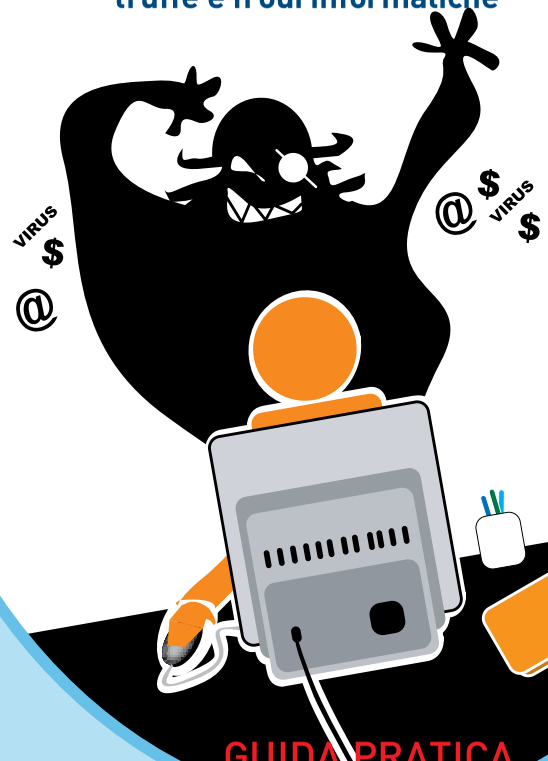
FEDER CONSUMATORI
BOLOGNA

Le insidie ed i rischi di Internet

strumenti e contromisure per evitare truffe e frodi informatiche



GUIDA PRATICA

A cura di:
Avv. Giampiero Falzone,
Consulente Legale Federconsumatori Bologna
Appassionato di Informatica Giuridica

Stampa: FD

IIIª edizione aggiornata ed ampliata

"Realizzato nell'ambito del programma generale di intervento 2010 della Regione Emilia Romagna con l'utilizzo dei fondi del Ministero dello Sviluppo Economico".

FEDERCONSUMATORI
BOLOGNA

SEDE FEDERCONSUMATORI BOLOGNA

Via Del Porto, 16, Bologna 40122
Dalle ore 9,00 alle ore 12,00 e dalle 14,00 alle 17,00.
e-mail: info@federconsumatori.it
www.federconsumatoribologna.it

È possibile tramite appuntamento,
telefonando al 0516087120 fax 0516087122
essere ricevuti da operatori qualificati, presso le seguenti sedi:

- **Bologna (centro): in via Del Porto 12 e 16. .**
- **Bologna (Corticella): in via Corazza n. 7/6.**
- **San Lazzaro di Savena: in via Emilia Levante n. 249/b**
- **Casalecchio di Reno: in Galleria Ronzani n. 3/2.**
- **Budrio: via Martiri Antifascisti 52/54.**
- **Castelmaggiore: piazza della Pace,7**
- **Porretta Terme: in via Borgolungo n. 64.**
- **Vergato: in Galleria 1° maggio.**

Presenza nei Municipi dei Comuni della Provincia:

- **San Giovanni in Persiceto**
- **Calderara di Reno**
- **Bentivoglio**
- **San Pietro in Casale**
- **Funo di Argelato**
- **Galliera**
- **Granarolo Emilia**
- **Anzola dell'Emilia**
- **Crevalcore**
- **Zola Predosa**

REDESIGN

LE INSIDIE ED I RISCHI DI INTERNET: strumenti e contromisure per evitare truffe e frodi informatiche

Piccola guida pratica a tutela dei consumatori

A cura dell'Avv. Giampiero Falzone
Consulente Legale Federconsumatori Bologna
Appassionato di Informatica Giuridica

1 Presentazione

La sicurezza dei dati e delle trasmissioni di rete sono argomenti che, forse più di ieri, oggi, nell'epoca del XXI secolo, d'altronde iniziato proprio con il timore e la paura del c.d. baco del millennio, presentano diverse sfaccettature e problematiche da analizzare.

Questa guida si propone un'analisi delle maggiori insidie cui si possono imbattere i consumatori utilizzando il computer e la rete. Illustrate le insidie, questo lavoro, nello spirito che contraddistingue la Federconsumatori, mira a far conoscere gli strumenti e le contromisure per affrontare tutti i rischi connessi alla sicurezza informatica.

Nella società del terzo millennio, la sempre maggiore diffusione delle tecnologie informatiche ha fatto sorgere, infatti, la legittima esigenza di apprestare un'efficace tutela dei beni-interessi, come il diritto alla riservatezza o il diritto all'integrità del software o il diritto alla sicurezza nelle reti informatiche. Le tecnologie informatiche costituiscono oggi uno strumento essenziale ed irrinunciabile di comunicazione, informazione, elaborazione ed archiviazione dati, e sono utilizzate a tutti i livelli, individuali e collettivi, per le finalità più varie, personali e professionali, pubbliche e private, civili e militari. La diffusione e l'importanza dell'uso del computer nella vita individuale e sociale non poteva non provocarne la distorsione per scopi illeciti, taluni dei quali così gravi da indurre il legislatore a sanzionarli penalmente e in modo molto pesante.

Questo manuale, di facile lettura anche per i non addetti ai lavori, nasce proprio da questa considerazione. I nostri obiettivi, quindi, sono due: 1) offrire indicazioni semplici per difendersi dalle numerose insidie che il web nasconde; 2) proporre un uso consapevole delle nuove tecnologie. Per il raggiungimento di questi obiettivi, molto importante risulta il ruolo della Polizia Postale e delle Telecomunicazioni ed è per questo che molti consigli presenti in questa guida faranno riferimento alle indicazioni reperibili sul sito http://www.poliziadistato.it/pds/informatica/index.htm.

Maurizio Gentilini
Presidente Federconsumatori Bologna

2 Le insidie di Internet in generale

Il Personal Computer, mediante opportuni strumenti e software, può accedere ad Internet, ossia ad una rete mondiale di informazioni. Internet è, in poche parole, una rete risultante dalla connessione di tante reti locali distribuite in tutto il mondo. Immaginiamo, per capirci, a milioni e milioni di computers virtualmente tutti collegati insieme. Ogni computer collegato alla rete (nodo) è in grado di originare, ricevere e trasmettere informazioni. Riesce in queste operazioni grazie all'utilizzo di un protocollo di comunicazione denominato TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol).

Proprio questa caratteristica del web, e cioè la semplicità di scambiare e ricevere informazioni, genera di per sé diverse insidie e diverse trappole per gli utenti meno esperti.

"Collegandosi" ad Internet, infatti, si può essere facilmente vittima di numerose truffe e di numerosi reati informatici (c.d. computers crimes), senza, spesso, accorgersi di nulla, se non solo successivamente.

Le insidie che gravitano nei meandri della rete in maniera diffusa, e di cui parleremo ampiamente nelle pagine che seguono, sono:

- accessi indesiderati e non controllati sul computer dell'utente da parte di soggetti terzi;
- ricevere attraverso siti o messaggi di posta elettronica dei virus, Worm o Trojan;
- imbattersi, a propria insaputa, nei dialers;
- incorrere in clonazioni delle proprie carte di credito, a seguito di acquisti on line;
- imbattersi facilmente, anche non volendo, in siti pedo-pornografici; (molto grave e diseducativo se ad utilizzare il computer ed internet sia un bambino);
- essere vittima di spamming.

Naturalmente, queste sei insidie appena descritte sono quelle che, a nostro avviso, riguardano ed interessano il consumatore che naviga sulla rete, senza avere una particolare esperienza informatica. Esisterebbero, dal

punto di vista giuridico (basti dare uno sguardo alla legge n. 547 del 1993), numerosi reati informatici, cioè reati commessi a fronte di comportamenti illeciti realizzati attraverso l'uso dei computers. Sono reati gravissimi che il nostro legislatore, giustamente, anche se con ritardo rispetto ad altre esperienze giuridiche, ha voluto sanzionare penalmente. Si veda in particolare il codice penale agli articoli 615 ter, 615 quater, 615 quinquies, 617 quater, 617 quinquies, 617 sexies, 621, comma 3, 491 bis, 635 bis, 640 ter.

Nei capitoli che seguono illustreremo le trappole che la nostra esperienza quotidiana, prestata sempre a fianco del consumatore, ci fa definire come le più comuni e ricorrenti.

3 Gli hackers: virus e dialers

• Gli Hackers

Il fenomeno dell'hacking nasce negli Usa tra il 1958 e il 1959 presso il Massachussetts Istitute of Tecnology (***MIT***) di Cambridge, all'interno del *Signal and Power Subcommittee,* uno dei due gruppi in cui si divideva il Tech Model Railroad Club.

Il termine ***hacker*** deriva dal verbo inglese *to hack* (fare a pezzi, tagliare) e, come è dato rilevare dal nome del club citato, non è nato nel mondo dell'informatica, come giustamente ci si potrebbe aspettare, bensì in un club di studenti appassionati di modellismo ferroviario. Le basi dell'hacking erano ormai poste, sin dagli inizi del 1960, specie dal punto di vista concettuale ed etico: l'informazione doveva essere libera; l'hacker si delineava come colui che migliorava qualcosa che oggettivamente era guasta. Anche l'istinto dell'hacker era delineato: correggere e testare i sistemi imperfetti.

Il fenomeno dell'hacking che oggi è a conoscenza di tutti deriva in maniera diretta dal ***phreaking***, da quella stessa cultura, cioè, che ebbe origine al Mit negli anni 50 e che si sostanzia nello studio dei sistemi di telecomunicazione, telefonici in particolare, nonché nella ricerca e sperimentazione delle tecniche idonee ad acquisire il controllo di dette apparecchiature. Da subito l'hacker viene identificato con il cracker, vero e proprio criminale informatico che danneggia dati, diffonde virus, altera i programmi. Gli anni '80 sono il periodo in cui i mass-media scoprono il fenomeno e subito compiono il clamoroso errore di associare indistintamente l'hacking alla criminalità informatica con la quale nulla, o poco, ha a che fare. Gli studiosi, infatti, dividono il fenomeno dell'hacking in due sottoinsiemi: hacking bianco ed hacking nero. L'hacking bianco assurge a simbolo eroico e dunque positivo del fenomeno hacking, mentre quello nero identifica un aspetto negativo dello stesso. L'hacker bianco, infatti, può essere qualificato come colui che irrompe all'interno di un sistema o di una rete senza trarre un manifesto vantaggio ma per esporre, in un certo senso, la debolezza del sistema stesso. Compie, è vero, dei reati informatici, ma con una finalità non "illecita" e soprattutto senza voler trarre dei profitti. La sua azione è mossa da una

ideologia di base che si concretizza nella convinzione che l'accesso ai computers deve essere libero e di tutti. A differenza di un hacker bianco, l'hacker nero (cracker) trae vantaggio economico nell'irrompere in un sistema informatico o telematico. Ecco perché un hacker nero distrugge una rete o un sistema computerizzato e cerca di non rendere conoscibile l'attacco per non dare ad altri l'opportunità di sfruttare la vulnerabilità stessa del sistema. Per lo stesso motivo, strumenti elettivi di un **black hat** sono le frodi informatiche e i virus informatici, ovvero dei programmi composti da istruzioni logiche, in grado di autoreplicarsi e progettati, appunto, per svolgere azioni distruttive o disturbanti all'interno di un sistema informatico. Di questo hacher (hacker nero o cracker) il consumatore deve temere e contro questo vero e proprio criminale il consumatore deve adottare tutte le contromisure di sicurezza per non incorrere, utilizzando la rete, in truffe e frodi.

• I virus

I reati di maggiore interesse che la legge 547/1993 ha disciplinato e che la dottrina fa rientrare nell'operato tipico del black hacker (cracker) sono il danneggiamento di sistemi, dati e programmi (art. 635 bis c. p.) e la frode informatica (art. 640 ter c. p.). Nei confronti dei consumatori il primo reato viene posto in essere mediante i c.d. virus; il secondo anche mediante i c.d. dialers. Ma vediamo nel dettaglio.

Le maggiori categorie di virus che il consumatore contrae utilizzando Internet, senza adottare idonee misure di sicurezza, sono tre:

virus: pezzo di codice in grado di diffondersi e duplicarsi in modo autonomo, attaccando ed unendosi ad un programma o ad un messaggio di posta elettronica. La sua caratteristica è data dalla possibilità di eseguire operazioni dannose sui sistemi infetti.

worm: ha caratteristiche simili ad un virus; la sua unica differenza sta nel fatto di non attaccarsi ad altri programmi, di non causare danni ma è finalizzato a rallentare il computer che si usa.

trojan horse: come dice il nome stesso si tratta di un cavallo di Troia finalizzato a permettere dall'esterno un accesso, ovviamente non autorizzato, al sistema su cui viene eseguito.

• I dialers

Oggigiorno le truffe via internet, perpetrate a danno dei navigatori ignari, creano a questi ultimi elevati danni economici per mezzo di veri e propri "furti virtuali".

È il caso dei dialers, software che, nascondendosi sotto apparenti innocui links o immagini, aprono automaticamente un finto certificato di protezione. Se questo viene accettato, il computer viene automaticamente disconnesso dal provider a cui il consumatore è abbonato per essere ricollegato ai numeri a valore aggiunto, satellitari o internazionali, pagando, a sua insaputa, ai truffatori somme elevatissime per una connessione alla Rete come una telefonata intercontinentale. Inoltre, i dialers possono essere ricevuti anche tramite la posta elettronica sotto forma di software autoinstallanti.

Questa truffa informatica oramai è diventata molto ricorrente. Sono sempre più numerosi i consumatori che quotidianamente incontriamo, disperati dall'aver ricevuto bollette "astronomiche".

Il problema sta anche nel fatto che i Gestori Telefonici, che nel caso dei precedenti numeri 709 provvedevano allo storno, ora rifiutano qualsiasi soluzione transattiva. Per questo motivo, nel paragrafo che segue, illustreremo tutti i consigli più opportuni per evitare queste spiacevoli insidie.

• Strumenti e contromisure per evitare virus e dialers

Per evitare di infettare il proprio computer da virus, worm o trojan horse occorre innanzitutto aumentare il livello di sicurezza del browser internet che si utilizza. Il più comune e diffuso browser è, senza dubbio, Internet Explorer. Aumentare il livello di sicurezza significa, nel caso di specie, limitare o bloccare l'esecuzione automatica di script e ActiveX. Se si utilizza Internet Explorer questo si può fare nel seguente modo:

- scegliere dalla voce di Internet Explorer *"Menu strumenti-opzioni internet-protezione"* e cliccare sul *"livello personalizzato*". Selezionare, quindi, *"chiedi conferma"* al posto di *"attiva"* in tutte le voci che riguardano l'esecuzione di controlli ActiveX;
- una volta portata a termine questa semplice procedura, occorre, naturalmente, installare sul proprio pc un antivirus, cioè un software in grado di intercettare un virus prima che entri sul nostro pc, di riparare il file infetto o di eliminarlo. Consigliamo di aggiornare il proprio software antivirus almeno ogni 15 giorni.

Con questi accorgimenti abbiamo notevolmente aumentato la sicurezza del nostro personal computer, ma occorre anche non essere superficiali e prestare molta prudenza nell'utilizzo della posta elettronica. Infatti, può capitare, anche se con minore frequenza se abbiamo adottato le misure descritte, che una e-mail contenente una minaccia non venga filtrata dal nostro antivirus. In tali circostanze bisogna:

- se esistono dubbi legati al mittente che ha spedito il messaggio, all'oggetto, ecc., cancellare definitivamente il messaggio ed i suoi allegati senza aprirlo;
- se il messaggio ricevuto è scritto in lingua inglese ed ha per oggetto "thanks" oppure "hi" cancellare, senza scrupoli, il messaggio;
- non farsi mai tentare dalla curiosità nel caso di e-mail riguardanti presunte vincite o comunicazioni importanti, con allegati ingannevoli del tipo "lettera.txt", "premio.txt". Cancellare subito questi messaggi, perché in realtà i files allegati non sono di estensione *txt* ma *exe*; sono cioè dei files autoinstallanti. Questo vale anche se si riceve da sconosciuti dei files con estensione zip.
- non rispondere mai al messaggio indesiderato ricevuto.

Per contrastare i dialers, e per quindi evitare spiacevoli sorprese in bolletta, occorre, invece, seguire le seguenti precauzioni:

- disabilitare col proprio gestore tutti i numeri a tariffazione speciale;
- evitare di aprire banner o links sospetti;
- installare un software antidialer, in grado di "staccare" la connessione nell'ipotesi in cui questa venga dirottata verso un numero diverso da quello del proprio provider. Consigliamo, perché può essere reperito gratuitamente, in quanto freeware, *l'antidialer digisoft,* il cui download può essere eseguito al sito internet http://www.digisoft.cc/.

Se applichiamo tutti questi piccoli accorgimenti, sarà molto difficile essere vittime di virus o dialers. Nel caso in cui, però, questo dovesse capitare (la percentuale in questo caso è davvero molto bassa), la Federconsumatori consiglia di sporgere querela presso la Polizia Postale, organo di Polizia Giudiziaria molto efficiente e tecnicamente preparato per il contrasto dei reati informatici (vedi amplius infra cap.7).

• Bluetooth

Lo scopo principale della nascita della tecnologia bluetooth risiede nella capacità di far **dialogare e interagire fra loro dispositivi diversi** (telefoni, stampanti, notebook, computer palmari, etc.) senza la necessità di collegamenti via cavo. In un sistema bluetooth la trasmissione avviene principalmente via radiofrequenza.La tecnologia Bluetooth può essere fonte di virus. A conferma ci sono test condotti da importanti aziende del settore che hanno individuato oltre 1300 dispositivi Bluetooth potenzialmente attaccabili da malware.

• Strumenti e contromisure per evitare truffe via Bluetooth

La Polizia di stato mette a disposizione un breve vademecum di suggerimenti per aiutare gli utenti a non cadere nelle trappole tese con detta tecnologia:

- attenzione a scaricare applicazioni da Internet o nuovi software con il vostro cellulare o computer palmare dotato di tecnologia Bluetooth: prima di procedere all'installazione di nuovi software o scaricare nuove applicazioni da Internet, verificare sempre l'affidabilità della fonte;
- prestare attenzione a eventuali anomalie nel funzionamento del proprio dispositivo: premesso che senza un'applicazione di sicurezza installata è piuttosto difficile rintracciare un virus, ci sono però delle situazioni che possono mettere l'utente in allarme. In linea di massima, infatti, i virus tipicamente causano anomalie sul telefono, come ad esempio l'aumento di attività di comunicazione, un consumo insolito della batteria, la ricezione di messaggi non richiesti, la cancellazione di icone o la modifica delle stesse;
- ricordarsi di disattivare Bluetooth dopo averlo utilizzato e se ciò non è possibile almeno impostare il dispositivo con connessione in modalità "nascosta". Questa precauzione garantisce almeno un livello minimo di sicurezza poiché allunga i tempi di un'eventuale aggressione;
- modificare il nome identificativo del cellulare: molti utenti tendono a mantenere il nome identificativo del proprio cellulare impostato di default dal costruttore, normalmente associato al modello specifico dell'apparecchio. Questa semplice informazione può consentire a un aggressore di associare a un apparato delle vulnerabilità note, che possono quindi essere sfruttate;

- aggiornare sempre eventuali software di sicurezza e antivirus: per poter contrastare con efficacia degli attacchi, tutti i software di sicurezza devono sempre essere aggiornati. Un software di sicurezza non aggiornato è inutile, in quanto la computer insecurity è in continua evoluzione e un software vecchio non è progettato per affrontare nuove problematiche. E' importante sottolineare che "vecchio" può indicare anche solo un mese di vita, dal momento che gli aggiornamenti dei software antivirus si svolgono su base settimanale;
- attenzione alla scelta dei codici PIN per associare i dispositivi: troppo spesso vengono mantenuti i codici forniti dal produttore o, peggio ancora, vengono usate informazioni a cui un aggressore può facilmente risalire (ad esempio la propria data di nascita).

4 Commercio elettronico ed acquisti on line: i rischi connessi all'utilizzo di carte di credito

• I rischi del commercio elettronico

Oggi è possibile, ed è spesso anche molto conveniente, acquistare on line qualsiasi tipo di bene e servizio. Bisogna, però, prestare molta attenzione alle insidie che il commercio elettronico può riservare. Sono tante le truffe telematiche che vengono realizzate in questi casi. Riportiamo di seguito alcune tipologie di frodi che la Polizia Postale elenca statisticamente come più ricorrenti:

- 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).

Nella maggior parte dei casi il tentativo di truffa inizia con l'invio di una e-mail alla potenziale vittima. In caso di sospetto, salvare l'e-mail ed informare immediatamente la Polizia Postale.

• I rischi connessi all'utilizzo di carte di credito

L'utilizzo di carte di credito per effettuare i propri acquisti on line porta in sé numerosi e preoccupanti rischi.

Il rischio principe è quello della **clonazione.** Il problema della truffa tramite carte di credito falsificate è ormai tristemente noto; la carta di credito è un documento intrasferibile per mezzo del quale il titolare può acquistare beni o fruire di servizi presso esercizi commerciali convenzionati con la società emittente della carta stessa, che s'impegna al relativo pagamento, rifacendosi sul conto bancario del titolare.

L'uso fraudolento della carta di credito può avvenire principalmente in due modi:

- attraverso metodi di *"sniffing"* con cui i pirati informatici riescono ad intercettare tutte le informazioni (numero carta, titolare, scadenza) che vengono inviate via internet nel caso di un acquisto on-line;
- attraverso l'utilizzazione, da parte di terzi, delle ricevute di pagamento che il titolare, a seguito di un acquisto in un locale commerciale, ha buttato, senza distruggere.

Ma vediamo gli strumenti da porre in essere per ridurre ed evitare questi rischi.

• Strumenti e contromisure per evitare le truffe del commercio elettronico

Anche in questo caso, la Polizia Postale, ci fornisce molti consigli per evitare le insidie del commercio elettronico. Questo tipo di commercio è sicuramente uno degli aspetti più innovativi offerti da Internet, anche se richiede un pizzico di accortezza non dissimile da quella richiesta nella vita privata. Ad esempio, il fatto che il sito sia scritto nella nostra lingua non è sufficiente a ritenere che stia operando dal territorio nazionale.

A questo proposito, può essere utile utilizzare il servizio offerto dal sito www.checkdomain.com che permette di conoscere la nazionalità del sito ed il nome dei suoi responsabili. Queste informazioni devono essere considerate alla luce di alcuni aspetti quali ad esempio la possibilità di esercitare il diritto di recesso.

Per fare acquisti o operazioni attraverso la rete internet di solito viene richiesto dal sito interessato solo il numero di carta di credito e la relativa data di scadenza. Le truffe, in questo caso, come dicevamo, sono possibili solo da due categorie di persone:

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

Ecco perché bisogna:

- verificare che i siti in questione utilizzino protocolli di sicurezza che permettano di identificare l'utente. Il più diffuso è il Secure Socket Layer (SSL): generalmente durante la transazione, in basso a destra della finestra, compare un'icona con un lucchetto che sta a significare che in quel momento la connessione è sicura;
- evitare di fornire informazioni troppo personali, in particolare quelle relative al proprio conto corrente: perché la transazione vada a buon fine serve solo il numero della carta di credito e la relativa scadenza;
- fare uso, per quanto possibile, delle soluzioni di home banking che le banche mettono a disposizione per controllare - quasi in tempo reale - il proprio estratto conto, in modo da bloccare, tempestivamente, la

carta qualora si disconoscessero delle spese addebitate;

- verificare con attenzione gli estratti conto segnalando immediatamente, alla società che emette la carta, ogni transazione sconosciuta e conseguentemente provvedere al blocco della stessa.

Al fine di evitare spiacevoli sorprese, la Federconsumatori suggerisce, accanto alle indicazioni fornite dalla Polizia Postale, una precauzione semplice, forse scontata, ma fondamentale: *non gettare mai le ricevute della carta di credito nei rifiuti.*
In moltissimi casi (provare per credere) basta comunicare il numero di una carta e la data di scadenza (registrati sulle ricevute che l'esercente deve consegnare come prova di acquisto) per poter tranquillamente effettuare ordini telefonici e relativi pagamenti di beni e/o servizi.

Nel caso in cui, invece, si è rimasti vittime di un uso fraudolento della propria carta bancomat o della propria carta di credito bisogna subito bloccare la stessa, sporgere denuncia (noi consigliamo sempre alla Polizia Postale e delle Comunicazioni) ed inviare appena possibile alle società emittenti una raccomandata a.r., allegando la denuncia rilasciata dall'organo di Polizia, per contestare l'eventuale uso fraudolento. Ebbene sapere, infatti, che nell'ipotesi di commercio elettronico (acquisti on line) o di contratti a distanza si applica l'art. 8 del d.lgs. n. 185 del 22 maggio 1999 e successive modificazioni il quale prevede che "l'Istituto di emissione della carta riaccrediti al consumatore i pagamenti dei quali dimostri l'eccedenza rispetto al prezzo pattuito ovvero l'uso fraudolento della propria carta di pagamento da parte del fornitore o di un terzo".
In genere, come dimostrano varie sentenze sul tema, nella maggior parte dei casi il titolare della carta clonata riesce ad ottenere il rimborso dimostrando di non essere stato lui a compiere l'acquisto (ed indubbiamente in tal caso siamo di fronte ad una *c.d. probatio diabolica*).

Nell'ipotesi in cui il consumatore noti sul proprio estratto conto dei movimenti che disconosce, è opportuno procedere all'immediato blocco della propria carta. Segnaliamo i numeri telefonici delle società della carte di credito più diffuse a cui telefonare per segnalare eventuali dubbi o bloccare immediatamente la carta in caso di furto o smarrimento:

- Servizi Interbancari: 800 151616
- American Express: 06 72900347
- Diner's: 800 393939
- Agos Itafinco: 800 822056
- Deutschebank: 800 207167
- Setefi: 800 825099
- Banca Sella: 800 822056
- Findomestic: 800 866116
- Cartasi/Visa: 800 151616
- Barclay Card: 800 908069
- Unicredit Card: 800 078777
- Poste Pay: 800 902122
- Banco Posta: 800 207167

5 L'utilizzo di Internet da parte dei bambini

• Premesse

Navigare su Internet per un bambino può essere veramente molto utile e divertente. Le potenzialità ludiche e culturali della rete sono veramente tante. Un bambino la può utilizzare (come in realtà la utilizza) per acquisire maggiori competenze informatiche sin da piccola età, per effettuare ricerche e studi, per trovare dei giochi e dei divertimenti.
Prima di cominciare, però, è importante conoscere alcune regole molto importanti, per evitare che i più piccoli siano vittima di diseducazione e, in molti casi, anche di reati pedo-pornografici.
Tali regole devono assolutamente essere conosciute sia dai più piccoli che dai loro genitori.

• Consigli per i più piccoli per un uso consapevole di Internet tratti da:

http://www.poliziadistato.it/articolo/1108-consigli_per_i_più_piccoli

Cari ragazzi, usate Internet perché è un patrimonio di conoscenze e divertimenti ma:

- 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 tratti da:

http://www.poliziadistato.it/articolo/1107-qualche_consiglio_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.

6 La tutela dei dati personali e lo spamming

• Premessa

Risale al 1996 il primo provvedimento in Italia, di carattere organico, sulla riservatezza nel trattamento dei dati personali. Si tratta della legge 675 del 31 dicembre 1996, la cui finalità principale è quella di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e della dignità delle persone; e, soprattutto, si svolga con il consenso del titolare.

Successivamente è stato elaborato il Codice in materia di protezione dei dati personali, meglio noto come T.U. sulla Privacy, adottato con il d.lgs n. 196 del 30 giugno 2003 ed entrato in vigore dal 01 gennaio 2004.
Con l'evoluzione informatica, la trasmissione dei dati ha assunto rilievi enormi. A riguardo è importante ricordare il fenomeno del c.d. "spamming". Lo spamming consiste nella pratica ormai diffusa di inviare e-mail pubblicitarie, non richieste ed autorizzate da parte dei destinatari, con l'obiettivo di promuovere determinati prodotti o servizi attraverso la raccolta di grandi quantità di indirizzi dalle fonti più diverse. Lo spamming usa diversi canali: quello preferenziale è la posta elettronica, ma può impiegare anche qualsiasi altro mezzo che, via Internet, consenta di raggiungere un alto numero di destinatari (ad esempio mailing list, chat, ecc).

Una particolare forma di spamming sono le cosiddette "Catene di Sant'Antonio". Al posto della casella postale della propria abitazione, questa volta c'è l'e-mail di un privato nella quale giunge, sotto forma di posta elettronica, una comunicazione (ad esempio la promessa di eventi fortunati o sfortunati a seconda che si partecipi o meno al gioco) con la richiesta di inoltrare ulteriormente la stessa ad un numero imprecisato di utenti.
Il fenomeno dello spamming, sempre più in crescita, rientra nelle c.d. "comunicazioni indesiderate" e costituisce un chiaro esempio di violazione del T.U. della Privacy e del D.lgs 171/98 che tutela la vita privata nel settore delle telecomunicazioni.

Lo stesso Garante per la Privacy riconosce la necessità di tutelare l'utilizzo dei dati personali nei confronti di forme di pubblicità e comunicazioni particolarmente invasive della sfera privata dei consumatori, come nel caso dello spamming. La disciplina richiede il consenso dell'interessato.

Questo significa che l'operatore commerciale quando intende utilizzare i dati di una persona (come l'e-mail) deve preventivamente informarla e chiedere il consenso dell'interessato, anche se i dati sono presenti in pubblici registri, o pubblicati in Internet.
La newsletter del Garante del 13-19 maggio 2002 riporta una decisione dello stesso Organo che conferma quanto appena descritto; accogliendo il ricorso di un consumatore, l'Autorità Garante ha ribadito che è illegittimo utilizzare a scopo commerciale un indirizzo e-mail, senza il consenso dell'interessato, ed ha inoltre condannato la società convenuta a rifondere al consumatore le spese sostenute per il procedimento.

• Strumenti e contromisure per evitare lo spamming.

Per evitare di ricevere comunicazioni indesiderate e non richieste, occorre seguire i seguenti consigli:

- collegandosi ad un sito, leggere attentamente la nota informativa sul l'uso dei dati personali prima di accettarla;
- se non si vuole ricevere materiale pubblicitario specificare, nel momento in cui si forniscono i propri dati, di non voler essere inseriti negli elenchi relativi all'invio della pubblicità;
- non fornire mai il proprio indirizzo e-mail se non sono indicate le finalità di utilizzo;
- installare sul proprio pc un software anti-spamming, in grado di filtrare i messaggi inviati ad una moltitudine di indirizzi.

Nell'ipotesi in cui, nonostante siano state adottate tutte queste misure, si continuano a ricevere comunicazioni indesiderate, occorre ottenere una tutela giuridico-amministrativa.
In caso di controversie, infatti, è possibile rivolgersi all'Autorità del Garante per la protezione dei dati personali per far sospendere o cessare le operazioni non autorizzate sui propri dati personali. Si può fare questo in tre modi:

- attraverso una segnalazione;
- attraverso un reclamo;
- attraverso un ricorso.

Riportiamo di seguito, tratti dal sito http://www.garanteprivacy.it, i significati di questi tre strumenti di tutela.

SEGNALAZIONE

Che cosa è e quali diritti tutela

Quando non è possibile presentare un reclamo circostanziato (in quanto, ad esempio, non si dispone delle notizie necessarie), oppure non si intende proporlo, si può inviare al Garante una **segnalazione** (art. 141, comma 1, lett. *b)*), fornendo elementi utili per un eventuale intervento dell'Autorità volto a controllare l'applicazione della disciplina rilevante in materia di protezione dei dati personali.

Modalità per la presentazione

La segnalazione può essere proposta in carta libera e non è necessario seguire particolari formalità. Possono essere utilizzati i recapiti indicati nella sezione "Contatta il Garante".

Gratuità

La presentazione di una segnalazione è gratuita.

RECLAMO

Che cosa è e quali diritti tutela

Il reclamo al Garante è, invece, un atto circostanziato con il quale si rappresenta all'Autorità una violazione della disciplina rilevante in materia di protezione dei dati personali (art. 141, comma 1, lett. *a)*). Il reclamo può essere proposto sia quando non si è ottenuta una tutela soddisfacente dei predetti diritti di cui all'articolo 7, sia per promuovere una decisione dell'Autorità su una questione di sua competenza. Al reclamo segue un'istruttoria preliminare e un eventuale procedimento amministrativo nel quale possono essere adottati vari provvedimenti (articolo 143).

Modalità per la presentazione

Il reclamo può essere proposto in carta libera, ma a differenza della segnalazione va presentato **solo** utilizzando il modello e le istruzioni del Garante, utilizzando i recapiti indicati nella sezione "Contatta il Garante".

Diritti di segreteria

Al reclamo va allegata la prova del versamento dei diritti di segreteria, seguendo le indicazioni contenute nel modello.

RICORSO

Che cosa è e quali diritti tutela

Il ricorso al Garante è un atto ancora più formale in quanto la decisione che viene adottata ha particolari effetti giuridici. Occorre, in particolare, seguire attentamente quanto prevede il Codice (articolo 147). Il ricorso va presentato **solo** per far valere i diritti di cui all'articolo 7 del Codice (art. 141, comma 1, lett. c)) e può essere presentato al Garante **solo** quando la risposta del titolare (o del responsabile, se designato) all'istanza con cui si esercita uno o più dei predetti diritti non perviene nei tempi indicati o non è soddisfacente, oppure il decorso dei termini sopraindicati lo esporrebbe ad un pregiudizio imminente ed irreparabile.

Diritti di segreteria

Al ricorso va allegata la prova del versamento dei diritti di segreteria (euro 150,00). Si consiglia di effettuare il versamento sul conto corrente postale n. 96677000 intestato a Garante per la protezione dei dati personali, Piazza di Monte Citorio, n. 121 00186 Roma.

• Il Phishing

Il *phishing* è un tipo di truffa realizzata attraverso Internet. Esso consiste nell'inviare e-mail del tutto simili nell'aspetto grafico a quelle provenienti da banche o siti dove è necessaria una registrazione, come, ad esempio, siti di *e-commerce*.

Nel testo dell'e-mail si invita l'utente, a causa di problemi di registrazione o di altra natura, a validare l'*identificativo utente*, la relativa *password* o altri dati personali, a collegarsi a uno specifico sito web, cliccando su un *link* segnalato sulla pagina stessa. Il collegamento in realtà rimanda ad un sito molto simile all'originale, dove è chiesto di inserire i propri dati (*password, account*), che, in questo modo, saranno carpiti dal truffatore, che poi li riutilizzerà per compiere transazioni od operazioni fraudolente.

Su tale tema, segnaliamo un interessante sito italiano dedicato al fenomeno. Si tratta di Anti-phishing Italia: il portale contro le truffe on-line (http://www.anti-phishing.it/).

Su tale portale possono essere reperiti rilevanti approfondimenti, con possibilità di conoscere i casi di phisping "più alla moda" in un determinato periodo e di avere a disposizioni gli strumenti utili per difendersi da tale truffa.

• Strumenti e contromisure per evitare il phishing.

Per evitare le truffe di phishing, occorre seguire i seguenti consigli:

1. Se sono stati forniti i propri dati personali, cambiare al più presto la password di accesso ai servizi online ed informare immediatamente la propria Banca.
2. Diffidare delle e-mail che chiedono l'inserimento di dati riservati (il nome utente e la password, il codice per le operazioni dispositive, i codici delle carte di pagamento, altre informazioni personali).
3. Verificare con attenzione le e-mail ricevute ad un indirizzo di posta elettronica diverso dalla casella attivata con la registrazione al sito della propria banca.
4. Nel caso in cui un'e-mail contenga richieste "sospette", non rispondere all'e-mail stessa.
5. Non cliccare sui link presenti nelle e-mail "sospette", ma accedere al sito della propria banca digitando manualmente l'indirizzo dello stesso sul browser che si utilizza.
6. Fare attenzione agli elementi sospetti nelle e-mail ricevute. Spesso sono scritte in un italiano maccheronico.
7. Custodire con cura i dati riservati e modificare la password di accesso ai servizi online almeno una volta al mese.
8. Quando si inseriscono dati riservati in una pagina web, assicurarsi che si tratti di una pagina protetta (presenza del lucchetto).
9. Controllare regolarmente gli estratti conto del proprio conto e delle carte di credito per assicurarsi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattare subito la propria banca.
10. Aggiornare costantemente il software dedicato alla sicurezza (antivirus, antispyware, ecc.) ed eventualmente anche il sistema operativo e i programmi per navigare in Internet. Le aziende produttrici dei software rendono periodicamente disponibili online (e scaricabili gratuitamente) aggiornamenti (cosiddette patch) che incrementano la sicurezza del sistema operativo e del browser. Sui siti di queste aziende è anche possibile verificare che il proprio browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.

11. L’utilizzo di una toolbar antiphishing può aiutare a riconoscere i siti potenzialmente pericolosi.

Queste toolbar segnalano il livello di rischio del sito che si sta visitando e, in caso di phishing, sono in grado di bloccare la navigazione (l’utente può, in ogni caso, scegliere di continuare a “navigare”). Alcune toolbar sono disponibili sul web (es.: Microsoft, Netcraft, ecc.) e possono essere installate gratuitamente sul proprio computer.

7 L'importante ruolo della Polizia Postale ed i suoi consigli.

• Il ruolo della Polizia Postale

La nostra Polizia di Stato, sensibile ai mutamenti della società, ha conseguentemente adeguato le proprie strutture investigative alle mutate esigenze strutturando, nel corso degli anni, unità sempre più specializzate nel contrasto ai fenomeni criminali legati all'utilizzo di tecnologie di avanguardia.

La Polizia Postale e delle Comunicazioni, specialità della Polizia di Stato, nata nel 1981 per la tutela del servizio postale e dei servizi di telecomunicazioni, sta vivendo un momento di profonda trasformazione, orientando sempre più la propria attività nel campo delle comunicazioni radio, televisive, telefoniche e telematiche, connotandosi come Polizia delle Telecomunicazioni.

Nel 1996 l'attività di questa equipe di esperti è stata ricondotta al settore più ampio delle attività di contrasto ai crimini commessi nel settore delle telecomunicazioni, prevedendo la nascita del Nucleo Operativo di Polizia delle Telecomunicazioni. La creazione di questo ufficio è stato il preludio di una vasta riorganizzazione di tutta la Specialità, che con decreto del Ministro dell'Interno del 31.03.1998 ha previsto la creazione del Servizio Polizia Postale e delle Comunicazioni con il compito di fornire il coordinamento operativo dei Compartimenti, di garantire la sicurezza delle comunicazioni, di analizzare ed elaborare strategie e di intrattenere rapporti internazionali.

L'articolazione attuale prevede una struttura centrale, costituita appunto dal Servizio Polizia Postale e delle Comunicazioni, incardinato all'interno della Direzione Centrale che sovrintende ai servizi delle singole specialità di Stato, e da unità periferiche (19 Compartimenti e 76 Sezioni presenti nei principali capoluoghi di provincia).

Al Servizio sono state affidate le competenze:

- di prevenzione e repressione dell'hacking e dei reati informatici;
- di studio ed analisi delle fenomenologie connesse ai danni delle rete

di comunicazione, frodi e pedofilia *on line*;
- di elaborazione di strategie e coordinamento investigativo;
- di formazione specialistica del personale;
- di instaurazione di relazioni internazionali finalizzate allo studio dei fenomeni criminali ed alla collaborazione investigativa.

Nell'attività repressiva dei "computers crimes", dunque, la collaborazione dei gestori dei servizi di telecomunicazione, dei servizi internet (*Internet Service Provider*) e degli altri operatori è pertanto un elemento imprescindibile se si vogliono ottenere risultati concreti nelle indagini. Tuttavia, vi è una recente indagine del *Federal Bureau Investigation* (FBI) che rileva che della maggioranza delle agenzie governative statunitensi e delle grandi aziende che hanno subito attacchi da parte di *crackers* davvero poche sono state quelle che hanno denunciato alle autorità competenti.

Perché le Forze di Polizia possano operare bene in questo settore occorre, dunque, una presa di posizione degli operatori di settore e degli utenti della Rete. Infatti, visto che gran parte dei reati informatici sono perseguibili a querela, senza la presenza di denunce le attività investigative di polizia non possono prendere la propria naturale strada, che è quella di "prendere notizia dei reati, impedire che vengano portati a conseguenza ulteriori, ricercarne gli autori ed assicurare le fonti di prova". Se le Istituzioni hanno risposto creando in tutto il mondo delle Forze di Polizia *ad hoc* che cooperano tra di loro (si pensi che la Polizia Delle Comunicazioni partecipa ad esempio con i suoi rappresentanti alle riunioni del G8- Subgroup on Hih. Tech Crime), ciò che occorre in questo momento è sensibilizzare gli utenti e gli operatori del cyber spazio a non sottovalutare l'offensività dei reati informatici.

• Il commissariato on line: www.commissariatodips.it

Un vero e proprio 113 on line, un commissariato di polizia virtuale. Così potremmo definire l'interessante iniziativa della Polizia di Stato con la creazione del sito www.commissariatodips.it, dove il cittadino-navigatore può denunciare o segnalare reati sul web e ricevere consigli ed informazioni.

L'immagine che appare al navigatore che accede al nuovo sito è proprio quella di un commissariato di polizia con diversi uffici: sicurezza telematica, denunce, passaporti, immigrazione, minori, polizia amministrativa e

sociale, concorsi.
Cliccando sulle sezioni, il cittadino può avere informazioni e consigli, ma può anche fare segnalazioni e denunce.

La Federconsumatori di Bologna ritiene molto importante tale iniziativa, in quanto strumento efficace per velocizzare il perseguimento dei reati e sconfiggere anche la burocrazia, i costi pubblici e le lunghe file nei commissariati, che spesso scoraggiano le iniziative di denuncia da parte dei consumatori. Inoltre, la rilevanza del servizio offerto dalla Polizia italiana sta anche nella possibilità per il cittadino di usufruire di utili servizi telematici, come la bacheca degli oggetti rubati, dei documenti smarriti, dei bambini scomparsi.

Un validissimo progetto, dunque, che merita di essere divulgato con particolare attenzione. Un progetto che, proprio per le sue peculiarità, ha fatto vincere all'Italia gli "European eGovernment Awards 2007", assegnati durante la Conferenza interministeriale sull'eGovernment di Lisbona. L'Italia si è aggiudicata, infatti, il primo premio nella categoria "aumentare l'efficienza dei servizi pubblici nazionali e locali e promuovere la partecipazione dei cittadini".
Il progetto della Polizia di Stato è risultato primo tra tutti i 311 presentati dalle pubbliche amministrazioni degli Stati membri dell'Unione Europea, degli Stati candidati e degli Stati dell'Efta
Una perla italiana, dunque, da valorizzare come tale!

• Alcuni consigli della Polizia Postale tratti da:

http://www.poliziadistato.it/articolo/1106-consigli_per_la_navigazione_su_internet
forniamo di seguito alcuni consigli schematici per evitare truffe e frodi informatiche.

- Se possibile, utilizzate per la connessione un computer completamente dedicato a questa funzione, privo quindi di altri dati importanti. Se ciò non è possibile, come abitualmente accade, è necessario configurare con attenzione il proprio computer per evitare di esporlo inutilmente a possibili rischi.
- Se uno dei computer si collega ad internet senza una adeguata protezione, è possibile che la configurazione così impostata permetta anche ad estranei di curiosare nei dati da noi conservati e condivisi.

- Può essere utile un programma firewall: un dispositivo che offre un'adeguata protezione al nostro sistema quando è impegnato da più servizi contemporaneamente, rilevando eventuali accessi abusivi.

Password

La scelta di una password deve essere effettuata con molta accuratezza poiché rappresenta la nostra chiave di accesso e la garanzia per mantenere riservate le informazioni che ci interessano. Questo discorso vale per la scelta della password di accesso al Bios del nostro computer, così come per quella relativa ai servizi di posta o commercio elettronico. A questo proposito, sarà bene tenere presenti alcune avvertenze:

- Evitate di scegliere nomi di congiunti e relative date di nascita, poiché sono abitualmente utilizzate per forzare la protezione da parte di chi vi conosce.
- Utilizzate per le password nomi di fantasia non presenti in dizionari italiani e stranieri, in quanto è possibile utilizzare tali dizionari in forma elettronica per violare un sistema protetto, utilizzando programmi adatti.
- Scegliete una combinazione di caratteri alfanumerici, vale a dire lettere e numeri, che creino una sigla facilmente memorizzabile per l'utente.
- Memorizzare la password, evitando di scriverla, è una garanzia per mantenerne l'integrità.
- Non rivelate le vostre password e comunque cambiatele spesso.

Internet e servizi

La rete internet offre una quantità di servizi utili in continuo e graduale aumento. Per usufruirne con una certa tranquillità vi offriamo una breve guida alle principali funzioni.

Ricezione e-mail

È possibile rifiutare quella indesiderata configurando adeguatamente il servizio di posta elettronica.

Posta elettronica

Scegliete una password seguendo le regole di cui abbiamo già parlato. Ricordatevi di uscire (effettuando il "log out") dal sistema a cui siete collega-

ti. In caso contrario il sistema potrebbe non comprendere che vi siete scollegati (magari spegnendo il nostro PC) e mantenere "appesa" la connessione permettendo a qualcun altro di utilizzare il nostro account.

Social Engineering

Si tratta di una modalità particolarmente amata nel mondo degli hackers che sfruttano l'impreparazione e l'ingenuità degli utenti per ottenere informazioni riservate.
Creando un indirizzo di posta elettronica, scelto in modo tale da trarre in inganno il ricevente, possono inviare delle e-mail che sembrano arrivare dal provider stesso in cui chiedono di modificare la password di accesso in uso e di comunicarla immediatamente tramite posta elettronica. Gli utenti che lo faranno consegneranno la chiave di accesso ai malintenzionati di turno.

Allegati

Possono contenere dei programmi eseguibili pericolosi per il nostro sistema informatico. Quindi cautela se provengono da persone non conosciute. Prima di sfidare la sorte chiedetevi se vale la pena formattare il vostro hard disk (nei casi più gravi può accadere anche questo).

Commercio Elettronico

È sicuramente uno degli aspetti più innovativi offerti da Internet, anche se richiede un pizzico di accortezza non dissimile da quella richiesta nella vita privata. Ad esempio il fatto che il sito sia scritto nella nostra lingua non è sufficiente a ritenere che stia operando dal territorio nazionale.
A questo proposito, può essere utile utilizzare il servizio offerto dal sito www.checkdomain.com che permette di conoscere la nazionalità del sito ed il nome dei suoi responsabili.Queste informazioni devono essere considerate alla luce di alcuni aspetti quali ad esempio la possibilità di esercitare il diritto di recesso.

Carta di credito

Anche su Internet è bene scegliere con cura i siti in cui utilizzarla seguendo alcuni criteri: affidabilità della società e riscontro delle caratteristiche di quanto offerto attraverso la verifica incrociata su altri siti Internet.

Aste Online

Quelle che le propongono sono società che non effettuano quasi mai il controllo dei prodotti offerti dai singoli privati. Possono essere quindi congegnati dei meccanismi per realizzare delle vere e proprie truffe da parte di un malintenzionato che potrebbe non consegnare il prodotto promesso o accordarsi con un complice per far aumentare artificiosamente il prezzo del bene.

Indirizzi Utili

Autorità Garante per la protezione dei dati personali
Piazza Montecitorio 121
00186 – Roma
tel 06/696771 fax 06/69677785
Sito: www.garanteprivacy.it
Mail: garante@garanteprivacy.it

Autorità Garante della Concorrenza e del Mercato
Piazza. G. Verdi 6/A
00198 – Roma
tel 06/858211 fax 06/8582125
sito: www.agcm.it

Corecom Emilia Romagna - Sportello Internet
Viale Aldo Moro 44
40127 Bologna
tel 800 202626 fax 051 5275059

Polizia Postale e delle Telecomunicazioni
Compartimento di Bologna
Via Zanardi 28
40100 – BOLOGNA
tel 051/6352611
Sito nazionale www.poliziadistato.it/pds/informatica/index.htm
Per segnalazioni www.poliziadistato.it/pds/informatica/contatti.html

Grafica: Redesign - Stampa: FD