



[www.adiconsum.it](http://www.adiconsum.it)



[www.savethechildren.it](http://www.savethechildren.it)



**easy4**

**Sicurezza  
informatica  
rischi e contromisure**



## Introduzione

*Il fatto che ormai molti aspetti della nostra vita sociale siano legati al mezzo informatico (solo per fare un esempio, non è forse sul computer della banca che si giocano i destini del nostro conto?) ci espone ad una serie di pericoli che è bene conoscere. Certamente non a tutti possiamo fare fronte con le nostre forze, ma ad alcuni sì. Usare il PC per navigare in Internet, pagare le tasse, fare un bonifico, intrattenere amicizie online, acquistare beni e prenotare vacanze, scaricare documenti e programmi, films o musica, sono tutte opportunità di risparmiare tempo e denaro, avere più scelta, consumare agevolmente a casa propria: di fondamentale importanza, questo è ovvio, è non fare "passi falsi".*

*Questa guida è dedicata a tutti coloro che usano un personal computer e la rete Internet, consapevoli dei rischi che questo può comportare: virus, intrusioni e molestie, pubblicità invadente e spam, attività che violano la privacy, frodi online...*

*La lettura di questo vademecum aiuta ad attrezzarsi per affrontare il rischio "sicurezza informatica", mettendo in atto ogni possibile contromisura. Non è un manuale tecnico per esperti, anzi ha lo scopo di offrire indicazioni semplici di autodifesa e di uso consapevole della tecnologia anche ai lettori meno "competenti".*

*Abbiamo scelto di trattare gli argomenti in forma di domande e risposte rigorosamente pratiche, con qualche nota di umorismo e senza pretese di completezza o estremo rigore scientifico, per rendere la lettura più piacevole ed istruttiva.*

*La Guida è parte del programma di pubblicazioni ed iniziative del progetto EASY per la sicurezza di Internet e delle nuove tecnologie, promosso dalle associazioni Adiconsum e Save the Children, con il sostegno della Commissione Europea, DG Information Society. Ha collaborato alla redazione dei testi, con i suoi esperti tecnici, l'Associazione Nazionale degli Specialisti di Sicurezza in Aziende di Intermediazione Finanziaria (ANSSAIF).*



## **P**erché preoccuparsi della sicurezza del proprio personal computer?

Ognuno di noi sa quali rischi si possono correre giornalmente e sa, per esempio, che uscendo di casa la porta va chiusa possibilmente a chiave; sa anche che se nella zona ci sono stati dei furti negli appartamenti, è bene avere dei sistemi di chiusura aggiuntivi (ad esempio: inferriate) e, ancora meglio, un antifurto; in casa, ognuno sa che se ci sono dei bambini è bene tenere lontane le bottiglie o flaconi contenenti acidi o sostanze pericolose; tutti sanno che un bambino molto piccolo non va lasciato solo con libertà di movimento, senza sorveglianza, perché potrebbe farsi male, giocando con una presa di corrente o arrampicandosi, ad esempio, sul mobile della televisione; chi ha un'automobile sa quali sono i rischi e conosce le cautele da adottare avendo tale mezzo, onde evitare di fare danni; e così via.

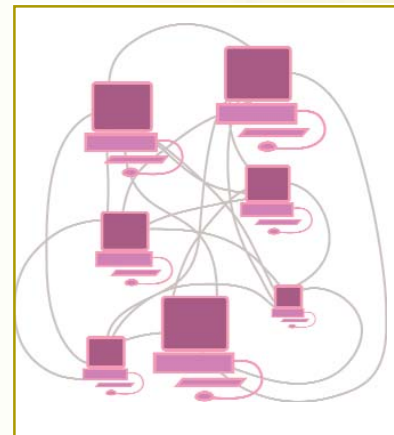
Allora, chi ha un computer perché non dovrebbe preoccuparsi di sapere quali sono i rischi a cui può andare incontro lui o suo figlio o suo nipote?

Perché non deve preoccuparsi di conoscere a quali rischi un bambino può andare incontro se accede ad internet e non è assistito da un genitore o da un fratello / sorella maggiore? Mai sentito parlare di siti dove si può parlare con chiunque? Anche con i pedofili?

Quindi il computer potrebbe divenire uno strumento utilizzabile da terzi per carpire informazioni, per rubarvi i documenti che avete memorizzato nel disco fisso, per controllarvi mentre accedete al vostro conto corrente, mentre pagate un conto corrente postale, mentre riservate un posto sull'aereo, e così via.

## **D**obbiamo dedurre che il computer è pericoloso e quindi è meglio non usarlo!

Ogni cosa può avere un risvolto "pericoloso": la porta e le finestre di casa, in quanto possibili vie d'ingresso di sconosciuti; l'automobile, in quanto potenziale fonte di danni a cose e persone; le posate, forchetta, cucchiaino e... coltello! in quanto potenzialmente potrebbero ferire e addirittura uccidere; un lettore di CD, se attivato mentre il coperchio è aperto e non vi è il CD, può essere pericoloso per la vista perché il raggio laser del lettore potrebbe colpirvi un occhio; e l'elenco sarebbe infinito!!!!!!



Sono questi motivi sufficienti a scoraggiarci dall'usare porte, finestre, coltelli e lettori CD? No di certo, ma sono sufficienti a farci prendere delle contromisure: di certo non permettiamo ad un bambino di giocare alla guerra con un coltello e cercheremo un lettore di CD con un dispositivo che ne impedisce il funzionamento con lo sportello aperto. E' quindi ovvio che quando usiamo qualche strumento dobbiamo fare attenzione e conoscere le avvertenze e, in con-

clusione, dobbiamo conoscere, di ogni cosa, i vantaggi, i possibili rischi e le contromisure.

Il computer non fa eccezione a questa regola!!

Quello che accade però è che i possibili rischi per svariati motivi non sono noti e questo ovviamente non va bene perché impedisce di agire responsabilmente.

Questa piccola guida è diretta proprio ad assistervi in ciò: conoscere, per meglio governare la tecnologia.

Ricordatevi comunque che possiamo aiutarvi a scoprire i rischi e dirvi come risolverli, ma rimarrete sempre voi a conoscere meglio di chiunque altro le vostre esigenze, cioè i problemi che volete risolvere utilizzando un computer.

La conoscenza di ciò che volete fare e dei rischi a cui potete esporvi nel vostro agire vi permetteranno, in ultima analisi, di decidere in merito ai possibili comportamenti da adottare e dei quali parleremo più avanti.

## **M**a, in parole semplici, che cos'è un personal computer?

Sostanzialmente possiamo dire che il Personal Computer è fatto da due insiemi di componenti: l'hardware, la parte fisica, tangibile, e il software, la parte immateriale, i programmi.

Il primo è tipicamente composto dal contenitore ("case"), l'alimentatore, la piastra madre ("mother board"), il disco rigido ("hard disk"), le unità floppy disk, CD-ROM, DVD e il masterizzatore, le schede video e audio, il modem, la scheda di rete, il monitor, la tastiera e il mouse.



Il secondo può essere definito come tutto ciò che in grado di far svolgere all'hardware un compito, cioè essenzialmente manipolare, archiviare e trasferire dati. Il software che attiva le funzioni elementari di un calcolatore si chiama sistema operativo ed è indispensabile al funzionamento del PC. Ulteriore software è, ovviamente, necessario per eseguire compiti specifici, come comporre un testo, disegnare, ritoccare un'immagine, accedere ad Internet, inviare o ricevere un'e-mail, ecc.



Normalmente, i software sono coperti dal copyright e richiedono il pagamento della licenza d'uso per essere utilizzati. La copia non autorizzata e l'uso, sia pur non commerciale, sono considerati un reato penale dalla legge italiana. Una alternativa all'uso del costoso software commerciale è ricorrere a quello di pubblico dominio disponibile in rete. Spesso questo è un software di qualità comparabile, se non superiore, a quello commerciale. Possiamo distinguere quattro tipi di software gratuito:

- **Software opensource;**
- **Software sponsored;**
- **Software freeware;**
- **Software shareware;**

Il software opensource è quel software gratuito o meno per cui è disponibile il codice sorgente. Opensource è soprattutto software non commerciale, di cui il più notevole esempio è LINUX disponibile in varie distribuzioni (Red Hat, Suse, ecc.) a pagamento e in distribuzioni reperibili gratis in rete: è un sistema operativo alternativo al classico WINDOWS.

Gratuiti gli ultimi tre della lista, con l'avvertenza che i freeware non essendo sponsorizzati e non accettando donazioni in denaro dagli utenti come gli shareware, espongono talvolta al rischio di controllo remoto da parte dell'autore, virus ed altro.

## **E** allora internet che cosa è?

Il computer, mediante opportuni strumenti e software, può anche accedere ad Internet, ossia ad una rete mondiale di informazioni e software.

Per chi non lo sa, con la parola Internet si intendono molte cose: una modalità universale di colloquio fra calcolatori di diversi costruttori (IBM, HP, SIEMENS, DELL, ecc.), un insieme di computer che gestiscono caselle di posta, "siti" contenenti informazioni disparate o reclamizzanti prodotti vari in vari luoghi del mondo, siti che consentono di trasferire sul proprio computer canzoni o film; "sale" virtuali dove si può dialogare, sia per iscritto che a voce con un microfono, con altri residenti in altre Nazioni; ecc.

Per capire cosa è internet da un punto di vista leggermente più concreto, immaginiamo una serie di collegamenti, normalmente di tipo telefonico, che uniscono fra di loro tanti computer; l'insieme dei numerosi collegamenti costituisce la rete, nel senso di ragnatela e non tanto di rete da pesca (nella quale comunque si finisce, ma di questo parleremo più avanti).

Per far sì che questi collegamenti vengano gestiti c'è bisogno di vari apparati costituiti sostanzialmente da altri computer seppur specializzati i quali agiscono secondo delle regole predefinite.

In sostanza quindi la rete internet non si limita solo a fornire il collegamento, ma offre dei veri e propri servizi ai computer connessi: la posta elettronica, l'accesso a fonti informative di vario genere quali giornali, banche, pubblica amministrazione, ecc..

Con riferimento ai discorsi che stiamo facendo, è bene considerare due aspetti sui quali non ci si sofferma mai abbastanza.

"Connettersi a internet", a prescindere dalla modalità tecnica con la quale realizzi la connessione, appare come una decisione volontaria: sono io che accendo il computer e il modem, che attivo i programmi, che decido su quale sito andare o quale casella di posta scaricare.

In realtà le cose stanno diversamente: è Internet, la "grande rete", che ci accetta e ci assegna un nome nella comunità e una volta connessi ci troviamo inglobati tra i milioni di computer connessi.

L'altro aspetto importante riguarda le regole che questa comunità si è data; non parliamo delle regole di comportamento degli utenti, la cosiddetta "netiquette" che è un sorta di codice etico che gli utenti connessi dovrebbero osservare.

Per regole ci riferiamo ai criteri di progettazione a suo tempo fissati e che sono incarnati dalle varie componenti tecnologiche della rete. Tali criteri sono stati improntati alla massima libertà e democrazia;



al contrario delle rete private utilizzate dalle aziende per motivi commerciali che sono ispirate a rigidi concetti gerarchici (tutto è vietato tranne ciò che è consentito ai soggetti che sono perfettamente identificati e ai quali un'autorità di amministrazione consente di fare esclusivamente ciò di cui hanno stretta necessità), internet è stata concepita in modo tale da consentire ad ogni computer di usufruire potenzialmente qualunque servizio senza che ci sia un amministratore centrale: in pratica tutto è consentito tranne ciò che è vietato, e di vietato c'è veramente poco.

Per fare un esempio, dal vostro computer connesso a Internet potete tranquillamente utilizzare dei servizi tecnici di amministrazione, gironzolare su altri computer connessi, ecc. a patto di saperlo fare.

La struttura semplice e l'assenza di vincoli hanno consentito a internet di diventare un formidabile strumento di comunicazione basato su quella che può essere considerata la più solida infrastruttura tecnologica esistente (internet da quando è nata non ha mai avuto interruzioni nella sua disponibilità).

Per contro, per quanto riguarda servizi, costi e possibilità di utilizzo Internet è paragonabile ad una giungla piena di trappole, dove vince il più forte che nella caso specifico è chi ne sa di più, sia in termini di possibilità di utilizzo sia in termini di conoscenza dei rischi e contromisure possibili.

Il Personal Computer, mediante opportuni strumenti hardware (modem, scheda di rete) e software (il "browser" o motore di navigazione), può accedere ad Internet.

Internet può essere definito come:

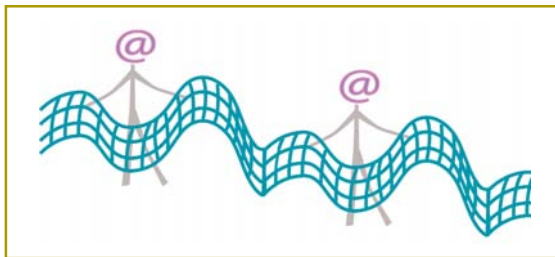
una rete che, collegando fisicamente milioni di computer, connessi a vari livelli e distribuiti su tutto il pianeta, assicura la possibilità di scambiare dati tra le diverse piattaforme;

un nuovo media che contiene e permette di accedere a tutti i mezzi di comunicazione comunemente usati.

un luogo immateriale, virtuale, in cui milioni di utenti possono allo stesso tempo coesistere e interagire secondo diverse modalità;

un contenitore di dati, notizie, informazioni, e infine di "sapere";

L'accesso a internet può avvenire con varie modalità, dal normale collegamento con modem su linea telefonica a 56 Kb, fino ai colle-



gamenti più veloci ADSL o Fibra Ottica. Internet, la "grande rete", quando ci connettiamo ci accetta e ci assegna un nome nella comunità: così ci troviamo inglobati tra i milioni di computer connessi.

Un aspetto importante riguarda le regole che questa comunità si è data: regole di comportamento degli utenti, la cosiddetta "netiquette" che è un sorta di codice etico che gli utenti connessi dovrebbero osservare, ma soprattutto criteri di progettazione a suo tempo fissati e che sono incarnati dalle varie componenti tecnologiche della rete. Tali criteri sono stati improntati alla massima libertà e democrazia: internet è stata concepita in modo tale da consentire ad ogni computer di usufruire potenzialmente qualunque servizio senza che ci sia un amministratore centrale: in pratica tutto è consentito tranne ciò che è vietato, e di vietato c'è veramente poco. Per fare un esempio, dal vostro computer connesso a Internet potete tranquillamente utilizzare dei servizi tecnici di amministrazione, gironzolare su altri computer connessi ecc., a patto di saperlo fare.

La struttura semplice e l'assenza di vincoli hanno consentito a internet di diventare un formidabile strumento di comunicazione basato su quella che può essere considerata la più solida infrastruttura tecnologica esistente (internet da quando è nata non ha mai avuto interruzioni nella sua disponibilità). Per contro, per quanto riguarda servizi, costi e possibilità di utilizzo Internet è paragonabile ad una giungla piena di trappole, dove vince il più forte che nella caso specifico è chi ne sa di più, sia in termini di possibilità di utilizzo sia in termini di conoscenza dei rischi e contromisure possibili.

**S**pero che poi venga l'aiuto. Perché per il momento siete riusciti solo a confondermi e spaventarmi: se ho capito bene io sono Mowgly mentre dovrei diventare Tarzan per affrontare una simile giungla!

In primo luogo se volete diventare Tarzan della rete non vi serve questa piccola guida, perché probabilmente vi siete orientati a diventare professionisti della rete: auguri e ci vediamo un'altra volta.

In secondo luogo non è necessario diventare Tarzan, perché avete già una vostra professionalità ed è bene che coltivate quella: è sicuramente preferibile che un medico passi il tempo che ha destinato al proprio aggiornamento a studiare come curare le malattie piuttosto che a come installare e utilizzare un firewall.

All'utente "normale" diciamo con la massima onestà che ottenere la



sicurezza assoluta non è un obiettivo realistica, mente raggiungibile. Eugene Spafford, famoso "guru" di sicurezza informativa esprime questo concetto con una frase ormai abbastanza nota: "L'unico computer veramente sicuro è spento, chiuso in un blocco di cemento sigillato in una stanza con le pareti di piombo e guardie armate alla porta. Ma anche in questo caso ho i miei dubbi."

Dubbi più che giustificati visto che nelle condizioni elencate non è stata prevista la disconnessione fisica da qualunque rete e la presenza di una copia integrale del contenuto dei dischi.

Visto che siamo nel terzo millennio non è pensabile attenersi a questi modelli di sicurezza.

Ma non è altrettanto realistico pensare che tutti i dispositivi hardware e software di questo mondo possano consentirci di dimenticare il problema.

La nostra sicurezza si deve basare innanzitutto su un nostro atteggiamento di prudenza: prima di fare qualunque click capire bene cosa vuol dire e nel dubbio astenersi.



## **D'** accordo. Ma che cosa si vuole intendere realmente con "sicurezza del personal computer"?

In precedenza vi abbiamo già spiegato, magari scherzando, che non può esistere un sicurezza assoluta e che quindi l'utilizzo di un personal computer ci espone in ogni caso, come qualunque altro oggetto, a dei rischi.

Ora pensiamo alla nostra automobile; uno dei rischi che può correre è il furto e quindi normalmente adottiamo delle contromisure per fronteggiare questo rischio: sistemi di antifurto, polizze di assicurazione, ricovero in locali chiusi, ecc.

A parte casi di particolare affezione verso la propria automobile, di solito non spenderemo 1.500 € di antifurto per un veicolo dal valore commerciale di 1.000 €.

La regola quindi è che le contromisure devono essere proporzionate al rischio, in particolare devono essere commisurate ai danni derivanti dall'avverarsi degli eventi cui è associato il rischio.

Per Sicurezza Informatica si intende quel particolare campo di interessi il cui scopo principale è la rilevazione e definizione dei principali fattori di rischio a cui le informazioni vengono esposte. Tali fattori di rischio sono poi generati da cause molto diverse fra loro, ma che possiamo distinguere in almeno due categorie:

La prima, di ordine prettamente tecnico, tiene principalmente conto dei fattori di rischio imputabili alle risorse applicate alla gestione delle informazioni, risorse quali ad esempio l'hardware, ma che

considererà anche il lato applicativo - il software -relazionabile quindi al processo di elaborazione delle informazioni;

La seconda categoria riguarda invece l'aspetto relativo alla protezione, riservatezza ed autorizzazione alla manipolazione dell'informazione, vero nodo spinoso della questione (vedi domanda "Come funziona la tutela della privacy in rete?")

Sicurezza attiva significa salvaguardare attivamente la salute dei nostri dati proteggendoli "attivamente" mediante frequenti back-up di sistema (salvataggio periodico dei dati o della configurazione del sistema), l'utilizzo di un buon antivirus, la configurazione di un altrettanto buon firewall di protezione, tutte cose salutari per la nostra tranquillità informatica.



Un firewall offre la possibilità di limitare la comunicazione fra Internet e un sistema interno. Lo si installa di regola dove può massimizzare il suo effetto, ossia nel punto in cui il sistema interno è connesso a Internet. Con un firewall si riduce il pericolo che aggressori possano penetrare dall'esterno in sistemi e reti interne. Il firewall può inoltre

impedire a utilizzatori interni di mettere in pericolo il sistema, trasferendo verso l'esterno informazioni importanti per la sicurezza, come password non codificate o dati confidenziali. Il firewall è quindi un genere di sicurezza che permette di collegare una rete a Internet mantenendo una certa misura di sicurezza. Nel caso poi il sistema stesso sia una rete aziendale di piccole, medie, o grandi dimensioni, starà all'abilità dell'amministratore provvedere ad un corretto setup del firewall, considerando alcuni parametri affinché venga aumentato il livello di sicurezza ma non venga conseguentemente deteriorata la funzionalità e l'efficienza del sistema stesso. Vi è però da considerare anche un altro aspetto, non meno importante, che riguarda il lato "passivo" del problema. Il livello di formazione ed informazione degli utenti risulta basilare per innalzare il livello di sicurezza dell'intero sistema, bisogna infatti essere consapevoli del fatto che ci sono:

- File eseguibili (.exe) provenienti da fonti incerte, ma anche da indirizzi conosciuti, possono potenzialmente contenere programmi con



potere distruttivo o a carattere di spionaggio. Dovrebbero persino già esistere file contrassegnati con .zip che in effetti sono file .exe camuffati; si consiglia dunque, prima di scoprire o di avviare un file o un programma "setup", di attivare l'antivirus effettuando la scansione del file in questione, anche se nemmeno questo provvedimento costituisce una protezione totale.

- File allegati alle e-mail, cosiddetti "Attachment", di cui non si conosce il mittente, dovrebbero essere eliminati immediatamente, senza aprirli né avviarli. I documenti Microsoft-Office, e in particolare i file \*.doc, dovrebbero per principio essere aperti con un Viewer, e non in Word, Excel o Powerpoint.

- Java, Java-Script, ActiveX-Controls e altri ampliamenti HTML possono introdurre troiani sul vostro disco mentre state tranquillamente navigando in Internet. Può essere d'aiuto impostare il proprio browser al livello di sicurezza più alto, anche se questo può limitare in parte la navigazione.

Nel caso del PC i comportamenti dolosi si possono manifestare essenzialmente in due modi:

tramite accessi indesiderati e non controllati per problemi legati all'utilizzo del browser.

Nel primo caso, ricordati che quando ti colleghi attraverso un modem (analogico o ISDN) o con una connessione ADSL, ti connetti alla rete Internet utilizzando un indirizzo IP. Esistono programmi che sono in grado di scansionare la rete alla ricerca di possibili indirizzi IP "vulnerabili" associati a macchine potenzialmente attaccabili.

L'attacco al tuo computer può avvenire, quindi, attraverso porte di comunicazione che normalmente il sistema operativo non controlla e lascia quindi aperte: il malintenzionato può tentare di usarle per collegarsi al nostro PC.

Se riesce a ottenere in qualche maniera l'accesso, la tecnica per impossessarsi del tuo amato computer consiste nell'introduzione di programmi che stabiliscono un collegamento fra lui e la tua macchina ogni volta che ti colleghi ad Internet. Un semplice sistema per controllare sul tuo computer quali porte siano attive è quello di eseguire dal Prompt dell' MSDOS il



comando netstat -na. Per vedere tutte le opzioni di netstat scrivere netstat /?. Ti consigliamo di lasciare attivo esclusivamente il protocollo TCP/IP e rimuovere dalla tua configurazione di accesso remoto tutti gli altri protocolli (esempio: NetBEUI e IPX/SPX).

Nel secondo caso dal punto di vista della sicurezza il browser (il programma che utilizzi per navigare sui siti web) è senza dubbio uno dei componenti più deboli dell'intero sistema.

Nessun browser di nostra conoscenza è esente da problematiche connesse alla sicurezza. Conoscerle tempestivamente e sapere come porvi rimedio è essenziale per l'integrità del tuo computer e dei dati in esso contenuti.

I browser Internet più popolari sono:

- **Internet Explorer**
- **Netscape Communicator**
- **Opera**

Il più diffuso è Internet Explorer perché Microsoft lo incorpora all'interno dei suoi sistemi operativi. Per evitare di correre rischi è determinante applicare le varie patch che Microsoft e gli altri produttori rilasciano periodicamente per i loro prodotti.

A questo fine ti segnaliamo il servizio Microsoft Windows Update che consente l'aggiornamento automatico di tutto il sistema, compreso il browser.

Puoi aumentare il livello di sicurezza di Internet Explorer limitando o bloccando l'esecuzione automatica di script e ActiveX.

Per configurare correttamente i controlli ActiveX esegui la seguente procedura:

Menu Strumenti -> Opzioni Internet -> Protezione

Clicca sul bottone Livello Personalizzato

Seleziona l'opzione "Chiedi conferma" al posto di "Attiva" in tutte le voci che riguardano l'esecuzione di controlli ActiveX.

Inoltre ti suggeriamo di togliere la memorizzazione automatica dei moduli e delle password.

Per cambiare questa impostazione segui la seguente procedura:

Menu Strumenti -> Opzioni Internet -> Contenuto

Premi sul bottone Completamento Automatico

Deseleziona le voci Moduli e Nome utente e password sui moduli

Premi sul bottone Cancella i Moduli e sul bottone Cancella Password per eliminare dati già memorizzati precedentemente dal browser.

La sicurezza del personal computer è quindi l'insieme di contromisure di varia natura che abbiamo adottato per fronteggiare le minacce legate alle varie tipologie di rischio e commisurate ai danni

che riteniamo sopportabili a fronte del possibile avverarsi degli eventi dannosi.

L'applicazione pratica di questo concetto richiede l'utilizzo di tecniche e strumenti non certo disponibili e convenientemente utilizzabili da utenti "normali" come quelli a cui si rivolge questa piccola guida.

Senza prescindere dalla consapevolezza delle vostre esigenze e dei rischi cui andate incontro, Vedremo più avanti quali contromisure sono poi possibili per avere un pò di tranquillità.

**M**a ogni volta che si parla di Internet si sentono termini che difficilmente riesco a capire; forse dovrei cercare di imparare il loro significato per potermi districare meglio nel cyberspazio?

Lo scopo non è diventare un provetto conoscitore di Personal Computer e Internet. Il nostro scopo è quello di rendere l'utente del PC e di Internet un "consumatore" attento e capace di schivare le insidie presenti in rete.

A tal fine, riteniamo che un glossario di base sia effettivamente indispensabile.

**Quando si parla di minacce possibili, si possono incontrare termini quali:**

#### **Virus**

Un pezzo di codice in grado di diffondersi e duplicarsi in modo autonomo, legandosi ad un programma, ad un messaggio di posta elettronica, ecc. Esistono migliaia di virus diversi, raggruppabili in alcune categorie base, che hanno in comune la capacità di duplicarsi automaticamente, di eseguire operazioni potenzialmente dannose sui sistemi infetti, di attivarsi in contesti o momenti determinati.

Un antivirus è un software in grado di intercettare un virus prima che entri sulla macchina locale (via posta elettronica, tramite un floppy disk infetto, tramite una condivisione di rete, ecc.) e di controllare ed eventualmente riparare i file infetti presenti sul computer.

#### **Worm**

Un worm ha caratteristiche simili ad un virus: si duplica automaticamente e può farlo in modo estremamente rapido. A differenza di un virus non si attacca ad altri programmi ma tende a mantenersi autonomo e non necessariamente fa danni diretti (come cancellare dei file) ma con la sua esistenza può seriamente limitare la veloci-

tà di funzionamento e le risorse a disposizione.

Tipicamente, inoltre, un worm si diffonde fra server in rete, sfruttando vulnerabilità note per penetrare in sistemi non protetti.

#### **Trojan Horse**

Il cavallo di Troia o Troiano è un programma modificato che esegue funzioni particolari e potenzialmente nocive all'insaputa del possessore, a cui il programma appare funzionare normalmente. Lo scopo di un Trojan Horse, fedele al mito ellenico, è spesso quello di permettere dall'esterno un accesso, ovviamente non autorizzato, al sistema su cui viene eseguito.

#### **Bomb**

Una bomba può essere un virus, un worm o qualcosa di analogo che si attiva in un determinato momento, dando luogo all'azione nociva per cui è stata realizzata. I meccanismi di attivazione possono essere legati ad una data, un giorno della settimana o un'ora specifici (time bomb) o correlati a qualche evento specifico di varia natura (logic bomb).

#### **Back door**

Una back door (o trap door) è un meccanismo (incorporato al momento della creazione in un software esistente o introdotto in tempi successivi come un trojan horse nel sistema) con cui si permette l'accesso al sistema, a prescindere dai metodi di accesso noti e conosciuti del possessore.

La back door può essere inserita dallo sviluppatore di un programma per operazioni di manutenzione o per ricattare chi ne fa uso, oppure da un intruso, che dopo aver violato la macchina sfruttando una vulnerabilità non protetta, vuole garantirsi la possibilità di rientrare sul sistema per vie autonome, senza dover riutilizzare la vulnerabilità usata la prima volta.

**I personaggi che popolano l'underground informatico hanno nomi quali:**

#### **Hacker**

Un hacker è un programmatore o tecnico informatico in grado di realizzare software particolarmente innovativo o valido.

Nonostante questa definizione tutt'altro che maligna, i media hanno spesso abusato del termine hacker per indicare un "pirata informatico", che penetra su sistemi remoti o elimina la protezione del software contro la pirateria.

Un termine più corretto per questa definizione è cracker.



### **Cracker**

Chi attacca sistemi remoti al fine di violarne le protezioni e prenderne il controllo o chi rimuove le protezioni di un software o, ancora, coerentemente con il significato della parola inglese, chi riesce a "rompere" e superare una qualsiasi forma di protezione informatica.

### **Script kiddie**

Si definisce tale, con nemmeno molto velato spregio, il "ragazzino" che, utilizzando strumenti e software comuni nell'ambiente underground, attacca sistemi remoti in modo sistematico.

Tradizionalmente lo script kiddie non ha le capacità tecniche di un cracker esperto, ma può essere ugualmente pericoloso per il carattere sistematico su larga scala dei suoi "scan" automatizzati.

### **Azioni tipiche da cracker sono:**

#### **Spoofing**

L'atto di modificare una connessione o un passaggio di dati in modo da far credere al destinatario di comunicare con un'entità diversa da quella che è realmente.

#### **Sniffing**

Il controllo e il monitoraggio del contenuto di pacchetti che transitano su una rete. Tramite lo sniffing tutte le informazioni che vengono inviate sono visibili, quindi se si tratta di informazioni sensibili come una login e una password, possono essere visualizzate.

#### **Defacing**

La modifica dell'home page, o di altre pagine, di un sito web, da parte di un cracker dopo un'intrusione eseguita con successo.

#### **Scanning**

L'analisi di un sistema remoto finalizzata all'individuazione di vulnerabilità note (vedi in seguito).

La forma di scanning più basilare è quella rivolta all'individuazione delle porte aperte sul sistema remoto. A sua volta, è possibile eseguire degli scanning più specifici alla ricerca di vulnerabilità sui servizi disponibili sulle porte aperte trovate.

### **Altri termini che si incontrano spesso quando si parla di sicurezza informatica:**

#### **Plaintext - cleartext**

Un testo in chiaro, leggibile così come è stato scritto. Se qualcuno è

in grado di accedere a questo testo è quindi in grado di leggerne il contenuto.

#### **Cipher text**

Un testo criptato, il cui contenuto deve essere decriptato per essere leggibile. In termini generici di sicurezza, usare delle connessioni o dei messaggi cifrati è raccomandabile in quanto anche nel caso in cui il testo giunga ad occhi non autorizzati a leggerlo, questi non potranno decodificarlo senza le opportune chiavi di decriptazione.

#### **Access Control List - ACL**

Un elenco di regole volte a individuare dei pacchetti secondo diverse caratteristiche (IP sorgente, porta di destinazione, IP destinazione ecc.) al fine di eseguire determinate azioni come permetterne il flusso o interromperlo. Vengono tipicamente implementate su dei firewall ma si possono riferire in ogni contesto in cui l'accesso ad una data risorsa è limitata in qualche modo.

#### **Trusted**

"Fidato". È un aggettivo che si riferisce a qualsiasi elemento in rete (Indirizzo IP sorgente, host, network...) da cui ci si possono aspettare connessioni non ostili. Tipicamente da certe sorgenti fidate si permette l'accesso a servizi di un host che sono impediti a tutti gli altri indirizzi IP.

#### **Vulnerability**

Una vulnerability è un difetto nell'implementazione di un protocollo o di un software che permette azioni ostili che possono intaccare la sicurezza di un sistema. Le vulnerabilità possono essere "note", cioè descritte in mailing list o su appositi archivi, oppure anche ignote, cioè non comunemente conosciute ma già scoperte ed eventualmente utilizzate da qualche cracker.

Molti prodotti di security scanning si basano proprio sugli archivi delle vulnerabilità note.

#### **Buffer overflow**

È una tecnica di hacking che consiste nell'inserire in qualsiasi contesto possibile una grande quantità di caratteri in modo da cercare di mettere in difficoltà il programma che deve gestirli qualora non preveda meccanismi di controllo sulla lunghezza delle variabili che gestisce. Quello che può accadere è che, da un certo byte in poi, il testo in eccesso provochi il collasso, o crash, del software o una intrusione vera e propria.



### Rootkit

*E' un insieme di tool e programmi che vengono utilizzati da un cracker dopo un'intrusione allo scopo di cancellare le proprie tracce e assicurarsi la possibilità di ritornare sul sistema violato anche senza dover riutilizzare la vulnerabilità usata la prima volta.*

## **Q**uali sono i rischi nei quali posso incorrere se ho un computer magari connesso a internet?

*Di solito quando si parla di sicurezza si pensa solo ai danni derivanti da attacchi esterni da virus o simili o da violazioni della riservatezza dei dati.*

*Sarebbe opportuno preoccuparsi in primo luogo dalle minacce al nostro sistema, cioè al nostro hardware al nostro software e ai nostri dati, che possono derivare da eventi più normali.*

*Ci sono rischi associati al fatto che il computer è un apparecchio connesso alla rete elettrica:*

*"Se lo aprite mentre la presa di corrente è attaccata alla spina, vi prendete una scossa elettrica e salutate questo mondo;*

*"Se state lavorando al computer e, per esempio, state scrivendo una lettera, l'eventuale improvvisa mancanza di corrente elettrica vi fa perdere quello che avete scritto e potrebbe anche provocare dei danni al computer stesso.*

*Vi è poi la possibilità che un malintenzionato potrebbe cercare di appropriarsi del vostro computer per:*

*"furto di hardware o software;*

*"furto di informazioni.*

## **I**n effetti non ci avevo pensato. Potrei capire meglio quali sono i rischi di cui si parla spesso attraverso degli esempi?

*Senz'altro. Tornando alla possibilità di furto, non c'è solo il malintenzionato che fisicamente cerca di arricchiarsi alle vostre spalle. Potrebbe farlo utilizzando una connessione del vostro sistema alla rete. Ci sono i "virus", ossia software fatti apposta per distruggere la logica dei computer o per rubare informazioni, che possono penetrare nel computer e compiere, a vostra insaputa, le finalità per le quali sono stati costruiti da terzi, vuoi seguaci di filosofie tecnologiche (anche detti "hacker"), vuoi bande criminali o più semplicemente aziende commerciali che a volte agiscono ai limiti della legalità.*

*Un malintenzionato potrebbe rubarvi i pezzi di ferro per rivenderli, ma se scrivete software, può esserci interesse a rubarvelo; se fate*

*una professione di possibile interesse di terzi per le informazioni che avete (ad esempio: magistrato, notaio, medico, funzionario addetto alle gare di appalto, ecc.) un terzo può cercare di carpire le informazioni utili a lui personalmente o comunque rivendibili sul mercato o a dei committenti.*

*Tenete presente che anche i vostri dati personali collegati ad un comportamento caratteristico (ad esempio navigazione su internet dalle 22.00 alle 24.00) costituiscono informazioni "ghiotte" per le società specializzate nella creazione di banche dati per esigenze di marketing e che quindi non esitano a utilizzare ogni mezzo consentito (e anche non consentito) per catturarli a vostra insaputa.*

*Se fate acquisti in rete (ad esempio: ordinate libri, partecipate ad aste su Internet, ecc.) dovete utilizzare un codice identificativo ed una chiave segreta di accesso (anche detta: password) per farvi riconoscere e comunicare gli estremi di un mezzo di pagamento (carta di credito): la loro "cattura" permette a terzi di fare acquisti a vostre spese!*

*Se scambiate software con altri, ad esempio via dischetto o CD ROM, un "virus" potrebbe farvi perdere quello che avete memorizzato sul computer.*

*Vi basta ??*

## **E**siste un decalogo delle misure minime di sicurezza che devo adottare per proteggermi dai virus e dagli hacker?

*Probabilmente ne esiste più di uno; c'è anche una legge che stabilisce le misure minime di sicurezza che certi soggetti devono adottare per la protezione di certi dati.*

*Tutti i decaloghi e le piccole guide come questa sono buoni purchè voi abbiate chiare le vostre esigenze e questi documenti vi aiutino effettivamente a capire a quali rischi potete andare incontro suggerendovi possibili contromisure.*

*Siccome non siete esperti in materia, potete rivolgervi, per i giusti suggerimenti, a un "guru", intendendo con questo termine, in modo scherzoso, un esperto di computer di vostra fiducia; in tale categoria potreste includere il fornitore dal quale avete acquistato il computer.*

## **A**bbiamo capito! Allora cominciamo a parlare di contromisure? Per esempio come mi proteggero dalle cadute di corrente elettrica?



Innanzitutto, se state scrivendo qualcosa, usate frequentemente la funzione di salvataggio del testo o dei dati su disco fisso.

E' anche opportuno attivare, se i programmi che utilizzate le prevedono, funzioni di salvataggio automatico ad intervalli di tempo definiti o funzioni che prevedono a creare copia del documento o del file prima che iniziate a modificarlo.

Nel manuale di istruzioni del software che state usando troverete come realizzare le contromisure di cui sopra.

Dal punto di vista dei danni che possono essere arrecati al computer per effetto dell'improvvisa mancanza di corrente mentre state lavorando, la nostra esperienza ci dice che i computer più recenti sono stati realizzati anche avendo a mente tali eventualità e, quindi, non ci risulta siano avvenuti danni seri a dei personal computer.

Se vi trovate in zone dove la fornitura di energia elettrica è particolarmente critica (interruzioni frequenti, sbalzi di tensione, microinterruzioni, ecc.), esistono delle apposite "batterie", denominate gruppi di continuità o "ups", che possono essere applicate fra la presa di corrente ed il computer al fine di stabilizzare la tensione e fornirvi corrente elettrica che vi consenta almeno di chiudere il lavoro che avevate iniziato.

Potete rivolgervi al negozio che vi ha venduto il computer per un preventivo.

## Come mi proteggo da eventuali scosse elettriche?

Se non vi siete protetti da eventuali scosse elettriche quando usate l'asciuga capelli, la lavatrice o toccate il frigorifero, è un po' strano che ci pensiate parlando di computer! Ci preoccupate alquanto!

Ci consoliamo pensando che questa piccola guida è almeno servita a farvi prendere coscienza di un rischio molto grave e i cui danni possono andare ben oltre quelli relativi al vostro corredo informatico.

Ci auguriamo che in casa abbiate la messa a terra ed un interruttore differenziale che tolga la corrente in caso qualcuno prenda la scossa. Se la risposta è negativa o non siete sicuri, vi suggeriamo di rivolgervi quanto prima al vostro elettricista di fiducia.



## Quando mi devo preoccupare della sicurezza del mio computer? Solo quando è in Internet? E se non accedo mai ad Internet?

Cominciamo a distinguere le due situazioni.

Dobbiamo infatti considerare un computer che non si connette mai ad internet (cosiddetto stand alone) da un computer che sia connesso anche occasionalmente.

In linea di massima un computer stand alone è sicuramente meno esposto (se poi utilizziamo il nostro computer senza mai leggere un floppy o un CD rom che venga dall'esterno sicuramente i nostri rischi sono ridotti al minimo, ma anche il suo utilizzo sarebbe ridotto al minimo!).

Le misure cui abbiamo accennato (ad es. salvataggi periodici dei documenti su cui lavoriamo, protezioni da caduta di corrente) possono essere utili per garantire la disponibilità del sistema e dei suoi dati.

A questo fine è sempre opportuno effettuare copie periodiche dei dati e del software; per i primi la cosa più semplice è copiare integralmente su un CD ROM tutte le cartelle che contengono dati.

Per il software è in primo luogo buona norma possedere una copia di riserva dei dischi di installazione (se avete scaricato il software da internet, create voi una copia su un CD ROM): questa accortezza ci permetterà di reinstallare un software (sistema operativo compreso) eventualmente non più disponibile.

Sul vostro sistema sono però presenti altri dati dei quali magari non conoscete nemmeno l'esistenza, ma che sono indispensabili per il vostro sistema: parametri di configurazione, personalizzazioni, rubriche, ecc.

Questi dati possono essere memorizzati nelle cartelle dei programmi o del sistema operativo.

Anche in questo caso una semplice copia su CD può essere la soluzione più semplice, ma può richiedere molto spazio e inoltre potrebbe non essere agevole il recupero dei dati relativi a personalizzazioni e configurazioni.

Potete utilizzare anche funzioni del sistema operativo o prodotti specializzati per singole tipologie di dati e informazioni: sono molto efficienti ma possono anche risultare complessi nell'utilizzo.

La soluzione a nostro avviso più pratica è utilizzare prodotti che creano una copia "immagine" del sistema, cioè una fotografia in formato compresso del contenuto del disco: il vostro fornitore sarà lieto di fornirvi tutte le indicazioni. Se poi siete bravi potete spulciare nei CD ROM allegati alle riviste specializzate o direttamente su internet.



Passando invece alle misure adottabili per garantire l'integrità e la riservatezza di quanto è contenuto nel vostro sistema, se al vostro computer possono accedere anche altre persone, è opportuno attivare la protezione a mezzo password fornita dal "bios" del sistema.

Quando accendete la macchina avrete notato che sullo schermo appaiono una serie di messaggi prima della partenza del sistema operativo (windows o altro): sono i messaggi di controllo generati dal bios, un software presente nell'hardware del computer cui spettano una serie di incombenze tecniche.

Questo programma può essere acceduto e configurato (leggete in proposito le istruzioni del computer o della scheda madre) in modo tale che richieda una password al momento dell'accensione del sistema.

Con l'occasione potreste configurare il bios in modo che il sistema possa essere inizializzato solo dall'hard disk, e non da altri supporti rimovibili (CD o floppy); anche per questo consultate i manuali già citati.

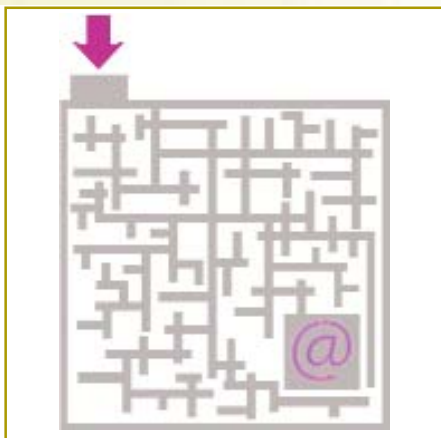
Non si tratta di misura di sicurezza invalicabili, ma sicuramente in grado di tenere lontani una buona parte di potenziali attaccanti. Attivare anche la richiesta di una password all'avvio del sistema operativo può rilevarsi una misura utile, specialmente con l'ultima versione di windows.

Se sul vostro computer mantenete informazioni particolarmente riservate può essere utile adottare un software che su vostra richiesta impedisca l'accesso a un determinato file solo fornendo una password.

Tutte le suite di produttività individuale, quali ad esempio office di microsoft, consentono di utilizzare questa funzione; esistono poi software che consentono di proteggere con meccanismi analoghi intere cartelle o una partizione del vostro hard disk.

Si tratta in questo caso di meccanismi di protezione sufficientemente forti quindi attenzione a non dimenticare le password.

Anche l'utilizzo di screen saver con password può risultare utile: dopo un certo tempo di attesa, alla partenza dello screen saver, viene precluso di nuovo l'accesso ai programmi e alle cartelle di



Windows se non viene digitata una password reimpostata. Tale password deve essere inserita entrando nel setup del BIOS dalle proprietà del Desktop (tasto destro da una zona qualsiasi), sotto cartella "screensaver": inserirne uno e scegliere l'opzione "al ripristino proteggi con password" (per Windows XP) del computer.

Esiste anche la possibilità di inserire una password di sistema: L'operazione, sui PC compatibili, si esegue generalmente premendo il tasto Canc quando indicato dall'apposita scritta in basso allo schermo nella fase di accensione e avvio del computer. In alcuni computer la procedura di lancio del programma di setup può essere diversa (Tasto Canc, oppure Ctrl-Alt-Esc, oppure Ctrl-Shift-Esc, F2 per i portatili ecc.). Una volta entrati nel Setup del BIOS, dovrà essere ricercata la sezione Password. Le diciture variano in base al tipo di BIOS. Una volta inserita tale password, il computer non effettuerà più l'avvio del sistema operativo se non viene inserita la password giusta.

**A** proposito di password, mi dicono che possono essere recuperate con programmi facilmente reperibili; come fate a dire che un meccanismo di protezione basato su password è forte?

Qui il discorso si fa complesso e cercheremo di essere il più chiari possibile.

Una password è un insieme di caratteri che permettono l'accesso ad un computer o a funzionalità dello stesso; è una misura di sicurezza valida se il proprietario non la rivela a nessuno e quindi non la scrive su documenti facilmente accessibili.

E' però chiaro che se per paura di scordarvela generate una password che vi ricordi qualcosa di personale (il nome di vostra moglie o dei vostri figli, la vostra data di nascita) sarà abbastanza semplice per chi vuole accedere ai vostri dati intuire, con pochi tentativi, la vostra password di accesso.

Dire che la password è un meccanismo di sicurezza forte, significa che provare a ricavarla tentando tutte le possibili combinazioni di caratteri può richiedere giorni o settimane utilizzando i programmi cui accennate.

Ma se la password contiene parole di senso compiuto (ad esempio bisonte51) i programmi di cui sopra hanno il compito molto semplificato, in quanto fanno uso di dizionari appositamente creati.

Insomma una password deve essere abbastanza complessa da richiedere tempi lunghi per il suo recupero, ma essere abbastanza semplice da poter essere memorizzata.

Inoltre, per maggior sicurezza deve comunque essere periodica-



mente (ogni 20 - 30 giorni) cambiata.

Le cose si complicano ulteriormente considerando che di password non ce n'è una sola ed è opportuno che non usiamo sempre la stessa. A questo punto dovremmo fornirvi delle regole ed un procedimento generale per costruirvi le vostre password, ma il buon senso impone di non indurvi alla paranoia.

A meno quindi che sul vostro computer non ci siano segreti di stato, potete seguire questi semplici consigli.

Quando generate una password:

- utilizzate almeno 8 caratteri
- non limitatevi ai soli caratteri alfabetici, ma utilizzate anche numeri, caratteri speciali, maiuscole e minuscole
- utilizzate una frase sufficientemente lunga e che ricordate con facilità (una poesia, una preghiera, un motto di vostro padre, ecc.) e costruite la password utilizzando la lettera iniziale di ogni parola (un esempio, da non utilizzare perché ampiamente sfruttato: NmdcdnV1
- in alternativa utilizzate una parola comune storpiandola in modo che non corrisponda più a una parola rintracciabile su un dizionario (sia italiano che inglese) e aggiungete caratteri a caso (per esempio, ZisontEe47)

#### **LE REGOLE DEL CERN PER UNA PASSWORD SICURA**

1. non usare il proprio nome e cognome, nemmeno abbreviato;
2. non usare altre informazioni facili da reperire come date e numeri di telefono;
3. non usare nomi e nomignoli di animali domestici, figli, partner e parenti;
4. non usare acronimi facili e sequenze di lettere o numeri sulla tastiera;
5. non usare nomi di cartoni animati, star della musica, luoghi o automobili;
6. non usare password corte con meno di 6 caratteri;
7. usare password composte da caratteri alfabetici insieme con numeri e caratteri speciali come chiocciola, punti esclamativi o di domanda e parentesi;
8. usare password che riportino il suono di una parola o frase straniera;

9. usare versetti da poesie o detti di cui però utilizzi solo la prima lettera o alcune lettere per ciascuna parola, combinando minuscole e maiuscole;

10. concatenare più parole brevi unendole con un + oppure con trattini o con @.

**Link** [http://consult.cern.ch/writeup/security/security\\_3.html](http://consult.cern.ch/writeup/security/security_3.html)

Comporre password seguendo tutte queste regole risulta difficile anche per chi scrive, ma è però basilare: non immaginate quanto possa essere facile dedurre una password costruita senza attenersi alle regole indicate. Ci permettiamo di consigliare di attenersi sicuramente ai divieti di cui ai punti 1-6 e di utilizzare il criterio 9 per la composizione che risulta sufficientemente adeguato per soddisfare tutte le esigenze (riportare l'esempio contenuto nella risposta originale)

## **E** per quanto riguarda i Virus? Possono attaccare un computer non connesso a internet?

Chi lavora con personal computer da un po' di tempo ricorderà che gli attacchi alla disponibilità ed all'integrità di sistemi, software e dati, perpetrati attraverso virus sono nati quando non si sapeva nemmeno cosa fosse internet.

Gli attacchi quindi possono ancora oggi avvenire a mezzo di floppy, CDROM o altri dispositivi rimovibili.

La contromisura consiste nel procurarsi e installare un buon prodotto antivirus: ce ne sono molti e per ovvii motivi non possiamo indicarvi le nostre preferenze.

Un programma antivirus, come peraltro qualsiasi software di sicurezza, ha la necessità di essere periodicamente aggiornato a fronte delle nuove minacce che in questo settore nascono ogni giorno. Se prevedete di non collegarvi mai a internet questo può essere un problema, dal momento che gli aggiornamenti ormai vengono forniti soltanto attraverso questo mezzo.

## **H**o un personal computer a casa e lo usa solo mio figlio per i compiti. Non ho l'accesso ad Internet. Sono necessarie misure di sicurezza?

In linea di massima sì, anche se saremmo portati a pensare che i suoi giochi e i suoi dati sono meno importanti: sono però importanti per lui!



*Inoltre i ragazzi si scambiano software come noi scambiavamo figurine e ciò aumenta il rischio.*

*Anche se le misure potranno essere meno impegnative di quelle descritte, è comunque formativo abituare i ragazzi ad essere consapevoli dei rischi che si corrono utilizzando un computer.*

*A proposito di formazione, i nostri ragazzi possono essere grandi utilizzatori di software e audio visivi illegali, se non produttori.*

*A parte le pene pesanti nelle quali si può incorrere e le nostre posizioni personali nei confronti delle multinazionali del software, le case discografiche o cinematografiche che mantengono alti i prezzi dei prodotti originali, sarebbe opportuno evitare di essere di cattivo esempio in questo campo.*

*La disciplina sul diritto d'autore, è bene ricordarlo, serve in primo luogo a tutelare i legittimi diritti che derivano ad un autore per il suo lavoro.*

**V**oi utilizzate sempre il termine virus, ma mi risulta che esistono spyware, worm, troian, sniffer, asynchronous attack, ecc.

*Bravissimi per l'elenco e specialmente per l'ultimo tipo di attacco che è roba da hacker seri!!*

*Se lo desiderate, ma non so a cosa possa servirvi, possiamo continuare con l'elenco.*

*Se andate da un medico presumiamo che non vi interessi l'ultima sua relazione ad un convegno, ma una soluzione al vostro problema.*

*Noi non ci consideriamo a livello dei medici, ma vorremmo che questo fosse il vostro approccio al problema.*

*In questa piccola guida noi intendiamo per virus qualunque software che si installi su un computer, senza il controllo del sistema operativo o dell'utilizzatore, per compiere azioni in generale dannose e sia in grado di replicarsi e diffondersi.*

*Il tipo di azione dannosa (il c.d. attacco), le tecniche di inserimento su un computer o su una rete e altre caratteristiche possono portare a una classificazione in tipologie dai nomi più o meno sinistri e fantasiosi.*

*Se l'argomento vi appassiona su internet potete trovare tutti i glossari e le guide tecniche che desiderate, come anche, purtroppo, le guide per il perfetto novello hacker: entrambe richiedono comunque un livello di conoscenza che probabilmente non avete e, soprattutto, alla cui acquisizione non dovrete essere interessati in quanto occupati in altre faccende.*

**P**erò devo sapere che rischi corro se accedo ad Internet?

*I rischi sono molti e non basterebbe un libro per esporre tutte le minacce e le contromisure possibili; e meglio quindi esaminare situazioni d'utilizzo e vedere cosa si può fare.*

*Vi invitiamo a visitare il sito [www.poliziadistato.it/pds/informatica/index.htm](http://www.poliziadistato.it/pds/informatica/index.htm) dove cliccando sulla voce CONSIGLI troverete una serie di suggerimenti concreti e di provata efficacia.*

**B**ene, allora cominciamo dalla connessione alla rete: ho saputo che anche lì ci sono minacce

*Normalmente, ma è presumibile ancora per poco, ci si connette a Internet da casa propria utilizzando un modem e una normale linea telefonica: praticamente il modem combina un certo numero corrispondente ad un altro modem, stabilisce la connessione e il vostro computer si collega a quello del Vostro fornitore (c.d. "provider").*

*Collegandosi a certi siti è possibile che ad un certo click venga scaricato ed attivato un software che, senza che ve ne accorgiate, abbatte la connessione esistente e ne stabilisce un'altra con un numero telefonico a tariffa elevatissima: gli effetti si manifestano sulla bolletta!. Si tratta di una truffa perpetrata utilizzando la vostra imprudenza. Ricordate che, come già detto, la prudenza e il sano buon senso sono la prima barriera e forse la più valida.*

*Contromisure tecniche possono essere l'utilizzo di linee veloci ADSL sulle quali il giochetto appena descritto non è realizzabile; è pur vero che tali linee realizzano però una connessione continua alla rete e quindi una maggiore esposizione alle minacce.*

*Mantenendo le stesse modalità di connessione si può utilizzare un programma di controllo apposito detto "antidialer": ce ne sono molti disponibili gratuitamente in rete (una possibile soluzione su [www.digisoft.cc](http://www.digisoft.cc)).*

**E** quando lavoro con la posta elettronica?

*Il messaggio di posta di per se non è in grado di causare danni: sono i suoi contenuti speciali e gli allegati che possono costituire serie minacce.*



Senza poi considerare che messaggi assolutamente innocui dal punto di vista della sicurezza informatica possono essere fastidiosi, se non addirittura pericolosi.

A livello personale un buon antivirus è senz'altro necessario; molti provider offrono un servizio di controllo aggiuntivo sulla vostra posta che sicuramente è una ulteriore contromisura.

Ricordate comunque che qualunque meccanismo automatico di filtraggio della corrispondenza, per quanto sofisticato, vi esporrà sempre al rischio di eliminare contenuti o allegati "buoni".

Anche in questo caso la vostra prudenza può evitarvi molte seccature: controllate bene i messaggi in arrivo e se avete dubbi che non riuscite a risolvere, ad esempio con una telefonata, sul mittente o sull'oggetto, non esitate a cancellare definitivamente il messaggio e i suoi allegati. Non lasciatevi mai tentare dalla curiosità: alcuni messaggi riportano testi e mittenti quasi credibili e allegati apparentemente innocui (tipo: lettera.txt); guardando meglio il nome dell'allegato si scopre che è mascherato: in realtà il nome è: "lettera.txt .exe" (quindi con contenuti potenzialmente pericolosi), solo che il qualificatore ".exe" non entra nella finestra di visualizzazione.

Una tecnica molto semplice quanto utile è quella di consultare e gestire i propri messaggi direttamente nella casella del server e scaricare sul computer solo ciò di cui si è ragionevolmente sicuri; un programma gratuito per fare ciò può essere "magicmail" e lo trovate su [www.geeba.org/magic/](http://www.geeba.org/magic/)

Dal momento che le caselle di posta elettronica sono di fatto gratuite può essere utile averne più di una e destinarle ad uno specifico utilizzo: un indirizzo sarà quello che fornirete alla vostra banca, un altro sarà strettamente personale, un altro sarà quello che fornirete in tutte le occasioni e che sarà una specie di casella "trash" sulla quale dirigere tutta la "spam" pubblicitaria, ecc..

Se avete bisogno di garantire la vostra identità ai destinatari o accertarvi di quella dei vostri mittenti, è senz'altro necessario che voi e i vostri corrispondenti vi procuriate un certificato di firma digitale: ci sono molte certification authority accreditate in grado di fornire tale servizio in Italia.

Un'ultima accortezza: se non desiderate più ricevere posta da qualcuno, non aderite mai ai servizi di cancellazione da mailing list (ad esempio: "se non desiderate più ricevere queste mail inviate una mail all'indirizzo [nuntereggepiù@mobasta.it](mailto:nuntereggepiù@mobasta.it)..."): semplicemente non rispondete e cancellate il messaggio: prima o poi vi classificheranno come indirizzo non consultato e la pianteranno.



## E se vado in chat?

In questo caso il problema non è più di natura tecnica, nel senso che nulla si può aggiungere a quello che abbiamo già suggerito (o andremo a suggerire più avanti) e ci sembra opportuno riportarvi i consigli della Polizia di Stato che condividiamo:

La diffusione dei sistemi chat-line ed email è riuscita ad influenzare il modo di incontrarsi e di interagire delle persone. Sempre più utenti di internet si conoscono sulla rete e alcune di queste conoscenze si trasferiscono nel mondo reale con incontri "dal vivo", a volte con soddisfazione (si moltiplicano i matrimoni tra persone conosciute in chat), a volte con profonde delusioni, altre volte con situazioni pericolose.

Un aspetto su cui vogliamo soffermarci è la mancanza di una identità certa negli utenti delle chat. Alcuni uomini e donne, sfruttando l'anonimato offerto dalla chat, si presentano infatti nelle conversazioni in rete talvolta con un'identità diversa, un sesso diverso un'età diversa. E in questo tutto sommato non c'è niente di male.

La rete consente infatti di sperimentare, senza troppi rischi, cosa vuol dire appartenere ad un'altro genere o come ci si sente ad essere un adolescente o cosa vuol dire svolgere una professione diversa. L'importante è però, per gli utenti delle chat, essere coscienti di questa situazione e non dimenticare mai che il loro interlocutore, per motivi vari, può essere diverso (o diversa) da quello che dichiara di essere, con tutto ciò che ne consegue.

Una facilità estrema nel lasciarsi andare a confidenze anche riguardanti aspetti intimi della propria vita, con una persona appena

conosciuta in chat, è insomma una cosa che comporta un certo coefficiente di rischio che va considerato

Questo non vuol dire ovviamente che si debba rinunciare a comunicare con persone appena conosciute (in fondo è la cosa più divertente che offre la chat) o di dover rinunciare all'allargamento della cerchia degli amici incontrando nel mondo reale delle persone conosciute on-line. Bisogna a nostro avviso semplicemente ricordare che le chat-line rispecchiano il mondo che le ha create.

Contengono cultura, informazione, dibattito politico, amore, arte, solida-



rietà, e soprattutto possibilità di nuove e interessanti amicizie, ma anche mercanti di pornografia, truffatori, terroristi, pedofili, maniaci come, del resto, la parte del mondo che si articola fuori del cyberspazio.

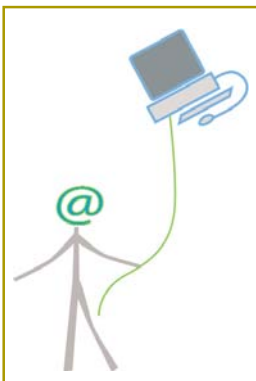
Nella chat si incontrano quindi persone di tutti i tipi. Ci sono, come nel mondo reale, persone a posto e brutti ceffi, nella stessa identica percentuale di una strada affollata o di qualsiasi altro luogo pubblico. Nei contatti con persone nuove conosciute sulle chat-line sembra quindi manifestarsi nei navigatori una minore diffidenza rispetto a quando si muovono nel mondo reale e una certa facilità alla caduta di tabù e resistenze.

In effetti la maggior parte dei "navigatori" adulti ed esperti ha imparato ad usare un minimo di cautela nell'interagire con chi non si conosce e tale cautela è generalmente sufficiente per evitare brutte sorprese.

Se si conosce qualcuno sulla chat e si decide di incontrarlo dal vivo, dare il primo appuntamento in un luogo pubblico e affollato e non andare all'appuntamento da solo rappresenta una precauzione sufficiente per evitare brutte sorprese.

Non è la stessa cosa per i bambini. La loro curiosità unita all'ingenuità può metterli in condizione di rischio nel momento in cui vengono avvicinati on-line da soggetti con cattive intenzioni, ad esempio con pedofili.

Sarebbe opportuno per questo motivo accompagnare i bambini nella navigazione e insegnargli a raccontare sempre ai genitori le loro esperienze di navigazione.



## **E** quando navigo sul web?

Qui il discorso dovrebbe allungarsi parecchio.

Tenete presente che ogni volta che digitare sul vostro browser un indirizzo ([www.chissadove.it](http://www.chissadove.it)) quello che compare non è una visualizzazione di contenuti che risiedono su un computer nella rete, ma bensì il risultato di software scaricato ed eseguito sul vostro computer.

Software in esecuzione che, potenzialmente, può fare qualunque cosa: mettere il vostro computer sotto il controllo di un altro utente della rete, rintracciare i vostri dati personali ed inviarli a qualcuno, registrare le vostre abitudini in fatto di navigazione, cambiare la pagina di partenza del vostro browser, innescare la visualizzazio-

ne di un numero infinito di pagine bloccandovi il computer, ecc. In questo caso la prudenza può aiutarvi ma sicuramente non è sufficiente perché effettivamente molti attacchi avvengono a prescindere dalle vostre azioni.

## **A** allora vediamo qualche caso pratico: se mi si apre automaticamente una pagina di Internet non richiesta o non prevista, che devo fare?

Bisogna distinguere se ciò capita all'inizio della navigazione o durante la stessa.

Nel primo caso si tratta di un virus che ha settato la pagina iniziale del vostro browser. Per ripristinare dovrete aggiornare il vostro antivirus e farlo girare su tutto l'hard disk: se non funziona andate sul sito del fornitore dell'antivirus per cercare informazioni o rivolgetevi al solito amico "guru".

Per prevenire il problema potete installare un programma gratuito (Start Page Guard) reperibile sul sito [pjwalczak.com](http://pjwalczak.com).

Nel secondo caso si tratta sempre di una specie di virus contenuto nella pagina web su cui siete andati che ha attivato un meccanismo cosiddetto di "pop up": se capita non spaventarsi ma interrompere il collegamento e agendo sulla combinazione di tasti "ctrl alt canc" individuare il browser e sospenderne l'esecuzione.

Per il futuro potreste settare le opzioni del browser in modo da inibire la possibilità di attivare il pop up.

## **M** i dicono che alcuni virus possono trasmettere ad altri i mie dati personali: come faccio ad accorgermene e ad evitare il problema?

I virus destinati a questo scopo prendono il nome di spyware e la loro esistenza può in certi casi essere palese: ci sono software famosi che vengono diffusi gratuitamente a condizione che ci si registri e si accetti di rilevare le proprie abitudini di navigazione; in altri casi è l'installazione di un programma gratuito (cd: freeware) che provvede ad installare il software spyware.

Rilevare questo tipo di virus è abbastanza semplice. Basta installare un software gratuito specifico (ad esempio: "ad aware" che potete reperire sul sito [www.lavasoft.nu](http://www.lavasoft.nu)) e farlo girare periodicamente (ovviamente mantenendolo aggiornato come qualsiasi software destinato a fornire servizi di sicurezza).

Attenzione: è probabile che eliminando la componente spyware di un programma, quest'ultimo non funzioni più e vi costringa a scegliere: utilizzare il software ed essere spiati oppure niente!



## **I**cosiddetti "banner" che mostrano avvisi pubblicitari sono pericolosi?

*In linea di massima i banner sono così palesi che è difficile pensare ad essi come a dei virus. Inoltre Internet offre programmi di tutti i generi che, distribuiti in modo del tutto gratuito o quasi, permettono di soddisfare qualunque esigenza.*

*Ci sono software famosi che vengono diffusi gratuitamente a condizione che ci si registri e si accetti di far comparire banner pubblicitari. Certi programmi, però, nascondono al loro interno delle insidie: si tratta di "spyware", ossia di quei programmi che utilizzano particolari algoritmi che permettono di raccogliere informazioni sul nostro personal computer e sulle nostre abitudini e di trasmetterle, via Internet, a terze parti. Il pericolo da gran parte delle applicazioni che, mentre sono in esecuzione, visualizzano banner pubblicitari. Tali banner vengono, infatti, prelevati da un server che si occupa della loro gestione: è facile, quindi, intuire come si instauri, in questo caso, un collegamento diretto tra il nostro personal computer e un server Web che si occupa dell'esposizione di banner.*

*Diciamo subito che i software distribuiti gratuitamente via Internet, sono migliaia ma ben poche le persone che, a fronte di un esborso economico di solito abbastanza contenuto, si registrano presso gli autori acquistando una licenza d'uso personale. Per ovviare a questo problema alcuni sviluppatori hanno deciso di fare uso della tecnologia "adware": a fronte dell'esposizione di banner pubblicitari all'interno dei loro prodotti software, essi ricevono un compenso variabile che, qualora il proprio programma abbia successo su scala mondiale, possono portare a grandi guadagni.*

*Il pericolo deriva dal fatto che, quando utilizziamo software "adware", non possiamo sapere, in modo certo, quali dati vengono trasmessi durante la connessione Internet. I programmi "adware", in quanto tali, ricevono dati da un server Web (le informazioni riguardanti i banner pubblicitari che il programma deve esporre) ma come possiamo essere certi che la comunicazione avvenga solo in questa direzione e non vi sia, quindi, anche una trasmissione di informazioni dal nostro computer verso la rete Internet?*

*È proprio questa la differenza che distingue i software "adware" dagli "spyware". Mentre i primi si limitano esclusivamente a ricevere informazioni da Internet in modo da visualizzare banner pubblicitari, i secondi inviano spesso anche dati relativi alla nostra identità, alle nostre abitudini, alle informazioni memorizzate sul*

*personal computer. Si pensi, per esempio, a quali e quante informazioni siano memorizzate all'interno del registro di sistema di Windows: codici di registrazione di software con il nostro nome e cognome in chiaro, username e password per la connessione ad Internet e tanti altri dati relativi alle applicazioni installate ed alla configurazione del sistema. Operazione assai semplice risulterebbe per un programma recuperare questi dati e ritrasmetterli altrove attraverso la Rete.*

*Un programma antispyware è di solito in grado di rilevare questi meccanismi, ma attenzione: togliere i banner pubblicitari può significare smettere di poter il programma!*

## **M**a c'è un modo di impedire che la connessione ad internet venga utilizzata solo per quello che voglio io?

*L'esigenza è fra le più sentite e la risposta si chiama firewall (letteralmente muro di fuoco): si tratta di software in grado di analizzare tutto il traffico diretto dal computer alla rete e viceversa e selezionare ciò che deve transitare e ciò che deve essere bloccato.*

*Questi programmi, nati per l'utilizzo in contesti professionali, sono oggi disponibili in versione per personal computer e prendono il nome di personal firewall; installando un simile software, ad esempio, posso impostarlo in modo tale da consentire l'accesso alla rete solo al mio browser e al mio client di posta elettronica e non consentire accessi al mio computer dalla rete che non siano risposte alle transazioni effettuate dai suddetti programmi.*

*Si tratta in generale di programmi abbastanza complessi ma per fortuna alcuni risultano abbastanza facili da utilizzare e ugualmente efficienti (ad esempio "zone alarm" che potete reperire gratuitamente su [www.zonelabs.com](http://www.zonelabs.com)).*

## **S**e mi accorgo che il computer sta improvvisamente avendo dei comportamenti "anomali" cosa devo fare? E' possibile che un hacker mi sia entrato nel computer?

*E' abbastanza difficile indicare dei sintomi precisi: rallentamento nell'esecuzione dei programmi, comportamenti inattesi, attività su internet (i due computer dell'icona della connessione ambedue accesi) in assenza di vostra attività, possono essere sintomi di pericolo. Se avete adottato tutte le misure che vi abbiamo suggerito, dovrete essere abbastanza tranquilli, se non lo siete fate uno scan*



completo con i programmi di antivirus e anti spyware e se non trovate nulla rivolgetevi al vostro amico guru per una eventuale bonifica della vostra macchina.

## **P**er motivi di studio vado su siti che non conosco: corro dei rischi?

Sicuramente la navigazione alla cieca fa correre dei rischi ma a volte è necessaria.

Antivirus aggiornato, antidiabler e personal firewall sono il minimo per stare tranquilli.

## **E**se ad utilizzare internet sono i miei figli, o meglio i miei bambini?

Sicuramente ogni genitore ha piacere che i propri figli acquisiscano quelle conoscenze che per lui sono state un grosso problema (il computer, la lingua inglese, internet).

Da padri di famiglia, e non da professionisti dell'educazione, vorremmo cercare in primo luogo di tranquillizzare i nostri "colleghi": noi che siamo cresciuti a computer, internet e inglese (perché altrimenti non potevamo capire i computer e internet) abbiamo comunque dovuto acquisire altre conoscenze per mantenerci aggiornati e poter continuare a svolgere la nostra attività.

Quindi ogni cosa a suo tempo e non abbiate fretta di far navigare vostro figlio su internet: l'espressione può sembrare esagerata ma riteniamo che mandare un bambino da solo su internet equivalga ad abbandonarlo in mezzo ad una strada.

Molti enti e associazioni hanno pubblicato decaloghi di comportamento per genitori e figli circa le regole di comportamento su internet; l'argomento esula un po' dalle nostre competenze (e rischierebbe di coinvolgerci sul piano personale) per cui riportiamo qui di seguito i consigli in materia del Servizio polizia di stato e delle comunicazioni, reperibili sul sito [www.poliziadistato.it/pds/informatica/index.htm](http://www.poliziadistato.it/pds/informatica/index.htm), che ci sembrano i più concreti.

### **Consigli per i bambini:**

- Navigare su Internet può essere utile e divertente, ma prima di cominciare è importante conoscere e ricordare alcune regole molto importanti.



- Non date mai informazioni come il vostro nome e cognome, indirizzo, nome della scuola o numero di telefono a persone conosciute su Internet.
- Non mandate mai vostre foto a qualcuno conosciuto via Internet senza il permesso dei vostri genitori.
- Leggete le e-mail con i vostri genitori, controllando con loro ogni allegato al messaggio.
- Dite subito ai vostri genitori o ai vostri insegnanti se leggete o vedete qualcosa su Internet che vi fa sentire a disagio o vi spaventa, per esempio fotografie di persone adulte o di bambini nudi.
- Non fissate incontri con persone conosciute via Internet senza il permesso dei vostri genitori.
- Ricordatevi che on line le persone possono non essere quello che dicono di essere. La bambina con cui credete di chattare potrebbe essere un uomo adulto!

### **Consigli per i genitori**

- Dite ai vostri figli di non fornire dati personali (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici), potrebbero essere utilizzati da potenziali pedofili.
- Controllate quello che fanno i vostri figli quando sono collegati e quali sono i loro interessi.
- Collocate il computer in una stanza di accesso comune piuttosto che nella camera dei ragazzi e cercate di usarlo qualche volta insieme ai vostri figli.
- Non permettetegli di usare la vostra carta di credito senza il vostro permesso.
- Controllate periodicamente il contenuto dell'hard disk del computer usato dai vostri figli, verificando la "cronologia" dei siti web visitati.
- Cercate di stare vicino ai vostri figli quando creano profili legati ad un nickname per usare programmi di chat.
- Insegnategli a non accettare mai di incontrarsi personalmente con



chi hanno conosciuto in rete, spiegando loro che gli sconosciuti così incontrati possono essere pericolosi tanto quanto quelli in cui ci si imbatte per strada.

- Leggete le e-mail con i vostri figli, controllando ogni allegato al messaggio.
- Dite loro di non rispondere quando ricevono messaggi di posta elettronica di tipo volgare, offensivo o pericoloso e, allo stesso tempo, invitateli a non usare un linguaggio scurrile o inappropriato e a comportarsi correttamente.
- Spiegate ai vostri figli che può essere pericoloso compilare moduli on line e dite loro di farlo solo dopo avervi consultato.
- Stabilite quanto tempo i vostri figli possono passare navigando su Internet e, soprattutto, non considerate il computer un surrogato della baby-sitter.
- Esistono particolari software, facilmente reperibili su internet, che impediscono l'accesso a siti non desiderati (violenti o pornografici per esempio). I "filtri" possono essere attivati introducendo parole-chiave o un elenco predefinito di siti da evitare. E' opportuno però verificare periodicamente che funzionino in modo corretto e tenere segreta la parola chiave.

In merito all'ultimo consiglio, i programmi per il c.d. Parental control sono sicuramente uno strumento efficace e mettono a disposizione funzioni valide (controllo sugli orari di utilizzo, sull'accesso a file a cartelle, inibizione dell'accesso a siti o file indesiderati, controllo dei siti visitati e della corrispondenza ricevuta) ma pensiamo valga la pena di ricordare alcune cose. Come qualunque contromisura a fronte dei rischi legati alla sicurezza informatica esso deve essere gestito e la stessa Polizia di Stato parla di verifiche periodiche; con questa tipologia di strumenti la gestione si estende anche all'aggiornamento della lista dei siti o delle parole indesiderate. Questi software infatti basano la loro azione di filtraggio su differenti meccanismi:

- la presenza di particolari certificazioni sul sito (una sorta di bollino blu rilasciato ai proprietari del sito e che dovrebbe garantire i contenuti);
- l'assenza dal sito di particolari parole considerate indesiderabili, che i genitori possono integrare;

- la presenza del sito in un elenco di siti indesiderabili, aggiornabile dai genitori.

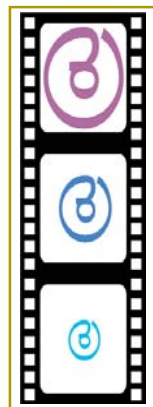
Dal momento che alcuni di questi meccanismi di filtraggio sono disponibili anche su alcuni browser, provate a impostare le funzioni ed a tenere aggiornati i vari elenchi, magari collegandovi a i vari siti specializzati.

Inoltre, più si spinge l'azione di filtraggio, più si limita la navigazione: includere la parola "sesso" tra le parole indesiderabili vi impedirebbe di accedere a documenti serissimi di natura scientifica.

Ricordando che l'utilizzo di sistemi di filtraggio non può esaurire il problema e soprattutto non può sostituire i genitori, vi segnaliamo un'idea interessante realizzata ormai da alcuni anni dal sito [www.davide.it](http://www.davide.it) che fornisce il servizio di provider gratuito come gli altri aggiungendovi un servizio di filtraggio dei contenuti violenti o pornografici. Il servizio, gratuito per le famiglie, è tenuto costantemente aggiornato da una équipe di specialisti e da una rete di "angeli", cioè dalle segnalazioni degli utenti. E' un servizio molto efficiente e, tra l'altro, senza costi aggiuntivi segnala anche la presenza di virus negli allegati della posta elettronica.

**A questo punto ho capito che i rischi sono tanti e che se voglio cautelarmi devo installare tanti prodotti diversi e impegnarmi a mantenerli costantemente aggiornati! La prospettiva non è delle migliori: non c'è qualcosa che raggruppi tutte le funzioni in un unico pacchetto?**

Noi abbiamo indicato singole contromisure a fronte di singole categorie di minacce, ma è chiaro che se vi trovate, a fronte delle vostre esigenze, a dover installare più di tre o quattro prodotti la complessità che introducete nella vostra attività potrebbe essere critica e influenzare l'utilizzo produttivo che fate del computer. In questi casi è meglio decidere di acquistare presso un negozio specializzato un prodotto che rientri nella categoria delle suite per la sicurezza. Si tratta di prodotti complessi dal punto di vista delle contromisure che pongono in essere per coprire un'ampia gamma di minacce (antivirus, antispam, controllo privacy, parental control, personal firewall, ecc.) ma contemporaneamente estremamente guidati nel loro utilizzo permettendovi, in ultima analisi, di costruire agevolmente il vostro sistema di contromisure a fronte delle vostre esigenze.



**A** desso parliamo di quelli che consideriamo gli utilizzi più rischiosi e cioè quando utilizzo Internet per utilizzare uno dei tanti servizi di commercio elettronico. E' vero che sono avvenute delle frodi che hanno interessato le persone che eseguono acquisti od operazioni bancarie su Internet? Quali sono quelle più frequenti?

La risposta alla prima domanda è la stessa che si potrebbe dare a una domanda del tipo. "E' vero che possono verificarsi incidenti stradali in autostrada?".

**Dal già citato sito della Polizia di Stato riportiamo le principali truffe telematiche che vengono realizzate su internet (di solito inviando una email):**

- Finte vendite all'asta sul WEB, con merci offerte e mai inviate ai clienti o con prezzi gonfiati;
- Offerta di servizi gratis su internet che poi si rivelano a pagamento o mancata fornitura di servizi pagati o fornitura di servizi diversi da quelli pubblicizzati;
- Vendite di hardware o software su catalogo on-line, con merci mai inviate o diverse rispetto a quanto pubblicizzato
- Schemi di investimento a piramide e multilevel business;
- Opportunità di affari e franchising;
- Offerte di lavoro a casa con acquisto anticipato di materiale necessario all'esecuzione di tale lavoro;
- Prestiti di denaro (mai concessi) con richiesta anticipata di commissione;
- False promesse di rimuovere informazioni negative per l'ottenimento di crediti (es. rimozione di nominativi da black-list);
- False promesse di concessione (con richiesta di commissione) di carte di credito a soggetti con precedenti negativi;
- Numeri a pagamento (tipo 899) da chiamare per scoprire un ammiratore segreto o una fantomatica vincita (di vacanze, di oggetti).



Per quanto riguarda le cautele da adottare, c'è poco di informatico e molto buon senso e ci associamo al consiglio che viene dalla fonte appena citata: **nella maggior parte dei casi il tentativo di truffa inizia con l'invio di una email al potenziale vittima. In caso di sospetto salvare l'email e informare immediatamente la Polizia delle Comunicazioni.**

**E** che rischi corro utilizzando la carta di credito su internet e come posso cautelarmi?

Non si può escludere che degli hacker neanche troppo abili abbiano potuto con tecniche di sniffing entrare in possesso di numeri di carte di credito.

Questi fenomeni però si misurano quantitativamente e i numeri ci dicono che fino ad oggi esistono tecniche e metodi più semplici per entrare in possesso di numeri di carte di credito e magari di copia delle firme: quante volte, ad esempio, avete consegnato la vostra carta di credito ad un cameriere sconosciuto senza sapere cosa ne facesse prima di restituirvela con la ricevuta di spesa?

Si può affermare che oggi i siti di banche e organizzazioni commerciali serie applicano sufficienti misure anche se si potrebbe fare di più.

Utilizzare misure di sicurezza forti, quali ad esempio la firma digitale, implica però una serie di problemi che esulano dall'ambito strettamente tecnico: accettazione di un livello di complessità maggiore da parte dei consumatori, adozione di standard internazionali esigenti in materia, necessità per i consumatori di dotarsi della tecnologia necessaria, ecc.

Da un punto di vista pratico, ci associamo ancora una volta alla concretezza della Polizia di stato ([www.poliziadistato.it/pds/informatica/index.htm](http://www.poliziadistato.it/pds/informatica/index.htm) e cliccare su "Consigli")

L'utilizzo su internet della carta di credito in assenza di supporti speciali quali lettori di smart card e/o bande magnetiche, si limita di solito alla richiesta da parte del sito del numero di carta di credito e della relativa data di scadenza. Con questo genere di utilizzo sono possibili transazioni fraudolente da parte di due categorie di persone:

1. pirati informatici (o dipendenti infedeli del sito internet) che acquisiscono i numeri della carta attraverso un'intrusione telematica;



**2.** altre persone che a qualsiasi titolo vedono la carta (camerieri, postini, conoscenti) e che si annotano il suo numero.

Per ridurre i rischi di frode è quindi consigliabile in primo luogo far sì che la propria carta venga maneggiata dal minor numero di persone possibile. In secondo luogo è opportuno effettuare spese su rete internet utilizzando siti conosciuti o che abbiano un minimo di credibilità sia per quanto riguarda il prodotto venduto, che la solidità del marchio. Forniamo a tal proposito tre accortezze che l'utente di un sito che effettua commercio elettronico dovrebbe adottare:



**1.** i siti dediti al commercio elettronico utilizzino protocolli di sicurezza che permettano di identificare l'utente, (il più diffuso è il Secure Socket Layer - SSL), e ne impediscano l'accesso casuale e non, ad altri utenti. A tal proposito un'accortezza da utilizzare è di verificare se durante la transazione in basso a destra della finestra compaia un'icona con un lucchetto che sta a significare che in quel momento la connessione è sicura;

**2.** evitare di fornire troppe informazioni personali nonché quelle relative al proprio conto corrente all'interno di un sito, in quanto per andare a buon fine la transazione necessita solamente del numero della carta di credito e la relativa scadenza;

**3.** per quanto possibile fare uso delle varie soluzioni di home banking che le banche mettono a disposizione per controllare quasi in tempo reale il proprio estratto conto del conto corrente o della società che gestisce la carta di credito, in modo da bloccarla tempestivamente qualora si disconoscessero delle spese addebitate; a tal proposito alcune banche mandano un messaggio di posta elettronica al cliente con gli ultimi tre movimenti sul proprio conto corrente;

**4.** verificare con attenzione gli estratti conto segnalando immediatamente alla società emittitrice ogni transazione sconosciuta.

Dal punto di vista del singolo utente, cioè dal vostro punto di vista, è questo il caso in cui non potendo eliminare completamente il rischio è il caso di contenerlo.

Senza intenzione di fare promozione commerciale, un modo per contenere i danni potenziali può essere quello di acquistando una carta di debito ricaricabile che avendo un limite di credito da voi definito può limitare l'eventuale danno di intercettazione del numero solo a tale importo.

## **C**ome faccio a sapere se un determinato sito su Internet è affidabile o no, in particolare quello della mia Banca?

Valgono in primo luogo le cautele dettate dal buon senso. Se comprate qualcosa su internet verificate la credibilità del venditore e del prodotto (ad esempio verificando che il venditore esista sulle pagine gialle, abbia un indirizzo e un telefono fisso a cui risponde qualcuno).

Come detto nella risposta precedente, i siti dediti al commercio elettronico, e quindi anche quelli delle banche, utilizzano protocolli di sicurezza che permettano di identificare l'utente, (il più diffuso è il Secure Socket Layer - SSL), e ne impediscano l'accesso casuale e non, ad altri utenti.

Per controllare la sussistenza di tale condizione verificare se durante la transazione in basso a destra della finestra compaia un'icona con un lucchetto che sta a significare che in quel momento la connessione è sicura, e quindi che nessuno può catturare le informazioni che scambio con la banca via Internet.

## **L**a mia banca mi ha dato un software per fare le operazioni via Internet: è sicuro?

In linea di massima se un fornitore rende possibile usufruire dei propri servizi su internet attraverso l'installazione di uno specifico software, vuol dire che intende utilizzare livelli di sicurezza più elevati rispetto allo standard realizzabile con i prodotti comuni. Inoltre se un fornitore di servizi adotta una simile soluzione, in un certo senso "da la faccia", nel senso che se qualcosa non dovesse funzionare i danni derivanti alla sua immagine sarebbero molto grave. Rispondere in dettaglio alla domanda richiederebbe considerare singole fattispecie, cosa non possibile in questa sede. Possiamo solo suggerire di verificare bene cosa dice in merito il contratto sottoscritto per il servizio, in particolare se viene citato l'ottenimento di certificazioni di sicurezza per il software che andrete ad installare sul vostro computer.



## **F**accio le mie operazioni con la mia banca via Internet. Che cautele devo avere?

Come già accennato in precedenza tutte le banche che forniscono servizi di home banking mettono a disposizione funzionalità che permettono di controllare in tempo reale la movimentazione del vostro conto corrente o della società che gestisce la carta di credito, in modo da potersi attivare tempestivamente per segnalare alla banca operazioni che disconosciamo o chiedere il blocco della carta. A tal proposito alcune banche mandano un messaggio di posta elettronica al cliente con gli ultimi tre movimenti sul proprio conto corrente.

Altre vi segnalano la data e l'ora dell'ultima volta che vi siete connessi al sito.

Verificate sempre con attenzione gli estratti conto segnalando tempestivamente qualsiasi discordanza alla banca o alla società emettrice della carta di credito.

## **C**osa devo fare se mi imbatto in pubblicità ingannevole su internet?

La pubblicità ingannevole in rete è un fenomeno diffuso, in parte sostenuto dalla stessa natura del mezzo e della sua fruizione: si ha fretta, pressati dal tempo e costo della connessione, talvolta si esamina sommariamente l'offerta e le sue condizioni integrali restano ignorate, talvolta la qualità delle immagini che illustrano il prodotto è scadente e non lascia apprezzare dettagli importanti. Le pretese qualità, spesso miracolose, dei beni proposti, sono difficili da verificare online. Dunque ad un esame meno attento del messaggio si aggiunge una difficoltà di verifica della qualità del bene, tipica della vendita a distanza.

Ad aggravare questa situazione si profila la non punibilità (o la oggettiva difficoltà di punire) operatori commerciali scorretti che hanno sede legale fuori dell'Unione Europea, dove invece la legislazione è chiara e precisa in materia di pubblicità ingannevole: in altri stati lo è molto meno o addirittura la materia non ha alcuna regolamentazione (ciò significa che ingannare con un messaggio pubblicitario è praticamente lecito).

Il rimedio ci viene offerto dall'Autorità Garante della Concorrenza e del Mercato, alla quale si può presentare una denuncia per pubblicità ingannevole\*, e che ha poteri inibitori sul messaggio, ovvero può interromperne la diffusione. Non bisogna infatti accontentarsi di dissuadere il figlio dall'acquisto o di scrivere una lettera sdegnata al

venditore: la denuncia è un gesto di civiltà e di prevenzione, un sostegno a tutti i giovani consumatori che non hanno avuto la fortuna di avere un genitore accorto al fianco. L'istruttoria dell'Autorità, aperta su segnalazione, si muove in modo autonomo e non ha alcun costo o conseguenza potenziale per il denunciante, anche in caso di non accoglimento (in questo è ben diversa da una denuncia al tribunale, che può essere comunque presentata per ottenere risarcimento del danno indotto dall'ingannevolezza del messaggio, che ha influenzato l'acquisto). Vale dunque la pena di farla, sempre.

### **Autorità Garante Della Concorrenza e del Mercato**

**Piazza Verdi 6/A**

**00198 Roma**

**Tel: 06/858211**

**Fax: 06/85821256**

**Sito internet: [www.agcm.it](http://www.agcm.it)**

**e-mail: [antitrust@agcm.it](mailto:antitrust@agcm.it)**

## **Q**uali possono essere le insidie degli acquisti online?

Oggi è possibile acquistare online libri, dischi, abbigliamento e accessori, software e hardware, viaggi e servizi di ogni genere, insomma praticamente tutto quello che si può acquistare con il sistema commerciale tradizionale.

L'attrattiva dell'acquisto online è legata in parte alla novità del mezzo, in parte al fatto che il prezzo è spesso migliore di quello dei rivenditori convenzionali (scompaiono i costi della struttura distributiva), in parte al fatto che rende accessibili prodotti di tutto il mondo, a prezzi ben diversi da quelli dei beni di importazione, facendoli arrivare direttamente a casa.

A proposito degli acquisti online, una prima considerazione da fare è che il rischio più invisibile, quello più insidioso, va ravvisato nella sollecitazione ad effettuare acquisti in base da una suggestione più che a reale necessità: il mondo virtuale è colorato ed accattivante, offre facili e rassicuranti occasioni per coltivare un senso di appartenenza e di identificazione, inibisce la capacità critica e la naturale diffidenza che accompagna un acquisto tradizionale, in una situazione commerciale ordinaria. Sarà opportuno, dunque, conservare una certa cautela e senso critico.

■ Tra i problemi più frequenti legati al cosiddetto commercio elettronico (o e-commerce) vi sono:



- *il caso in cui il bene o servizio è illustrato con messaggi di pubblicità ingannevole*
- *il caso in cui siano richiesti dati personali (ad esempio per la spedizione), senza specificare l'uso che ne verrà fatto in seguito*
- *il caso in cui il pagamento con carta di credito non sia sicuro, ed i dati della carta vengano intercettati per farne uso fraudolento*
- *il caso in cui il venditore accetta valute diverse dalla propria ma applica un cambio estremamente sfavorevole o in cui la banca che effettua la transazione (o il circuito della carta di credito) addebita pesanti commissioni di cambio. Il problema oggi non si pone con tutti i paesi che aderiscono all'Euro*
- *il caso in cui il sito di e-commerce ha una cattiva manutenzione, prodotti, prezzi ed offerte sono obsoleti: si rischia di acquistare beni di cui il venditore stesso non dispone più o che oggi hanno un prezzo diverso da quello indicato*
- *il caso in cui il bene non è disponibile nel modello, tipo o colore prescelto: viene sostituito con altro ritenuto "sostanzialmente equivalente" ad arbitrio del venditore.*

*Particolare attenzione ed una certa diffidenza va riservata alle proposte di entrare in sistemi di vendita conosciuti come "piramidali" (o anche come "catena di S. Antonio") che non offrono adeguate garanzie al consumatore e che aggiungono, ai noti inconvenienti di questo particolare settore, quelli derivanti dal fatto che l'operatore commerciale è remoto e soggetto a legislazione di altro stato.*

## **C**ome difendersi dalle insidie degli acquisti online?

- *Preferite gli operatori dell'area Europea, meglio ancora se dispongono di un rappresentante legale in Italia: in caso di controversia, sarà più facile ricorrere alla giustizia. Con ciò, non si vogliono sottovalutare le garanzie offerte dagli operatori e dalla legislazione dei paesi extracomunitari, ma va ricordato che i problemi processuali correlati alla soluzione del contenzioso con quei paesi sono di difficile soluzione.*



- *Stampate tutte le pagine del sito sui cui si stanno facendo acquisti, particolarmente quelle che illustrano o descrivono il prodotto/servizio offerto, il prezzo e le spese accessorie: servirà per dimostrare cosa avete inteso acquistare, se quello che avete ricevuto o l'importo addebitato non dovessero corrispondere.*
- *Preferite i siti di e-commerce che si appoggiano a sistemi di pagamento sicuri (server con criptazione dati) o, meglio ancora, quelli che affidano la transazione al server di una banca: la transazione effettuata da terzi garantisce la correttezza dell'addebito e la riservatezza dei dati della carta (non comunicati al venditore)*
- *Se è prevista una conferma via e-mail dell'ordine, precisate nell'eventuale spazio riservato alle "note" del vostro ordine, che non desiderate siano trascritti i dati della carta.*
- *Usate la massima prudenza e applicate rigorosamente il cosiddetto "principio di precauzione" se non capite bene tutti i termini dell'acquisto (ad esempio se il sito è in una lingua diversa dall'italiano)*
- *Attenzione con i cosiddetti "supermercati virtuali": a volte, la raccolta dell'ordine e dei dati della carta di credito è eseguita correttamente e su server sicuro, ma poi l'ordine (e con esso tutti i dati) è trasmesso all'operatore interessato via e-mail, con rischio di intercettazione*
- *Non lasciate mai i vostri ragazzi liberi di effettuare da soli procedure di acquisto online con la vostra carta di credito, ma seguiteli sempre e verificate personalmente ogni dettaglio del contratto di vendita (incluse le lunghissime "condizioni generali di contratto", in cui si celano spesso sorprese sgradevoli)*
- *In caso di dubbio sull'esito della transazione con la carta di credito, non effettuate subito un altro tentativo (con il rischio di pagare una seconda volta), ma chiedete conferma all'operatore ed alla eventuale banca che gestisce i pagamenti*

## **C**ome funziona la tutela della privacy in rete?

*Ormai da tempo assistiamo al proliferare di società specializzate nella creazione di elenchi di consumatori (reali o potenziali) di pro-*



dotti e categorie di prodotti, suddivisi e ordinati e classificati in base ai gusti e alle preferenze, alle abitudini di acquisto, alle attività professionali, agli hobby, alla tipologia di nucleo familiare, al luogo di residenza... Si potrebbe continuare all'infinito, elencando le tante notizie che si forniscono senza pensarci su due volte, nel corso di una banale ed insospettabile intervista o di un



questionario compilato per ricevere il premio di un concorso a punti. Esse vengono utilizzate per l'individuazione del target specifico (cioè della porzione di pubblico che presenta il profilo più interessante per l'azienda che vuole promuovere il prodotto/servizio) destinatario di programmi pubblicitari a base di lettere, telefonate, visite a casa di incaricati aziendali...e ora anche di e-mail. Va detto, a questo proposito, che i dati personali hanno un valore economico rilevante, dunque vengono ceduti a terzi ogni volta che sia possibile. Il loro valore è legato al fatto che consentono un notevole risparmio di risorse nel corso delle campagne pubblicitarie, aiutando le aziende a raggiungere solo i potenziali clienti, e non la generalità del pubblico. La fortuna di molte società proiettate nella New Economy si è fatta proprio così: offrendo allettanti servizi gratuiti (come l'accesso ad Internet o la posta elettronica stessa) hanno potuto raccogliere immense basi dati che contenevano ogni sorta di notizie sul loro pubblico; al momento di quotarsi in borsa, questi database hanno avuto un peso enorme in fase di valutazione: un vero patrimonio, è il caso di dirlo. In tutta l'Europa la tutela dei dati personali è assicurata da una legislazione abbastanza matura: la legge italiana (L. 675/96) ha istituito una Autorità Garante\* preposta alla vigilanza della corretta applicazione delle disposizioni in materia, ha stabilito la necessità di concessione del consenso alla raccolta, al trattamento ed alla diffusione dei dati personali da parte dell'interessato, ha fissato un elenco di diritti in suo favore (tra cui la facoltà di richiederne la cancellazione o la rettifica), istituendo fra l'altro un obbligo di comunicazione al Garante da parte di coloro che detengono banche dati. Ciascuno ha dunque il diritto di conoscere (gratuitamente) notizie sul chi e come sta trattando i suoi dati e può opporvisi.

Il vero problema si pone quando questi dati sono stati rilasciati ad una azienda extraeuropea, soggetta, come noto, alla sola legisla-

zione del suo paese e comunque difficilmente perseguibile.

Bisogna dunque ricordare sempre che, se possibile, è meglio non concedere i propri dati (o almeno non concedere il consenso al loro trattamento), onde prevenire il rischio che ne sia fatto un uso diverso da quello per cui sono stati concessi. Questa regola vale in un albergo ai Caraibi come su un sito Internet. Un rischio specifico, semmai, della rete, risiede nella non sempre garantita sicurezza della loro trasmissione o della loro permanenza nei database sui server, in qualche modo violabili (la loro intercettazione da parte di pirati informatici è peraltro poco conveniente, a meno che non si tratti dei numeri di una carta di credito).

**\*Garante per la Protezione dei Dati Personali**

Piazza Montecitorio, 121 00186 Roma  
Tel 06/696771 Fax: 06/6967785  
Sito Internet: [www.garanteprivacy.it](http://www.garanteprivacy.it)  
e-mail: [garante@garanteprivacy.it](mailto:garante@garanteprivacy.it)

<b>Perdita di programmi e / o dati memorizzati su disco fisso</b>	Copia periodica (ad esempio ogni settimana) dei "file" e programmi su CD Rom o su nastro magnetico; Mantenere una copia su CD dei programmi utilizzati e relativo codice di registrazione; Oppure, dotare il computer di due dischi fissi e fare la copia del primo sul secondo; in ogni caso, è bene anche fare una copia (con periodicità più bassa) su CD Rom o nastro magnetico e riporre detto supporto in un luogo sicuro e distante dalla stanza nella quale risiede il computer; Se nella zona vi è il rischio di cadute improvvise di tensione, dotare il computer di una batteria "tampone" in grado fornire continuità di corrente elettrica senza sbalzi e di dare energia al computer per il tempo necessario a permetterne lo spegnimento "regolare"; Nelle tabelle delle opzioni dei programmi utilizzati (ad esempio: Word, Excel, ecc.) inserire l'opzione di salvataggio in background (per Word: Strumenti/ Opzioni/ Salva/ Consenti salvataggio in background ogni ___ minuti).
<b>Accesso al computer non autorizzato</b>	Abilitare la password d'accensione e quella dello "screen saver"; Usare una password il più possibile difficile da indovinare (ad esempio: zufalo51); Acquisire un "personal firewall" e personalizzarlo in modo da limitare la possibilità che ignoti, mentre "navigate" in Internet, vi catturino delle informazioni riservate; Evitare di accedere a siti sconosciuti e di contenuto non molto "trasparente" (ad esempio: c.d. siti a "luci rosse");
<b>Attacco da virus</b>	Personalizzare in modo adeguato i parametri di sicurezza offerti dal "browser" (ad esempio: nel caso di Microsoft Internet Explorer: Strumenti / Opzioni Internet / Protezione / Livello di protezione/ e fissare i giusti livelli di protezione); Acquisire e mantenere aggiornato un antivirus efficace; Periodicamente eseguire l'apposito programma dell'antivirus per la ricerca di possibili virus nascosti nel disco fisso;
<b>Accesso ad Internet da parte di minori</b>	Non aprire email da sconosciuti e, soprattutto, non aprire gli allegati di questi messaggi; Evitare di accedere a siti sconosciuti e di contenuto "dubbio" (ad esempio: a "luci rosse"); non permettere che i bambini accedano al computer e, quindi, ad Internet senza la vostra presenza e supervisione (usate password di protezione; mettetevi il computer in una stanza ove avete maggiore visibilità; ecc.); adottate, quindi, tutte le più opportune cautele, in modo da limitare al massimo la possibilità che possano cadere in una trappola tesa da male intenzionati (cfr. per gli opportuni suggerimenti il sito: <a href="http://www.poliziadistato.it/pds/informatica/index.htm">www.poliziadistato.it/pds/informatica/index.htm</a> ).
<b>Altre avvertenze</b>	Se possibile, non lasciare mai il computer acceso quando non siete in casa; Non aprire il computer a meno che siate certi di saper operare senza creare pericoli per voi o per il sistema; se lo aprite, accertatevi prima di avere tolto tutte le spine dalle prese di corrente; Quando navigate in Internet, non comunicate mai i vostri dati personali, a meno che non siate assolutamente certi che il sito il destinatario sia effettivamente chi dice di essere e che, qualora, nella peggiore delle ipotesi, i vostri dati venissero in possesso di terzi, il danno che potreste riceverne non è elevato; in caso contrario, o usate un sistema alternativo (ad esempio: fax), oppure, se possibile, inviate i dati protetti da cifratura e certificato digitale.

