

Vademecum

Responsabilità e sicurezza

I nostri ragazzi, senza leggere alcun manuale d'uso, sanno cavarsela con telefonini, lettori DVD e computer. Genitori e insegnanti restano ammirati da tale disinvoltura; a volte, di fronte a qualche procedura un po' troppo complessa, si rivolgono a loro per avere delle consulenze.

Ma non lasciamoci ingannare. Genitori e insegnanti sono responsabili anche delle avventure che i ragazzi compiono in Rete con il PC. Siamo consapevoli che i loro comportamenti avventati potrebbero recare danni, oltre che alla salute psichica dei ragazzi, al nostro nuovo, potente portatile, e alle nostre finanze?

Per i ragazzi, "scaricare" un brano musicale senza pagarlo può valere più della mezz'ora di lavoro che occorre per reinstallare il sistema operativo eventualmente andato in crash a causa di un virus.

Allora è il caso che genitori e insegnanti si soffermino su alcune procedure e che perdano un po' di tempo per esaminare le impostazioni che influiscono sulla sicurezza dei computer.

Software e attacchi esterni

Il PC oltre ai **dati**, contiene i **software**. Se l'**hardware** è piuttosto solido, i software - compreso il sistema operativo - sono costretti a lavorare con migliaia, talvolta milioni, di istruzioni, non sempre del tutto coerenti fra di loro. Si comprende allora come un computer non possa essere una macchina perfetta. Tanto più che risulta possibile, a chi conosce il linguaggio informatico giusto, inserire informazioni ingannevoli e dannose in diversi programmi, alterandone così il buon funzionamento. Tali intrusioni possono essere finalizzate 'semplicemente' a far sapere che si era capaci di realizzarle oppure a trarne un qualche illecito guadagno.

La maggior parte dei virus più famosi non arrecavano alcuna utilità ai programmatori che li avevano sviluppati, se non appunto la soddisfazione di aver bloccato con poche righe di codice interi dipartimenti di importanti aziende informatizzate.

Altri tipi di software dannoso, in inglese **malware**, molto spesso si infiltrano nelle porte del PC, nei file che custodiscono le password, e le trafugano per poi scippare documenti preziosi o denaro.

Cautele da usare

Questo argomento interessa da vicino i genitori ed è senz'altro un tema di scontro fra giovani e adulti anche per i costi che questi ultimi sono tenuti a sostenere in caso di danni o di eventuali multe. Infatti, la legge attribuisce responsabilità precise e prevede pene piuttosto severe per alcuni reati commessi attraverso la Rete, ad esempio quelli configurabili nella pratica del **p2p** (o "peer-to-peer": scambio alla pari) molto diffusa fra i ragazzi.

Le strategie che si possono suggerire, in linea di massima, per evitare danni al software sono le seguenti:

- **Utilizzare un firewall:** se si è sprovvisti del **Centro Sicurezza PC** fornito dal *Service Pack 2* di Windows, vi sono software appositi, anche scaricabili gratuitamente.

- **Aggiornare con regolarità il sistema operativo:** Nessun software, compreso il sistema operativo, nasce perfetto, ma è impegno della Microsoft perfezionarlo attraverso aggiornamenti e installazioni di file che vengono forniti gratuitamente.
- **Usare i nuovi strumenti di Windows:** in **Vista, Defender** protegge dallo spyware (<http://www.microsoft.com/italy/windows/products/windowsvista/features/details/defender.msp>) e **Live OneCare** comprende funzionalità automatiche di protezione, manutenzione, ottimizzazione delle prestazioni del PC (<http://onecare.live.com/site/it-it/default.htm?mkt=it-it>).
- **Installare un programma antivirus e mantenerlo aggiornato:** un buon programma antivirus è assolutamente necessario. È possibile utilizzarne anche uno gratuito, purché gli si consenta di accedere a Internet per aggiornarsi periodicamente.
- **Installare e utilizzare un programma anti-spyware:** vi sono buoni antispyware anche gratuiti. Nei siti delle riviste di informatica è possibile saperne di più.