

# I vicoli bui di Internet-città

di Giovanni Pasanisi (\*)

Ormai è sicuro, Internet è divenuto, in questi ultimi dieci anni, il mezzo più potente di comunicazione al mondo superando di gran lunga quello televisivo, radiofonico e cartaceo. Basti pensare all'ultima proposta di Microsoft per acquistare l'altro colosso Yahoo.

**Proprio per la sua potenza e diffusione desta ancora diffidenza e sono in molti a chiedersi se il suo utilizzo sia sicuro.**

**Internet è una minaccia o una risorsa allora?**

Certamente la seconda, ma non si deve dimenticare, in chiave di sicurezza informatica, che un canale così vasto è anche fonte di numerosi quanto sofisticati pericoli.

**Internet, è assimilabile ad una grande città. E' attraversata da vie sicure da poter esplorare ma anche da strade pericolose da evitare. Dipende solo da dove si vuole arrivare.**

Ciò non deve ostacolare la conoscenza di questa bellissima invenzione. Essa veniva utilizzata negli anni '60 solo dai militari americani e si è, poi, diffusa tra la gente comune come mezzo di comunicazione.

Si pensi ai vantaggi, anche economici, che offre questa rete mondiale. Si può comunicare e videocomunicare a costo zero da una parte all'altra del mondo usando i software appropriati. (tra i più utilizzati Skype e Messenger).

Si pensi all'immediatezza con la quale è possibile rendere disponibile una notizia a livello mondiale semplicemente pubblicandola su Internet.

Tra qualche anno potrebbe scomparire il telefono fisso per far spazio alla tecnologia VoIP (parlare attraverso la rete internet oltre che navigare), tecnica già utilizzata da un po' di anni da skype senza alcun costo per l'utilizzo del programma.

La stessa si sta diffondendo anche sui cellulari e sui palmari.

Si pensi alla possibilità di fornire e reperire informazioni particolari nello studio, nella ricerca medica su malattie, in particolare su quelle rare. Senza internet sarebbe estremamente lungo e difficile trovarle.

In molti si chiedono se esiste sicurezza nell'utilizzo di internet poiché hanno timore di attivarla nella propria abitazione.

**Internet è una tecnologia da saper utilizzare altrimenti e come frenare con un auto sul bagnato!!!**

Non è necessaria una conoscenza informatica da professionisti per utilizzarla al meglio.

La paura di usare internet scaturisce dalla sua non conoscenza e la conoscenza è acquisibile solo utilizzando la rete.

Bastano poche regole da osservare per navigare tranquilli e una tra queste è: **“niente per niente, nessuno ti da niente”**.

L'implementazione della sicurezza in Internet varia da utente ad utente. Un conto è che a porsi il problema sia una azienda che deve salvaguardare un intero parco PC, server di rete e apparati di rete, un altro conto è che a preoccuparsene sia un utente privato.

Se si entra nel dettaglio della sicurezza su Internet prendendo come riferimento una famiglia l'importante è utilizzare sul proprio personal computer un buon **antivirus** tenendo conto che molti gestori provider (Tiscali, Telecom, ecc., ecc) provvedono già e rendere sicure ed esenti da virus le email e bloccano la posta indesiderata (spam).

Per quanto riguarda l'uso di Internet da parte dei ragazzi esistono, oggi, molti software che garantiscono la sicurezza di navigazione verso siti attendibili ed il blocco totale verso siti non leciti, anche se è consigliabile sempre la supervisione del genitore.

Esistono moltissime soluzioni per proteggere i ragazzi da pornografia, violenza, gioco d'azzardo online e via dicendo come [ScrubIT](#), [CyberPatrol](#) o [Davide.it](#), e così come esistono diverse soluzioni di content filtering adatte all'azienda, come [Websense Web Security Suite](#) o [ISS Web Filter](#) tra le tante.

Anche Microsoft ha provveduto a realizzare un prodotto simile [OneCare Family Safety](#) per salvaguardare la famiglia da siti non leciti.

Ecco alcune regole comuni da osservare al fine di garantire un sicuro utilizzo di internet:

### **Regole di base per la navigazione su internet:**

- 1) Aggiornare periodicamente il Sistema Operativo Windows con l'utility Windows Update)
- 2) Installare un antivirus ed aggiornarlo quotidianamente
- 3) Utilizzate Password complesse min 10 caratteri alfanumerici con maiuscole minuscole (non date di nascita, nomi o altro di facile intuizione).
- 4) Navigare in rete in modo prudente e non accedere a siti non considerati affidabili e soprattutto non comunicare i propri dati sensibili;
- 5) E' consigliabile avere più di una email personale per comunicare i propri dati (attenzione ai "gratis" in particolare ai siti di loghi e suonerie, siti di informazioni o invio sms gratis o giochi d'azzardo)
- 6) Non eseguire transazioni utilizzando circuiti bancari non conosciuti (Banca Sella la più conosciuta) ed assicurarsi che sul percorso dell'indirizzo del sito in internet Explorer ci sia la dicitura "[HTTPS://nome sito](#)" la "S" (security) fa la differenza.
- 7) Evitare quanto più è possibile di scaricare programmi crackati e soprattutto dalla rete P2P per intenderci (Emule).

### **Regole di base per la posta elettronica:**

- 8) Tenere aggiornato il software per la posta elettronica. Per questo visitare spesso il sito dei produttori del programma, scaricare ed installare le patch indicate;
- 9) Installare un antivirus che controlli la posta in entrata e quella in uscita;
- 10) Filtrare lo spamming, creando regole o scegliendo i produttori che permettono di impostare filtri automatici;
- 11) Non aprire gli attachment (allegati) considerati pericolosi;
- 12) Non rispondere allo spamming, perché si confermerebbe di avere un account di posta attivo. Semplicemente cancellare le e-mail indesiderate;
- 13) Non fornire mai dati sensibili via e-mail. Per esempio non trasmettere mai password, numeri di carta di credito, informazioni personali.
- 14) Diffidare delle email che contengono la richiesta di informazioni circa il conto corrente. Questo fenomeno si chiama **Phishing** e consiste nell'invio di false e-mail con grafica e loghi ufficiali di eBay, PayPal, ma anche di servizi Bancari e di Carte di Credito, chiedendo di riempire un modulo su una pagina web con indirizzo Internet presente nella stessa e-mail.

### **Regole di base per i più esperti:**

1. Installare un buon firewall;
2. Crittografare i dati mediante programmi come PGP;
3. Disabilitare sulle proprietà della connessione Internet o scheda di rete alla voce TCP/IP, proprietà avanzate, WINS l'opzione "*disabilita NetBIOS su TCPIP*";(una piccola modifica che dice tanto
4. Cancellare frequentemente i cookies ed i file temporanei creati durante la navigazione su internet;
5. Disabilitate dalle proprietà dei browser come Internet Explorer la memorizzazione della password nei moduli.

**Seguendo queste poche, semplici regole la navigazione sarà quasi senza pericoli.**