L'angolo informatico

Antivirus e antispyware vanno aggiornati quotidianamente. I pericoli sono sempre in agguato

# Sicurezza, come proteggersi

## *Un pc connesso viene infettato in appena quattro minuti*

Chi ha acquistato una linea Adsl quasi subito si è dovuto porre una domanda: come fare a tenere alla larga, dal computer di casa, i pirati informatici?

Recenti statistiche dicono che un Pc connesso ad Internet, senza alcuna protezione, attraverso una linea broadband, viene colpito da un virus o da uno spyware entro solo quattro minuti. No, non si tratta di un errore, è proprio così.

Ecco che cosa succede di solito. Si accende il Pc, si apre un browser, ci si collega a qualche sito e come per magia, entro pochissimo tempo, cominciano a succedere le cose più strane. Si aprono finestre di Explorer all'impazzata, la connessione rallenta, e si scopre (spesso molto tempo dopo) di aver mandato e-mail piene di virus, a tutti i contatti che sono conservati in rubrica. A questo punto ci prende il panico. Solitamente qui interviene un amico, informatico di professione, che consiglia di formattare la macchina, reinstallare il sistema operativo, e adottare da ora in avanti, qualche accorgimento tecnico.

Insomma chi non mastica pane e informatica, prima prende la fregatura e poi corre ai ripari.

Ma allora, per navigare o inviare qualche e-mail in tranquillità, cosa si deve fare?

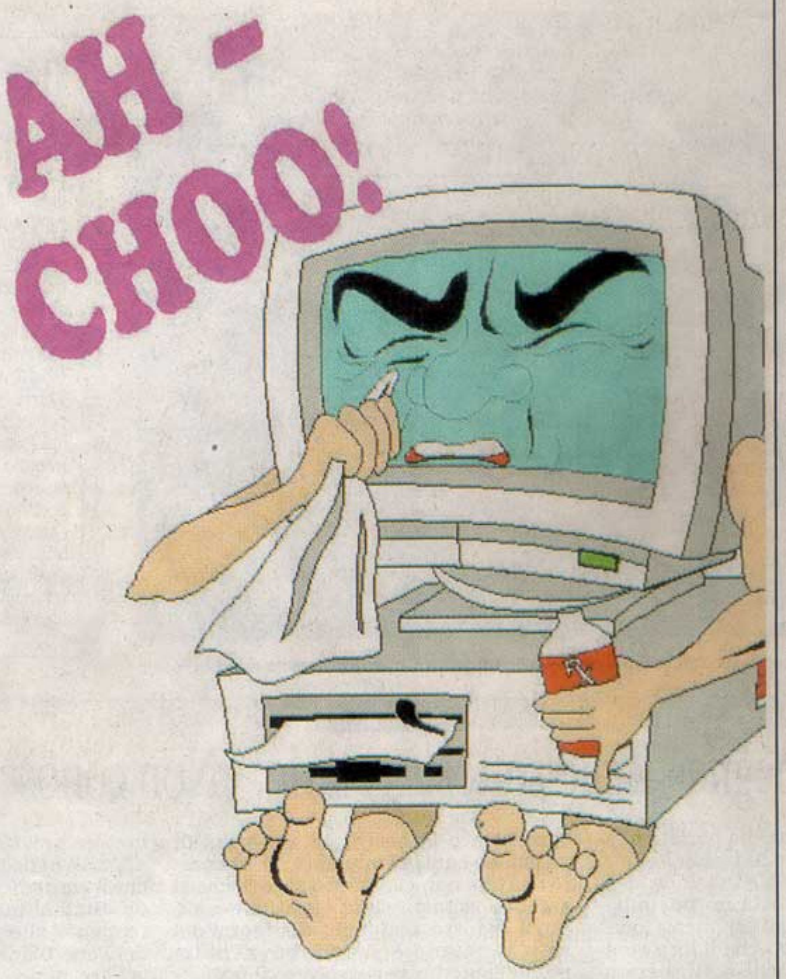
Ci sono solo due strade. Prima ipotesi: mettere dietro le spalle le preoccupazioni, andare avanti finchè il computer non è completamente infestato da virus e, quando non se ne può più, chiamare il solito amico per reinstallare il pc.

Seconda ipotesi: per conservare la riservatezza e l'integrità dei dati, installare un buon antivirus (ce ne sono anche di gratuiti,) in grado di controllare, sia i file sul sistema che la posta elettronica; abilitare il firewall (quello presente in Windows XP è limitato, ma è meglio che niente!); installare e far girare ogni tanto un antispyware, per eliminare quei programmi «birichini» che cercano di carpire informazioni a nostra insaputa; infine, scaricare gli aggiornamenti periodici che Microsoft propone per il sistema operativo Windows, con un'attenzione particolare a quelli che riguardano problemi di sicurezza.

Tutto qui? Non proprio, purtroppo. L'antivirus va aggiornato quotidianamente, per garantire una protezione adeguata. Lo stesso dicasi per l'antispyware. E il firewall, per chi è alle prime armi, può essere ostico da configurare.

Ma niente paura: con i consigli di qualche amico «smanettone», si può riuscire a venirne fuori. L'importante è non perdersi d'animo. Se poi si condisce il tutto con qualche lettura sull'argomento, si potrò caversela alla grande.

Questo non significa che saremo al riparo da tutti gli eventi: gli accorgimenti da seguire sono sicuramente più numerosi. In ogni caso, è bene sapere che la sicurezza assoluta non esiste. I furti di dati riservati nelle reti informatiche di Cisco Systems e le azioni perpetrate dagli hacker contro i siti della Nasa e del Pentagono, dimostrano che nemmeno le reti governative superprotette e quelle delle mega-aziende sono immuni da rischi. Tuttavia, adoperare strumenti che consentano una minima protezione, permetterà di correre meno pericoli e rendere la vita agli hacker un po' più complicata.




### VOCABOLARIO INFORMATICO

**Hacker**
Il termine ha assunto il significato generico di criminale informatico, a causa dell'uso fatto principalmente dai mass-media.
In realtà la parola hacker ha un'accezione positiva: identifica una persona che possiede un'approfondita conoscenza dei sistemi e dei linguaggi di programmazione, e che cerca di superare i limiti e le difficoltà tecniche che gli si pongono innanzi.

**Cracker**
È colui che vìola o danneggia sistemi informatici per interesse economico (per perpetrare frodi o per fini di spionaggio industriale). Può agire anche per far riconoscere la propria abilità all'interno della comunità virtuale di pirati (in inglese: "crew") cui appartiene. Quest'ultima motivazione è tipica dei soggetti che hanno un'età compresa tra i 12 e i 18 anni.

**Virus**
Programma che, se eseguito, infetta file e altri software, danneggiando il sistema informatico ospite. I virus contengono al loro interno le istruzioni per riprodursi e cercare di insinuarsi in altri sistemi.

**Spyware**
Software malevolo creato per raccogliere informazioni e dati sensibili all'insaputa delle persone (indirizzi e-mail, password, siti preferiti visitati dall'utente, ecc.) . I dati raccolti dallo spyware sono girati automaticamente a pirati informatici o ad aziende senza scrupoli, che li possono utilizzare per frodi o altre finalità illecite, come lo "spam" (= grande quantità di messaggi di posta elettronica non sollecitati, inviati a scopo pubblicitario o commerciale).

Testi a cura di
**MARCO CIPRIANI**
Email
**informatica@media-alpi.it**