvia una connessione verso numeri a pagamento e sul pc vengono aperte schermate con siti a carattere quasi sempre a "luci rosse".
Sono molto pericolosi poiché oltre a quanto indicato (ricordo che questo genere di connessione può costare anche molte centinaia di €) possono veicolare il download di altri virus e modificare le impostazioni del browser.
Generalmente, per rimuoverli occorrono dei Tool specifici.

N.B. questi virus possono agire solamente in pc dotati di modem analogico. Se il vostro pc è connesso tramite linea ADSL e non ha un modem analogico connesso, un dialer, NON può causare i problemi sopra descritti.
Esistono però dei Dialer che riescono a modificare le impostazioni del modem ADSL ma, niente di grave.
In parole semplici viene bloccata la navigazioni perché le impostazioni sono errate: basta ripristinarle e il "gioco" è fatto.

Altri generi
Esistono anche particolari infezioni che presentano caratteristiche "miste" cioè riescono a compiere "funzioni" di più categorie contemporaneamente

Altre minacce

Esistono solo queste minacce?
NO!
Purtroppo esistono altri generi di rischi come truffe on-line,siti camuffati , attacchi diretti al proprio pc.....
Chiaramente se si installeranno i software adeguati i rischi si riducono ma ricordo un famoso detto:
L'unico pc davvero sicuro è un pc spento!

PRIMO PASSO
INSTALLARE I SOFTWARE DI SICUREZZA
La prima cosa da fare, ripeto PRIMA di accedere ad internet, é installare i programmi essenziali per la prevenzione e la sicurezza:

- Antivirus
- Firewall
- Antispam

ai quali aggiungerei:

- Anti Spyware e Malware
- Anti Rootkit
- Anti Dialer
- Programma di controllo su quale sito si sta effettivamente navigando
- Filtro blocca banner pubblicitari ed affini

Esaminiamo assieme la funzione di ogni singola categoria
ANTIVIRUS
Il software antivirus protegge il pc dalla stragrande maggioranza di software "maligno".
Come accennato all'inizio voglio indicare agli utenti come proteggersi "gratis" quindi prenderò in considerazione i 3 più famosi software di protezione gratuiti presenti sul mercato:

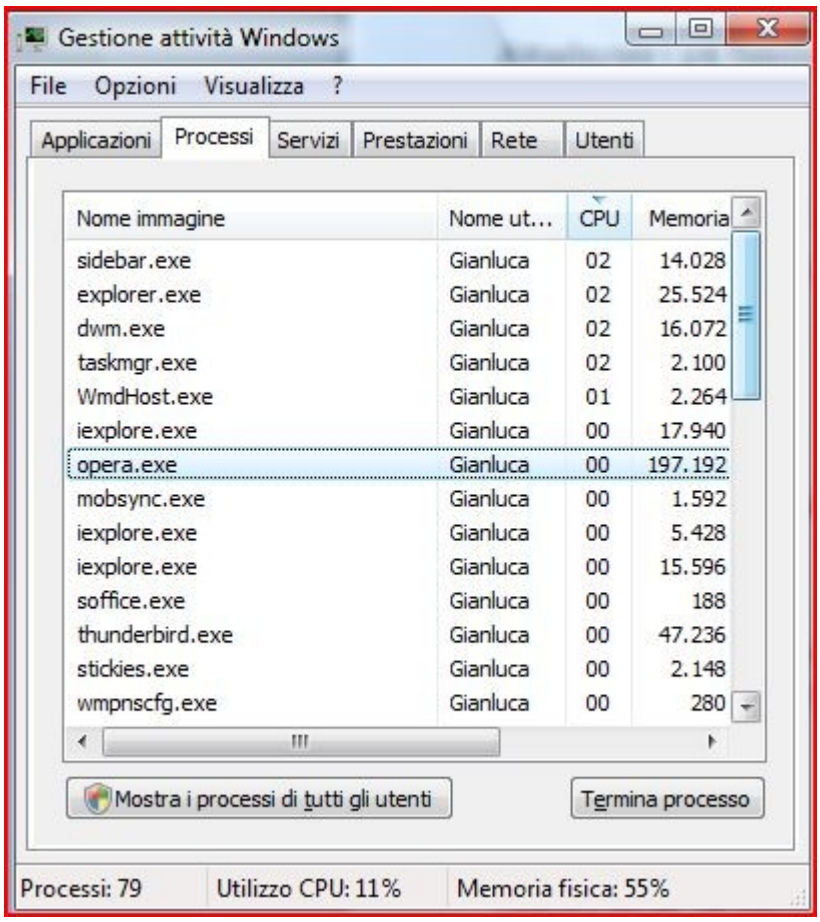

AVG free
http://www.avg.com/it.product-avg-anti-virus-free-edition

Questo antivirus integra anche la funzione antispyware ed il "safe search" cioè una protezione sulle ricerche in internet: aiuta a riconoscere tramite comode icone se i siti che appaiono nelle ricerche sono sicuri o meno (funzione simile al McAfee Site Advisor descritto più avanti)
Mi sembra giusto ricordare la grossa "papera" di AVG di qualche tempo fa: l'antivirus in questione ha riconosciuto come infetti degli essenziali file di sistema..... al riavvio i pc "colpiti" non avviavano!
il prodotto è buono ma una software house di questa importanza poteva evitare simili errori .....
speriamo che non si ripetano casi simili in futuro
"*sbagliare è umano perseverare è diabolico*".....


Avast! Home Edition
http://www.avast.com/eng/download-avast-home.html
Altro famoso antivirus free..... a differenza degli altri ,anche se totalmente gratuito, richiede di registrare la propria copia rilasciando una licenza free della durata di un anno
Dopo il 1° anno bisogna semplicemente rifare la registrazione.. sempre gratuita
Offre una buona protezione.... ed ha una funzione "unica"; la possibilità di effettuare la scansione antivirus prima dell'avvio di Windows !

 **Avira Antivir**
http://www.free-av.com/
Uno dei più famosi ed apprezzati antivirus free... veloce nelle scansioni ed anche piuttosto leggero.... unica “pecca” oserei dire che consiste nelle fastidiose finestre di invito all'acquisto della ver. completa che appaiono di tanto in tanto !
Gratis non si può volere tutto :)

FIREWALL
Altro software di primaria importanza, il firewall controlla il traffico da e verso la rete che avviene nel vostro pc.... diciamo che assomiglia ad una “dogana” !
Quando viene rilevato un software che tenta di accedere ad internet ,qualsiasi firewall usiate, apparirà una richiesta di consenso o meno..... questo, logicamente, comporta una scelta da parte dell'utente che, soprattutto se nuovissimo nel mondo dell'informatica, potrebbe trovarsi di fronte al non facile compito di dare o meno l'ok al processo.
Come norma generale si dovrebbe considerare quali software sono installati sul pc e quali si “aggiornano” in rete automaticamente.
Se non sapete neanche da dove partire , non sapete nemmeno cosa significa il “.exe” ..... francamente vi sconsiglio di iniziare a navigare senza aver prima appreso qualche nozione di base perché di processi in un pc ce ne possono essere davvero tanti e,non per spaventare, un virus può benissimo camuffarsi da processo “lecito”.....
Cito qualche processo di “esempio”:
Explorer.exe
processo fondamentale di Windows: permettere sempre l'accesso
iexplore.exe
browser di navigazione Internet Explorer Microsoft: se lo bloccate non “navigate” da nessuna parte
Firefox.exe
browser di navigazione Mozilla FireFox: se avete installato il browser alternativo FireFox e volete navigare lasciate passare
Opera.exe
Come sopra ma solamente se avete installato il browser Opera
msimn.exe
ovvero Outlook Express - programma di gestione posta elettronica in Windows Xp: lasciare passare sempre.



Questo è il task manager di un pc ...come vedete di processi ce ne sono molti!

Questo tanto per fare un esempio di processi che in un qualsiasi pc esistono..... ce ne sono tanti, ma tanti altri ...(dipende anche da quali e quanti programmi avete installato sul pc).

Ma un firewall oltre a controllare “cosa esce” dal proprio pc controlla anche “chi cerca di entrare”....
Come accennato in precedenza esistono dei criminali informatici che tentano di prendere possesso del vostro pc.... molti si chiederanno il perché di questi attacchi che ,se possono sembrare abbastanza ovvi per un' importante azienda , non si può dire lo stesso dell'attacco ad un pc “casalingo” dove magari i “dati più importanti” sono le fotografie delle vacanze :)

Invece un importante “perché” esiste...
molti attacchi informatici avvengono dai cosiddetti “pc zombie” ….....pc di ignari utenti usati da remoto (= a distanza) SENZA CHE IL PROPRIETARIO SE NE ACCORGA per compiere azioni illegali in maniera di non riuscire oppure riuscire in maniera più difficoltosa a risalire al responsabile dell'attacco
(ad esempio un attacco ad un server sito in Italia può benissimo avvenire da un pc Americano comandato in remoto dalla Cina.....)
Attualmente i più famosi firewall free disponibili sono:

Zone Alarm free
http://www.zonealarm.com

Jetico Personal Firewall

http://www.jetico.com

Comodo che si è più trasformato in una suite di sicurezza dalla ver. 3...)
http://www.personalfirewall.comodo.com

Outpost firewall free
http://free.agnitum.com/
(integra anche un blocco pop-up pubblicitari)

Ne esistono anche molti altri... ma i più famosi sono questi
Adesso devo aprire una parentesi sul firewall già integrato in Windows Xp: il difetto più grande del software integrato dalla Microsoft nel suo sistema operativo è la mancanza di controllo del traffico dal proprio pc verso l'esterno.... questo riduce già in partenza minimo del 50% la protezione offerta.
Discorso molto diverso per il firewall integrato nell'attuale S.o. della Microsoft; Windows Vista
Infatti il software integrato pur rimanendo di utilizzo molto "facile" controlla TUTTE le connessioni.
Quindi si tratta di un software davvero fruibile dall'utente!

ANTISPAM
Abbiamo accennato che il processo msimn.exe corrisponde al software di gestione della posta elettronica Outlook Ex. In Xp (Windows Vista dispone del nuovo Windows Mail).
Bella cosa la posta elettronica!!!
In pochi istanti uno scritto può essere letto da qui all'altra parte del pianeta: altro che posta prioritaria !!!!
L'unico "difetto" che oltre agli scritti un mail può essere anche "farcita" con foto, file musicali e.... virus.
Anche qui si può rischiare di contrarre qualche infezione.
Ma di questo se ne occupa , come già detto, l' antivirus (almeno ogni software che si rispetti integra il controllo della posta in entrata ed uscita)
Apro quindi la parentesi di fare MOLTA attenzione a cosa si riceve e da chi si riceve.
Oltretutto state ben attenti anche se la mail la ricevete da un vostro conoscente: esistono dei virus che, una volta infettato il pc, "pescano" dalla rubrica gli indirizzi mail che trovano e si autoinviano per tentare di infettare altri pc..... non è per creare inutili allarmismi ma esiste anche questo rischio.
Oltre al "pericolo" allegati esistono anche altre genere di e-mail potenzialmente pericoloso oppure semplicemente fastidiose..... pensate a a quando vedete una partita in televisione.
Ogni tot. Minuti appare il solito e fastidiosissimo spot pubblicitario.....ecco in maniera "ingigantita" capita anche alle mail.
Ad esempio con una media generale su 100 mail:

- E-mail di amici/lavoro: 20/25
- pubblicitarie: 40
- truffaldine: 30

- virus e company: 5/10

Sorpresi?
E se per caso partecipate a Newsgroup, forum e affini i rischi crescono ancora se la vostra mail è "pubblica" (cioè visibile a tutti gli utenti)
Come difendersi quindi?
Innanzitutto utilizzando un antispam: questi software "filtrano" la posta in arrivo ed evitano quanto spiegato sopra.

Personalmente consiglio **Spamihilator:**
http://www.spamihilator.com
gratuito, in italiano ed ampiamente configurabile.
Oltretutto, a differenza di altri software simili, permette di recuperare la posta elettronica che,erroneamente, potrebbe essere stata considerata spam.
In alternativa il nuovo software
Microsoft Windows Live Mail http://download.live.com/wlmail
(da non confondere con Windows Mail che è un altro software)
oppure Mozilla Thunderbird
http://www.mozilla-europe.org/it/products/thunderbird/
integrano una protezione antispam....
Tutti questi software richiedono un periodo di apprendimento durante il quale "imparano" le vostre preferenze; quindi è normale che inizialmente "disturbino" un po' chiedendo cosa è e cosa non è spam !
Un importante consiglio: se per qualche motivo dovreste scrivere pubblicamente la vostra mail su internet (ad esempio in una inserzione di qualche mercatino dell'usato) non scrivete la vostra mail completa.... mi spiego meglio
Mettiamo caso che la propria mail sia mario.rossi@tiscali.it (il provider è solo indicativo potrebbe essere @libero, @alice, @fastwebnet e così via)
Se viene trascritta integralmente così come è su internet c'è un forte rischio che i messaggi pubblicitari aumentino in maniera notevole...
Ma ,come detto, esiste un semplice trucchetto... basta scrivere
mario.rossi@LEVAQUESTOtiscali.it oppure mario.rossi_AT_tiscali.it

Facendo così si riducono (ma non si annullano) i rischi ;)

ALTRI SOFTWARE DI SICUREZZA
Adesso prendiamo in considerazione altri software da installare:

ANTI SPYWARE e MALWARE
Sono software , con funzionamento simile all'antivirus, che a differenza di quest'ultimo sono più "specializzati" verso certi software maligni: spyware e malware per l'appunto.
A differenza degli antivirus solitamente questi programmi non rimangono costantemente attivi ma devono essere avviati manualmente (certi integrano una protezione attiva ma non ha nulla a che vedere con un "classico" antivirus).
Tra i più famosi ricordo:

Ad-Aware
http://www.lavasoft.it
Sicuramente da installare è uno dei più celebri software in questa categoria: l'attuale ver. 2008 integra anche molte funzioni e rileva anche molti generi di software dannosi e non “solo” spyware e malware come nelle precedenti versioni.
Disponibile in italiano

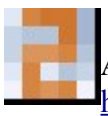
Spybot-S&D
http://www.safer-networking.org
Assieme al precedente è uno dei più famosi software.
Integra qualche utile funzione aggiuntiva: Blocco delle modifiche al registro del sistema (TeaTimer) – da attivare durante l'installazione;
“trita file”: permette di cancellare in maniera definitiva (o quasi) i file. Molto semplice da utilizzare può tranquillamente “convivere” con Ad-aware: basta far ignorare ad entrambi la cartella del programma opposto (in maniera che gli archivi e la “quarantena” non vengano riconosciuti a vicenda.....altrimenti pensereste di avere sempre infetto il pc).
Disponibile in italiano

Spyware Terminator
http://www.spywareterminator.com
Altro software per la protezione da spyware e malware che, a differenza dei primi due, integra una vero e proprio modulo di protezione sempre attiva. E' pesante: occhio se non avete un pc recente.

Disponibile in italiano

SUPERAntispyware
http://www.superantispyware.com

Altro potente spyware... leggero , potente ed è anche rapido nella scansione del pc
Finalmente anch'esso disponibile in Italiano.. anche se la traduzione attuale non è delle migliori



A-Squared Free
http://www.emsisoft.com/en/software/free/
Molto veloce lo trovo anche affidabile nelle sue scansioni.... purtroppo sono stati segnalati dei casi di “falsi positivi” e qualche problemino con l'eliminazione di alcuni malware individuati.

Malwarebytes' Anti-Malware
http://www.malwarebytes.org/

Altro potente software di protezione... funziona molto bene ma,nella sua ver. freeware, bisogna ricordarsi di aggiornarlo “manualmente” ;)

Windows Defender:
http://www.microsoft.com/italy/windows/products/winfamily/defender/default.mspx
INCLUSO E PREINSTALLATO in tutte le versioni di Windows Vista può essere gratuitamente scaricato per Windows Xp dal link indicato

ANTI ROOTKIT
Come indicato inizialmente i rootkit sono pericolosi processi che tentano di nascondere l'attività di virus, malware e altri processi maligni “camuffandoli” in maniera che software antivirus non riesca a rilevarne la presenza nel pc.
Per eliminare questo genere di software maligni esistono specifici software: sicuramente il più famoso freeware (almeno per quanto mi riguarda) è

Sophos Anti-Rootkit.
http://www.sophos.it/products/free-tools/sophos-anti-rootkit.html
Specifico contro questa “calamità” informatica conviene farlo “girare” una volta al mese tanto per sincerarsi che il pc sia “pulito” sotto questo particolare aspetto.
Necessita di registrazione gratuita

ATTENZIONE; purtroppo il programma NON è compatibile con Windows Vista
Per gli utenti di Windows Vista esiste

GMER:
http://www.gmer.net/index.php

Chiaramente sempre free ;)

ANTI DIALER
Come detto in precedenza, i dialer tentano di stabilire una connessione remota a pagamento verso siti “pericolosi”.
Per evitare che la chiamata riesca a “passare” basta installare un semplice e gratuito software che “blocchi” ogni tentativo non autorizzato di connessione.
Tra i disponibili io ho provato

Digisoft

Digisoft antidialer
http://www.digisoft.cc
che è gratuito ed in italiano.... certo non sarà aggiornatissimo come estetica (le icone e la finestra sono in stile Win98) ma è sicuramente funzionale.
N.B. come precedentemente indicato questo rischio "nasce" esclusivamente se sul proprio pc è presente un modem analogico.
Se volete essere sicuri al 100% chiedete alla vostra società telefonica di bloccare le telefonate verso i numeri a tariffazione speciale e verso le chiamate satellitari

ANTI PHISHING / SPOOFING
In questi ultimi mesi c'è stata una vera e propria ondata di e-mail truffaldine rilasciate a nome delle "poste italiane" o di famose banche tutte contenenti link a pagine riprodotte ,delle volte alla perfezione, che invitano l'ignaro utente a rilasciare i propri dati d'accesso con la scusa o del "conto sospeso" , o dell'accredito bloccato o altre stupidaggini simili.
Per identificare immediatamente questo tentativo di truffa esistono degli appositi filtri.
Se utilizzate Internet Explorer 7 , IE8 ma anche Opera Browser 9,6x e Firefox 3 esiste già un filtro antiphishing.
Comunque per tutti gli utenti che abbiano Internet Explorer 8,7 o 6 (se avete ancora questo browser meglio aggiornarlo!) , Firefox ed altri browser esistono 2 piccoli, leggeri e utili programmi gratuiti che, secondo me, sono da installare senza pensarci 2 volte:

McAfee Site Advisor
http://www.siteadvisor.com/
prodotto dalla famosa McAfee si presenta come una piccola barretta nella barra degli strumenti de browser. Durante le ricerche con Google immette vicino ai risultati delle icone di 4 diversi colori:
Verde: sito ok
Arancio: sito con possibilità di spam o software indesiderato
Rosso: sito infetto o che rilascia anche spyware, malware , virus, ecc.
Grigio: sito non ancora verificato.

Allo stesso modo si comporta la "barretta" (che nelle ultime versioni non è proprio "piccolina"....) che si è andata ad insediare nella barra degli strumenti.
Se il sito in cui state navigando è stato riconosciuto come "pericoloso" blocca la navigazione e avverte dei possibili rischi.

SPOOFSTICK
Browse freely but carry a SpoofStick
Spoofstick
http://www.spoofstick.com
Spoofstick "lavora" in maniera più semplice ed immediata: mentre voi navigate lui vi indica in quale sito state effettivamente navigando evitando così di "cadere" in qualche imitazione ben fatta.
Come il primo si installa nella barra del browser: da installare.

FILTRO BANNER, POP-UP ed affini.
Questo è un discorso più personale..... se siete navigatori ai quali non interessa nulla della (fastidiosissima) apparizione di finestre pubblicitarie, banner e simili potete anche evitare di leggere questa sezione.
Considerate però che delle volte gli stessi pop up possono essere "pericolosi" perché invitano alla

navigazione su siti potenzialmente dannosi.
Se siete invece come il sottoscritto che “odia” pubblicità ed affini per i “piedi” allora dovete installare uno specifico software:

WebWasher Classic
http://www.cyberguard.com/products/webwasher/webwasher_products/classic/download/index.html

Ho cercato a lungo ma come programmi “free” ho trovato solo ed esclusivamente questo.
Lavora bene , non è troppo “intrusivo” ed è ben configurabile, difetti?
Beh è solo in inglese.

CONSIGLI E REGOLE COMPORTAMENTALI
Chiudo questa “carrellata” di spiegazioni con qualche consiglio.

- Evitate siti di giochi on-line, suonerie, musica,video sono luoghi “stupendi” per un virus dove trova tanto traffico e poco controllo: quindi massima attenzione a cosa e da dove scaricate file!!!!

- Altra cosa da evitare è l'utilizzo di programmi tipo Emule e simili: siamo sinceri, tanto servono solo per scaricare materiale piratato.. magari l'ultimo album dell'artista preferito oppure un film... Solitamente questi file, oltre ad essere illegali, sono anche “farciti” con virus e affini. Inoltre il PC, di solito, resta per parecchie ore connesso alla rete ..quindi è a rischio. Dal vecchio proverbio “*uomo avvisato, mezzo salvato”*.

- Utilizzate regolarmente un software di pulizia tipo

Ccleaner:
http://www.ccleaner.com

molti virus si posizionano nei file temporanei scaricati da internet.
Per evitare questo basta una “passata” con il programma indicato ed il pc viene “ripulito”.

- Controllate anche le impostazioni di sicurezza del browser che non devono MAI essere impostate a valori “bassi” (nella scheda sicurezza: varia da browser a browser).

Soprattutto nella sezione “siti con restrizioni”(prendendo Internet Explorer ad esempio). il valore DEVE essere impostato al livello di protezione massimo.

- Durante le vostre ricerche in internet state attenti e tenete sempre sott'occhio la barretta del SiteAdvisor e dello Spoofstick.
- Controllate regolarmente l'elenco dei programmi installati e sincerateVi che non ci siano programmi installati a vostra insaputa.
- Stessa cosa per i componenti aggiuntivi del browser di navigazione.
- Aggiornate regolarmente il sistema operativo del vostro pc

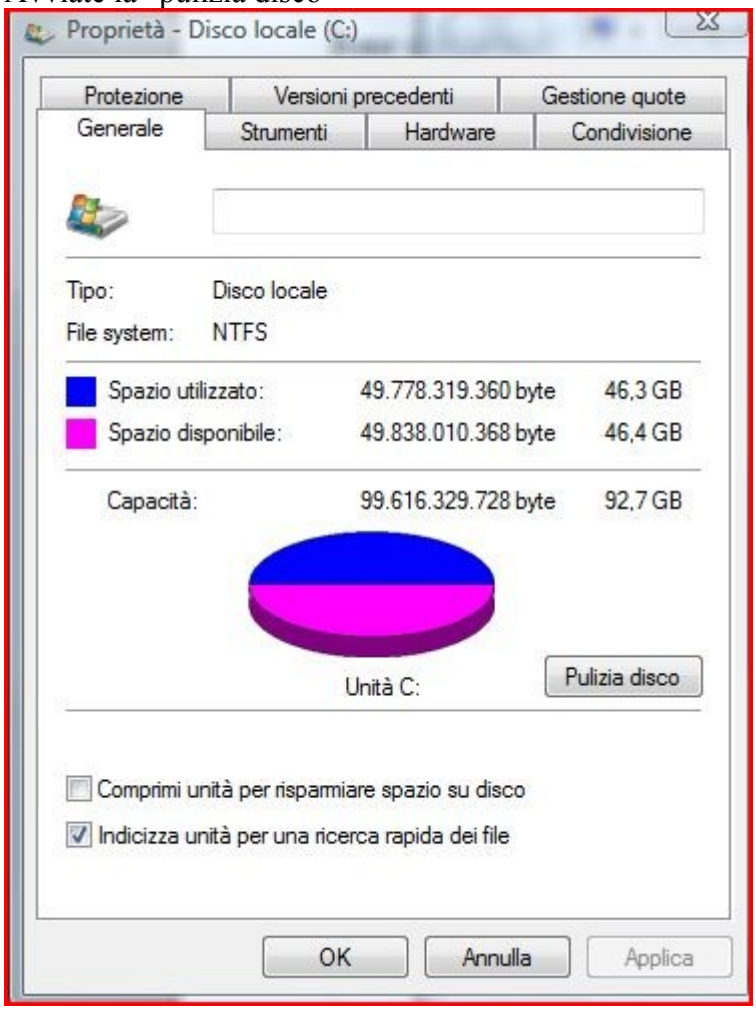
Anche se dovesse capitare che un virus riesca ad entrare non preoccupatevi eccessivamente e non fatevi prendere dal panico!
Seguite l'articolo del MVP Microsoft Vincenzo Di Russo
“**Spyware e malware: chi ci spia?”**
http://technet.microsoft.com/it-it/library/cc645560.aspx

In alternativa,se trovate troppo complesso l'articolo, leggete le procedure suggerite,come inizialmente promesso, nel nuovo capitolo:

Procedure per tentare di rimuovere un virus:
Il pc rallenta?
Apre schermate non volute?
Aprite il task manager e trovate voci strane oppure processi “conosciuti” ma ripetuti più volte?
Insomma siete quasi certi che il pc sia infetto?

Bene cioè male :)

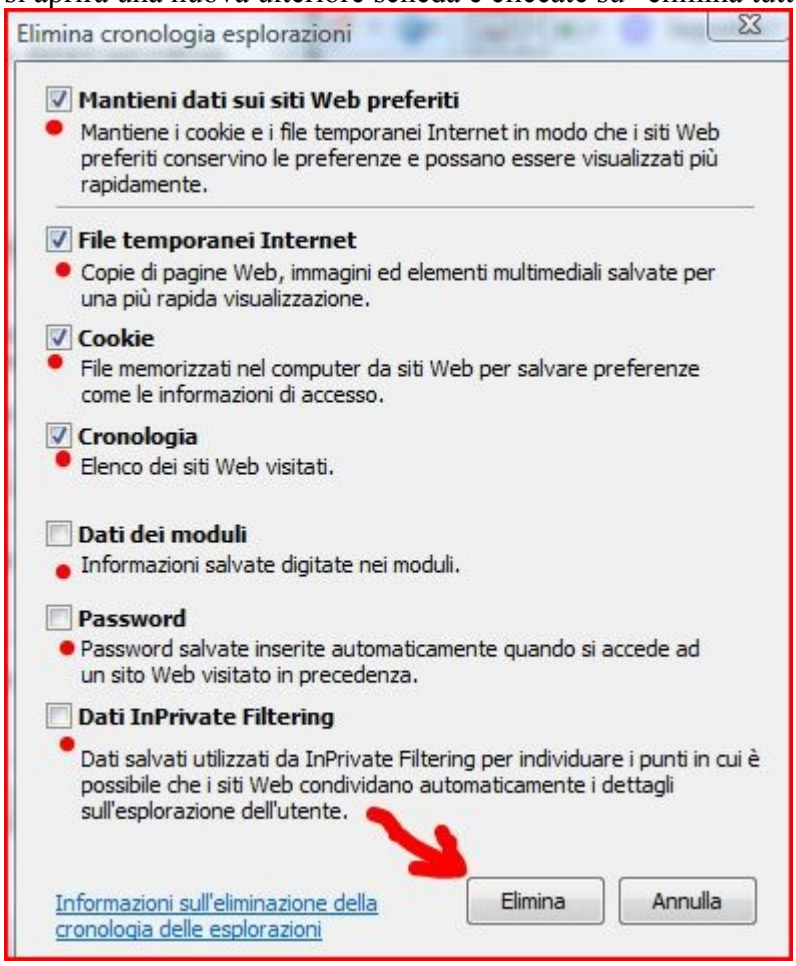
Operazioni Preliminari:
Iniziamo ad isolare il pc da internet scollegando i cavetti di rete.
Riavviamo il computer e ,appena appare la schermata iniziale del bios (la schermata con varie scritte che appare pochi secondi durante l'avvio) iniziate a premere ripetutamente il tasto “**F8**” sulla tastiera.
Dovrebbe apparire una schermata con un elenco definito
“Menù opzioni avanzate di Windows”:
Selezionate:
“Modalità provvisoria”
ed avviate il sistema op.
Andate in “risorse del computer”, selezionate il vostro disco fisso (solitamente “C”) in cui è installato Windows, fate click destro sul disco quindi “proprietà”
Avviate la “pulizia disco”



Ecco come si presenta la schermata “proprietà” di una unità logica in Windows Vista

Dopo questo aprite il vostro browser ed effettuate la pulizia della memoria cache del browser stesso:

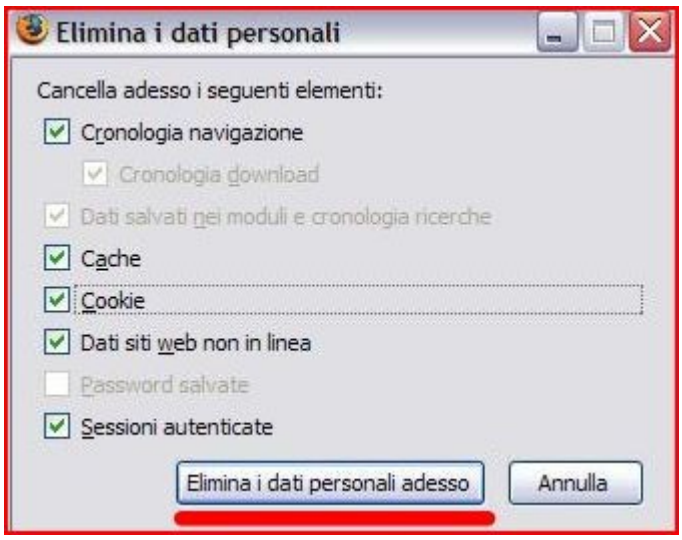
Internet Explorer 7 ed 8:
avviate il programma, cliccate su “strumenti”>opzioni internet
Nella scheda che si aprirà cliccate su “elimina.....” sotto “Cronologia esplorazioni”
si aprirà una nuova ulteriore scheda e cliccate su “elimina tutto” una volta spuntate TUTTE le voci



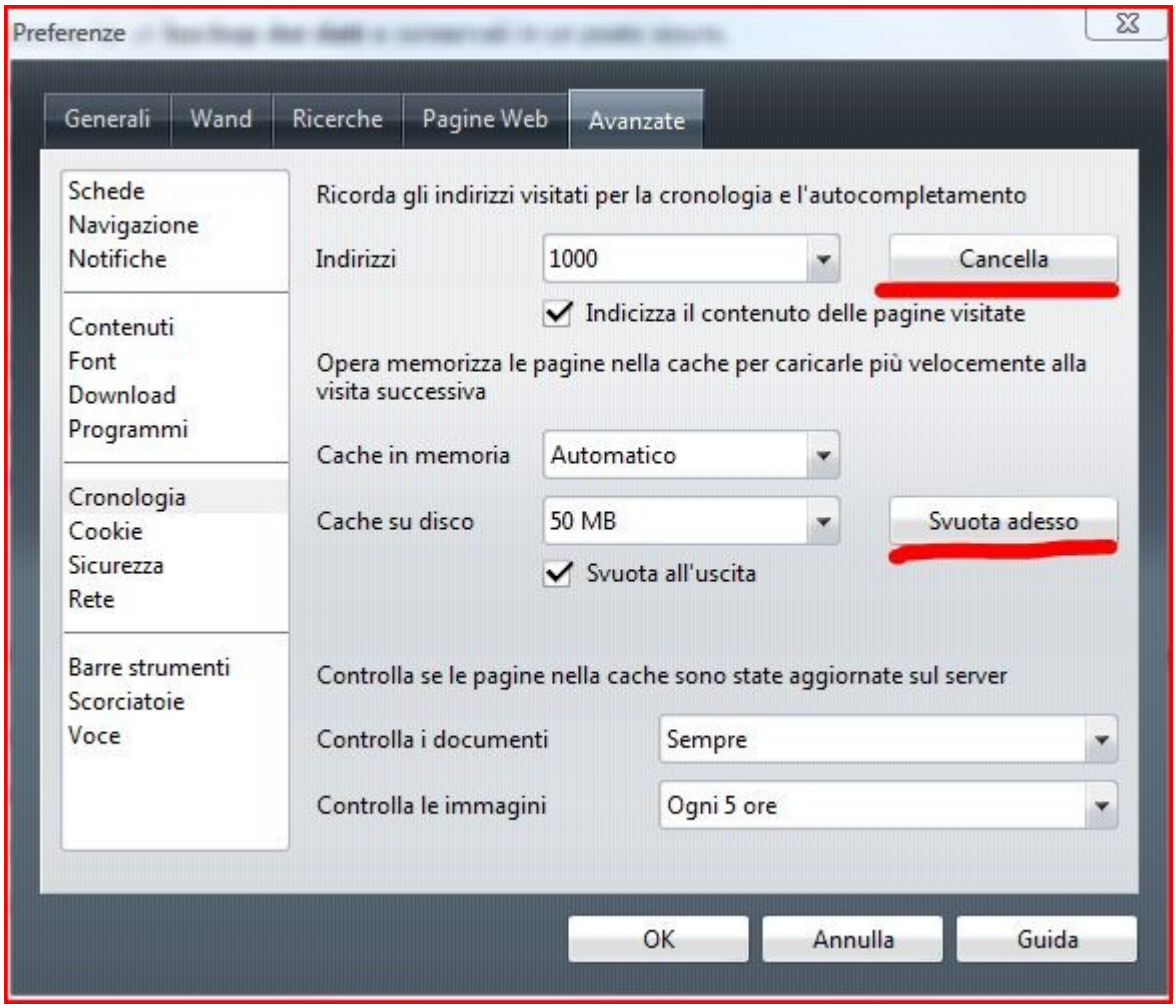
Ecco la scheda che apparirà... spuntate tutte le voci (indicate con i punti rossi) ed avviate l'eliminazione cliccando su “elimina”

Sempre dal menù strumenti cliccate su “gestione componenti aggiuntivi”
Controllate quali componenti sono installati ed eliminate eventuali componenti dei quali ignorate la provenienza

Firefox (ver. 3 del programma):
avviate il programma e cliccate su “strumenti”> elimina i dati personali... > spuntate tutte le voci nella scheda che si aprirà e proseguite con la pulizia
Ecco la schermata di eliminazione dei dati personali di Firefox....



Opera Browser (ver. 9,64 del programma):
Avviate il programma quindi click su "strumenti">preferenze
Nella scheda che si è aperta cliccate su "avanzate" quindi su "cronologia" nel menù sulla sinistra
Cliccate su:
"cancella" a fianco di "indirizzi"
"svuota adesso" a fianco della scritta "cache su disco"



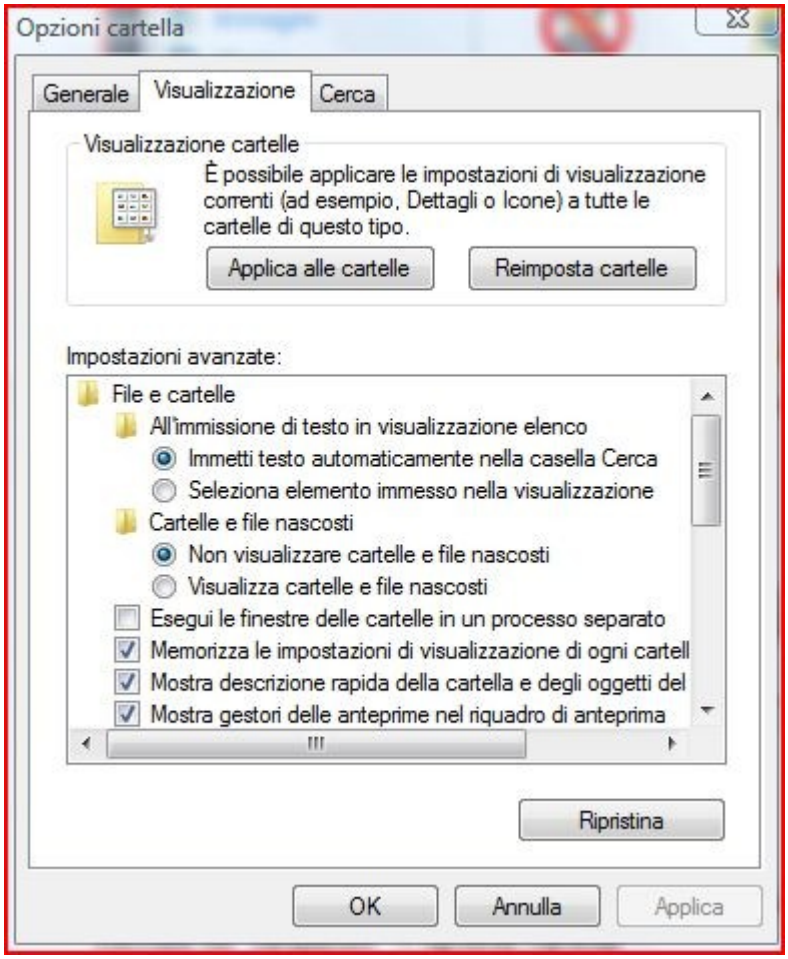
La schermata presente in "preferenze" di Opera Browser..... cliccate sui due pulsanti sottolineati in rosso per effettuare la pulizia

Aprite una qualsiasi cartella (ad esempio documenti")

Con Windows XP:
cliccate su “strumenti” > opzioni cartella”
Nella schermata che si aprirà cliccate su “visualizzazione”
Spuntate le voci:
“ Visualizza cartelle e file nascosti”
“nascondi file protetti di sistema (consigliato)”

Con Windows Vista:
Cliccate su “Organizza” quindi “opzioni cartella e ricerca”
Quindi nella schermata cliccate su “visualizzazione”
Spuntate le voci:
“ Visualizza cartelle e file nascosti”
“nascondi file protetti di sistema (consigliato)”

Ora “applica” ed “ok”



Ecco la schermata “visualizzazione” in “opzioni cartella” Windows Vista.... in Xp è quasi identica

Avviate la ricerca di Windows e cercate i file **.tmp** e **.temp**
Selezionateli ed eliminateli TUTTI quindi svuotate il cestino

ATTENZIONE:
Una volta terminati i controlli e le procedure di “disinfezione” ripristinate le impostazioni di default in “opzioni cartella”
Avviate anche Ccleaner ed effettuate la pulizia anche con il famoso software free
Tentate di eseguire la scansione antivirus in modalità provvisoria; molti antivirus lo permettono

Dopo la scansione con l'antivirus fate “girare” anche Ad-Aware sempre dalla modalità provvisoria
Quando avete completato le scansioni ed eventualmente fatto rimuovere il/i file infetto/i riavviate il computer e ricollegate il cavetto di rete.
Al riavvio , se non cliccate nuovamente F8, il computer si avvierà in modalità “normale”

SCANSIONI :
Una volta riavviato il pc fate effettuare una scansione completa al vostro antivirus e, successivamente, con ogni software di sicurezza precedentemente installato (quindi Ad-Aware, SUPERAntispyware, Spy e Bot, ecc)

ATTENZIONE: prima delle scansioni effettuate l'aggiornamento delle “firme” di ogni software di protezione con il quale si intende eseguire la scansione

Un qualsiasi software di sicurezza non aggiornato è come un medicinale scaduto; può non fare alcun effetto!

NON AVVIATE più software alla volta
Fate effettuare ad ogni software una scansione “completa”

ATTENZIONE: lasciate “lavorare” le varie applicazioni e NON utilizzate il pc durante i vari controlli/scansioni

ricordo ancora una volta l'elenco dei software da utilizzare:

- Ad-Aware
- Spybot-S&D
- Spyware Terminator
- SUPERAntispyware
- Malwarebytes' Anti-Malware
- Windows Defender
- A-Squared Free

Una volta completate queste scansioni utilizziamo anche questo programma:

STINGER:
http://vil.nai.com/vil/stinger/
Particolare utility creata da McAfee in grado di rimuovere oltre 50 virus... non è un software antivirus e nemmeno si “aggiorna”.. si scarica dal sito l'ultima versione del programma e si avvia.

Se non individuano nulla oppure, anche dopo l'eliminazione di qualche “porcheria”, il pc presenta ancora strani “sintomi” iniziamo ad effettuare delle scansioni antivirali direttamente on-line

Scansioni on-line disponibili:
Panda Active Scan:
http://www.pandasecurity.com/usa/homeusers/solutions/activescan/default.htm?sitepanda=particulares

Windows Live One Care:
http://onecare.live.com/site/it-IT/default.htm
(non compatibile con Win. Vista)

Trend Micro House Call
http://housecall.trendmicro.com/it/
(non compatibile con Win. Vista)

E-Set on-line scanner
(è la società produttrice del NOD32)
http://www.eset.eu/online-scanner

Kaspersky Online Scanner:
http://www.kaspersky.com/virusscanner

Symantec Security Check:
http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=it&venid=sym

McAfee free scan:
http://home.mcafee.com/Downloads/FreeScan.aspx

CA Online Threat Scanner:
http://cainternetsecurity.net/entscanner/

BIT Defender online scanner:
http://www.bitdefender.com/scan8/ie.html

F-Secure virus scanner on-line:
http://support.f-secure.com/enu/home/ols.shtml

Avast! On-line scanner:
http://onlinescan.avast.com/

ATTENZIONE; anche se il vostro browser preferito è Opera o Firefox usate Internet Explorer per effettuare le scansioni!!!!!

Selezionate un link alla volta e portate a termine TUTTE le varie scansioni.... si lo so è un lavoro lento e noioso … ma necessario!

Il vostro pc ancora non ha voglia di funzionare correttamente?
Tentiamo di disinfettare il sistema tramite delle particolari distribuzioni definite
Rescue CD Antivirus

Andate da un amico o un collega con il pc "sano"
portate appresso 4 cd-r da masterizzare

Scaricate le seguenti immagini .iso da masterizzare sui cd

- **Kaspersky Rescue Disk:**
  http://kaspersky-rescue-disk.softonic.it/

- **F-Secure Rescue CD:**
  http://www.f-secure.com/linux-weblog/2008/06/19/f-secure-rescue-cd-300-released/

- **Avira AntiVir Rescue System:**
  http://www.free-av.com/en/products/12/avira_antivir_rescue_system.html

- **BitFender Rescue CD:**
  http://www.antivirusbitdefender.it/faq/cose-bitdefender-rescuecd.html

Una volta completati i download scaricate questa piccola e gratuita utility
http://www.terabyteunlimited.com/downloads/burncdcc.zip

che vi permetterà di masterizzare “al volo” le immagini sui cd

Una volta masterizzati i dischi utilizzatene uno alla volta semplicemente avviando il pc dall'unità ottica (cioè il lettore DVD – CD) e proseguite con le scansioni.

Se fallisce anche quest'ultimo tentativo i casi sono 3:

1. Non avete seguito le procedure.... rileggete bene lo scritto e seguite TUTTE le procedure indicate
2. Vi ha infettato un virus di nuovissima generazione che gli antivirus non sono ancora in grado di individuare.... complimenti per la sfortuna!
3. I problemi non sono d'origine “virale” ma causati da altri fattori....

In qualsiasi caso vi conviene, se non siete utenti stile “mostro informatico”, - e se lo foste non sareste qui a leggere queste righe :) - portare il pc in assistenza... o in alternativa, dopo aver salvato i vostri documenti più importanti, formattare e reinstallare da “0” il sistema operativo inutilizzabile. Se seguirete quest'ultima ipotesi state bene attenti che nei file salvati prima della formattazione non si “annidi” qualche virus ….

Bene siamo giunti alla fine spero di avervi aiutato e non annoiato :)

glm2006ITALY

FINE GUIDA