ANTIVIRUS E FIREWALL

Di questi tempi, utilizzare un PC senza aver installato un antivirus valido e sempre aggiornato è un po' come uscire di casa lasciando le chiavi nella serratura della porta d'ingresso.
Esistono moltissimi programmi antivirus in grado di riconoscere un virus e impedire che esso abbia accesso al vostro computer, sia che il virus sia contenuto nel CD prestatovi dall'amico, sia che giunga da Internet.
Tra i più conosciuti e diffusi vi sono (in ordine alfabetico) il *Kaspersky,* il *Mac Afee,* il *Nod 32,* il *Norton Antivirus,* in genere utilizzabili gratuitamente per un periodo di prova, dopo di che smettono di funzionare e richiedono l'acquisto del prodotto.
Esistono però anche dei validi **antivirus gratuiti**, ne elenco alcuni in ordine alfabetico: *Avast* (liberamente scaricabile dal sito www.avast.com), *AVG* (http://free.avg.com), *Avira* (www.free-av.com), *Comodo* (www.comodo.com).
Qualunque sia l'antivirus che sceglietе, ricordate che **è indispensabile aggiornarlo costantemente**, perché vengono messi in circolazione nuovi virus letteralmente tutti i giorni, e l'antivirus li può riconoscere soltanto se lo aggiornate.
Questi aggiornamenti sono disponibili su Internet e in quasi tutti i programmi antivirus vengono installati automaticamente mentre siete collegati alla Rete.

L'installazione di un antivirus non è differente da quella di altri programmi. In genere basta cliccare due volte sul file cha avvia l'installazione (cfr. la scheda "Installare un programma" a pagina 216.
All'installazione, le impostazioni di default configurano già il programma per gestire automaticamente:

- ✔ la scansione (termine che indica l'analisi dei file alla ricerca di virus) iniziale dei file di avvio del computer e di alcuni file a ogni accensione;
- ✔ la scansione di un file quando viene aperto con un'applicazione (ad esempio un documento di testo che avvia il programma *Word*);
- ✔ la scansione di supporti di memoria rimovibili (CD, DVD, penne USB, ecc.);
- ✔ la protezione del computer durante l'esplorazione di siti Internet;
- ✔ la scansione di tutti i messaggi di posta elettronica e degli eventuali allegati;
- ✔ l'aggiornamento automatico del programma (il cosiddetto *live update*) a intervalli regolari mentre il computer è connesso a Internet.

Se il programma antivirus è configurato come sopra, è difficile che un virus possa introdursi nel computer. È comunque sempre preferibile verificare la presenza di eventuali virus, attraverso la **scansione del computer**, oppure di file o cartelle sospette.

Basterà – dopo aver cliccato su *Scansione* (se il programma è in inglese, il comando sarà *Scan*) – scegliere l'opzione desiderata (diversa da programma a programma ma, sostanzialmente, simile nei risultati) e procedere seguendo le istruzioni. Se desideriamo controllare una unità di memoria (hard disk, penna USB, CD, DVD o altro) la sceglieremo dall'elenco, mentre per le cartelle e i file dovremo utilizzare il comando *Sfoglia* (se il programma è in inglese, il comando si chiamerà *Browse*).
Una volta individuata l'unità di memoria, la cartella o il file da sottoporre a controllo, selezioneremo quanto di nostro interesse con un clic del mouse e avvieremo la scansione. Sia che la scansione avvenga in automatico o manualmente, se sono presenti virus, il programma ne indicherà il tipo e suggerirà la procedura da eseguire: se *disinfettare*, *mettere in quarantena* oppure *eliminare* il file nel quale è presente il virus.
La scelta tra queste opzioni dipende anche dal tipo di virus individuato. Vediamo, sinteticamente, il significato di queste tre scelte:

- ✔ *Disinfetta*: il programma antivirus è in grado di eliminare il virus dal file infetto e restituirci il file com'era prima dell'infezione.
- ✔ *Metti in quarantena:* il programma non è in grado di disinfettare il file, lo colloca quindi in una cartella protetta, in attesa di scaricare un aggiornamento che contenga le istruzioni necessarie per eliminare quel tipo di virus.
- ✔ *Elimina:* il programma non è in grado di svolgere le prime due operazioni e quindi l'unica soluzione è l'eliminazione del file. Quest'ultima opzione è l'unica possibile quando il file infetto si trova su un CD o su un DVD non registrabili, sui quali il programma non può intervenire giacché, una volta inciso, il dischetto a lettura ottica non è modificabile.

Una situazione più complessa consiste nel **"disinfettare" un computer privo di applicazioni antivirus**, quando il PC è già infetto. In questi casi, una possibile soluzione è – se il computer infetto dispone di un collegamento a Internet ancora funzionante – quella di provare a *disinfettare* il PC ricorrendo a un **antivirus on-line**.
Collegandosi ad alcune pagine internet di siti di aziende produttrici di programmi antivirus, è infatti possibile far esaminare il proprio PC (tutte le sue unità di memoria, oppure solo alcune, oppure solo determinati file) mentre si è collegati a Internet.
Dal momento che la scansione dell'intero sistema richiede parecchio tempo (in alcuni casi anche ore, dipende dalla quantità di file da esaminare e dalla velocità

del vostro collegamento a Internet) questo tipo di soluzione è indicata solo in alcuni casi, ad esempio per chi dispone di una connessione *flat,* cioè a tariffa fissa.
Ecco gli indirizzi web di alcuni antivirus on-line attualmente funzionanti ed efficaci, anche se un numero sempre maggiore di essi tende solo a rilevare l'eventuale presenza di virus, invitando poi all'acquisto del programma:

- http://www.bitdefender.com/scanner/online/free.html
- http://housecall.trendmicro.com
- www.kaspersky.com/scanforvirus
- www.pandasecurity.com/activescan

Specie se restate collegati per diverse ore a Internet, sarebbe opportuno installare sul vostro PC anche un **firewall**.
Il firewall è un sistema di sicurezza che cerca di evitare che estranei possano accedere a dati presenti in un computer collegato a Internet, o trasmettere virus informatici.
Il firewall può essere costituito sia da un programma sia da un apparato. I programmi firewall vengono sempre più utilizzati anche da privati; gli stessi sistemi operativi *Windows XP, Vista* e *7* comprendono già al loro interno un software di questo tipo.
Il firewall informa l'utente di tutti i tentativi di intrusione subiti dal computer e ne segnala il numero identificativo (*IP*), impedendo che il computer risponda alle istruzioni esterne. Va detto che molti di questi tentativi non hanno in realtà intenzioni negative e che, comunque, anche il firewall non garantisce al cento per cento l'utente da malintenzionati particolarmente abili.
Ogni firewall vi segnala quando un programma contenuto nel vostro PC cerca di accedere a Internet e vi propone, in genere, quattro scelte:

- *Sì, solo per questa volta* (la successiva vi verrà riproposta la domanda);
- *Sì, sempre* (al programma sarà sempre consentita la connessione a Internet);
- *No, solo per questa volta* (la successiva vi verrà riproposta la domanda);
- *No, sempre* (al programma sarà sempre impedito di sfruttare il collegamento a Internet).

La regola di base è "autorizzare" soltanto l'indispensabile; se non siete veramente sicuri di cosa fa un certo programma che chiede l'autorizzazione, non autorizzatelo.