NAVIGARE IN SICUREZZA SU INTERNET

Centro Europeo Consumatori Italia

ECC-Net

Che cos'è?

Il Centro Europeo Consumatori Italia fa parte della Rete ECC-Net, istituita dalla Commissione Europea in tutti gli Stati membri e cofinanziata dai Governi nazionali con l'incarico di offrire, in modo del tutto gratuito, informazioni, assistenza e consulenza ai cittadini europei per tutto ciò che riguarda il consumo transfrontaliero nel Mercato Unico.

ECC-Net

Centro
Europeo
Consumatori
Italia

Sommario

Introduzione

Al giorno d'oggi Internet è entrata a far parte delle nostre vite, come fosse una di famiglia. Tutti lo conosciamo, almeno per sentito dire, e se anche non lo usiamo spesso o proprio mai, sappiamo che è "quello strumento che ci permette di cercare informazioni, fare acquisti o pagare bollettini". Internet è diventata una presenza costante nelle nostre vite; con l'avvento di smartphone e tablet e la conseguente possibilità di essere sempre connessi ne siamo diventati dipendenti, non ne possiamo più fare a meno.
Il punto è: siamo così sicuri di conoscerlo davvero? Siamo sicuri di poterlo considerare come un caro amico fidato, che mai ci tradirebbe o farebbe un torto?
Internet è uno strumento fantastico, dalle grandi potenzialità, che ha rivoluzionato in meglio le nostre vite, ma non sempre affidarsi ciecamente a lui è da considerarsi una scelta saggia. Anzi, parlando di Internet, si farebbe meglio a tenere sempre a mente il proverbio "fidarsi è bene, ma non fidarsi è meglio". Internet è un mezzo talmente potente, che per essere usato al meglio e in sicurezza, necessita nell'utente la capacità di saperlo ben gestire. È importante mantenere sempre un atteggiamento "sul chi va là", così da sapersi difendere dal suo "lato oscuro", quello che pochi conoscono e di cui molti non si rendono neanche conto, perché ben nascosto o camuffato.

Questa guida vuole essere un aiuto agli utenti per un utilizzo corretto e sicuro di Internet. Si prefigge l'obiettivo di mettere a nudo il "lato oscuro" della rete, i rischi e i pericoli che un uso poco consapevole può generare, al fine di armare l'utente di quelle conoscenze base e astuzie che permettono di navigare in maniera serena. Internet non va demonizzato, ma è importante conoscere i rischi e i pericoli in cui si può incappare, così da saperli riconoscere ed evitare!

Internet: cos'è?

Prima di indagare in profondità nei meandri meno conosciuti e più pericolosi di Internet, è bene fare una breve panoramica su cosa sia e a cosa serva effettivamente questo strumento.

Le origini

Ma che cos'è davvero Internet? Alla parola "Internet" che immagini associamo? È un luogo di incontro, un enorme enciclopedia o un groviglio di cavi e fibre? Ognuno di noi dà a Internet significati diversi e associa immagini differenti, ma Internet, altro non è che una rete di computer (oggi diventata una rete di reti) inventata nel 1969 negli USA. In quell'anno, infatti, venne creata Arpanet, la prima rete di computer del mondo, responsabile per lo sviluppo di nuove tecnologie ad uso militare. In seguito, negli anni Settanta alcuni brillanti ricercatori inventarono l'Internet Protocol Suite (TCP/IP), la struttura su cui ancora oggi poggia Internet. Tale protocollo creava un insieme di regole atte a consentire ai computer di "parlare" tra loro e di scambiarsi informazioni. In pratica è stato creato un linguaggio comune per permettere ai computer di comprendersi e inviarsi informazioni.

Il passaggio da Arpanet ad Internet è avvenuto negli anni Ottanta, quando i militari si sono staccati per ragioni di segretezza e la rete, sotto il controllo delle università, è diventata uno strumento per scambiare conoscenze scientifiche e per comunicare. Da lì a diventare la moderna Internet il passo è stato breve: sempre più computer collegati tra loro hanno permesso a sempre più persone di comunicare, anche per scopi non accademici, fino a che l'avvento dei personal computer ha aperto il mondo della rete anche agli utenti comuni.

Nel 1991 si assiste poi alla nascita del Web, della navigazione Internet come la intendiamo ai giorni nostri. Il World Wide Web, infatti, altro non è che uno spazio elettronico e digitale di Internet destinato alla pubblicazione di contenuti multimediali (testi, immagini, audio, video…). È stato inventato dal CERN di Ginevra, che nel 1993 ha deciso di renderlo pubblico, rinunciando ai diritti d'autore e spalancando così le porte all'avvento dell' era del Web.

Un mondo di opportunità e non solo

Chi avrebbe mai detto che uno strumento nato per condividere informazioni militari e accademiche finisse per cambiare il mondo intero? Eppure è stato così. La rete Internet e soprattutto il Web, permettono oggi di comunicare da un capo all'altro della terra in tempi rapidissimi. Ma non solo, grazie ad Internet è possibile fare tantissime cose, che solo 20 anni fa erano impensabili.

La rete offre un mondo di opportunità: si può comprare, vendere, lavorare, giocare, conoscere nuova gente, scrivere, leggere, documentarsi, annoiarsi, divertirsi…si può fare tutto e il contrario di tutto. Al giorno d'oggi si può letteralmente vivere su Internet, o meglio, vivere davanti ad un computer, senza bisogno di uscire mai di casa. Si può quindi affermare che Internet ha cambiato le nostre vite.

Accanto alle milioni di opportunità però, ci sono anche tante insidie. Si può infettare il computer con dei virus, essere truffati, fare cattive conoscenze... La rete offre tanto, ma è importante saper scegliere bene e distinguere, per non ritrovarsi in spiacevoli situazioni.

I rischi in rete: dai virus al furto d'identità

Come proteggere il PC

Il rischio forse più conosciuto della navigazione online è quello legato alla salute del nostro computer e dei dati in esso contenuti. Esistono, infatti, virus e altri programmi malevoli che possono danneggiare il sistema operativo, impedendo così il corretto funzionamento della macchina o addirittura cancellare documenti dagli archivi.

La prima cosa da fare per proteggere il proprio PC dagli attacchi esterni è capire quali sono e come agiscono i nemici del nostro computer.

Ne esistono davvero tanti, qui di seguito una lista dei più comuni:

- **VIRUS**

  Si tratta di un programma che si autodiffonde nel PC, cioè lo infetta autonomamente o sfruttando la vulnerabilità di altri programmi (ad esempio i software di posta elettronica) o dei sistemi operativi (ad esempio autorun dei dispositivi rimovibili come le chiavi usb). È un programma come quelli che si installano normalmente sul PC per scrivere o ascoltare musica, la differenza è che l'installazione dei virus avviene senza che il proprietario del PC se ne accorga, perché il virus sfrutta le falle di sicurezza del sistema, la vulnerabilità di altri programmi e anche la disattenzione dell'utente.

- **MALWARE**

  È un programma informatico creato con il solo scopo di causare danni più o meno gravi al computer o al sistema informatico sul quale viene eseguito. Il termine deriva dalla contrazione delle parole inglese malicious e software, e ha dunque il significato letterale di programma malvagio.

- **WORM**

  È un malware che modifica e che infetta il computer, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo fino a che il computer non viene spento. Si tratta di un auto-replicante che, a differenza dei virus, non ha bisogno di programmi o file per diffondersi né per attivarsi, perché sfrutta semplicemente le debolezze del sistema operativo ospite. I worm si insidiano nella memoria del PC e prendono il controllo delle funzioni dedicate al trasporto di file o informazioni. Tendono ad utilizzare le parti del sistema operativo automatiche e di solito invisibili all'utente. È comune, infatti, accorgersi di essere stati contagiati da un worm solo quando la sua replica incontrollata provoca un vistoso rallentamento del sistema, se non il suo crash. Il maggior pericolo dei worm è proprio la loro capacità di riprodursi in automatico. Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il worm, infatti, ricerca gli indirizzi email memorizzati nel computer ospite, ed invia una copia di se stesso come file allegato a tutti o parte degli indirizzi che è riuscito a raccogliere.

- **TROJAN HORSE (cavallo di Troia)**

Si tratta di un programma informatico apparentemente normale che, tuttavia, contiene al suo interno un malware, proprio come il cavallo di Troia conteneva al suo interno Ulisse e i suoi uomini. La sua particolarità è che non si diffonde da solo come worm, ma è il proprietario stesso del PC che, installando il programma, inconsapevolmente installa anche il trojan nascosto. Il trojan è composto quasi sempre da due elementi principali: la parte server e la parte client.

- **SPYWARE E ADWARE**

Sono programmi informatici che vengono usati per raccogliere informazioni dal sistema sul quale sono installati e trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche dell'utente. Tutti i programmi gratis che si caricano dalla rete, vivono alle spalle di programmi spyware o adware inconsapevolmente installati dagli utenti. È bene precisare che non si tratta di trojan horses, in quanto non è presente un codice malevolo, bensì un codice che comunque svolge attività di acquisizione dati e invio (spyware) o semplicemente di pubblicità mediante apertura di pagine Web. A volte alcuni di questi software deviano l'utente che sta navigando su siti apparentemente simili ad altri, in modo tale che, ad esempio, l'utente creda di trovarsi sulla home page normalmente impostata, trovandosi invece su una pagina che in realtà appartiene a terzi interessati ad acquisirne i dati.

- **DIALER**

Si tratta di programmi informatici che si occupano di gestire la connessione ad Internet tramite la normale linea telefonica, in modo illecito, modificando il numero chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente. Non funzionano nel caso di connessioni Internet a banda larga.

- **SCAREWARE**

Sono programmi che ingannano l'utente facendogli credere che il proprio PC sia infetto, al solo scopo di fargli installare particolari malware, i quali a loro volta si spacciano per antivirus veri e propri, talora anche a pagamento.

- **HIJACKER**

Questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine Web indesiderate.

- **ROOTKIT**

I rootkit sono di solito composti da un driver e, a volte, da delle copie modificate di programmi normalmente presenti sul sistema. I rootkit non sono dannosi in sé ma hanno la funzione di nascondere, sia all'utente che a programmi antivirus, la presenza di particolari file o impostazioni del sistema. Servono sovente per mascherare spyware e trojan.

- **RABBIT**

Sono programmi che esauriscono le risorse del computer autoriproducendosi a grandissima velocità.

C'è quindi una grande varietà di modi per danneggiare un computer, e i pirati informatici ne inventano di nuovi ogni giorno. È quindi necessario tutelarsi il più possibile, per evitare seri danni alle parti vitali del PC o problemi ancora più gravi nel caso di furto di dati sensibili.
Spesso non ce ne rendiamo conto, ma non proteggere un computer dagli attacchi informatici è come andare in automobile pur sapendo di avere le gomme sgonfie, i freni usurati e i fari rotti: è un modo per sfidare la sorte sperando che non ci accada niente di brutto, ed è quindi da evitare.
Benché i PC più avanzati utilizzino sistemi operativi in grado di limitare gli attacchi e le minacce, è comunque necessario che l'utente prenda degli accorgimenti essenziali per proteggersi, perché molte impostazioni dei PC devono comunque essere attivate dall'utente stesso. I computer rimangono sempre macchine che funzionano tramite l'input dell'uomo, è bene ricordarlo.
Per essere il più protetti possibile è importante prendere questi accorgimenti:

- installare un software antivirus. Ce ne sono moltissimi scaricabili dalla rete, sia gratis che a pagamento. Una volta installato è bene aggiornarlo ogniqualvolta il programma lo richieda, perché, come detto, nascono virus nuovi ogni giorno;
- utilizzare il firewall: può essere un apparato, quindi un hardware, o un firewall personale, cioè un programma installato sul PC. Alcuni sistemi operativi lo incorporano e lo abilitano in origine. Si tratta di un filtro che controlla le comunicazioni in entrata e in uscita dal PC, permettendo o vietando determinati tipi di comunicazione in base alle regole di sicurezza impostate dall'utente;
- utilizzare un browser aggiornato: permette di limitare gli attacchi durante la navigazione sul Web;
- fare attenzione a ciò che si installa: se il PC segnala contenuti non attendibili è bene uscire dalla pagina che si sta visitando e cercare pagine alternative. In particolare, è bene stare alla larga da siti che propongano in vendita programmi a pagamento con queste caratteristiche:
  - Nome del prodotto troppo generico
  - Grafica troppo generica
  - Promesse esagerate
  - Scarsa informazione sull'autore
  - Mancanza di forum o community in cui si parla del prodotto o testimonianze troppe vaghe di utenti soddisfatti.
- È preferibile connettersi alla rete con un router, invece che con un modem, perché se è di buon livello, riesce a sopportare i possibili attacchi e a proteggere il PC.

In generale è sempre consigliabile navigare e soprattutto scaricare programmi e file da siti rinomati e conosciuti, e diffidare sempre di quei siti che propongono ciò che nessun altro propone, perché spesso si tratta di specchietti per le allodole che possono comportare non pochi rischi.

Il furto d'identità: cos'è e come evitarlo

Il furto di dati personali e sensibili a scopo di frode è un crimine vecchio quanto il mondo. Esiste da sempre, e numerosissimi sono i casi che riempiono le cronache e le pagine di ogni epoca.
L'avvento del Web tuttavia ha riportato in auge il problema, poiché la rete consente nuove opportunità di truffa ai moderni criminali, che si sono rapidamente adattati alle nuove tecnologie trovando diversi sistemi per carpire preziose informazioni e raggiungere i propri scopi illeciti. Con l'evoluzione digitale, infatti, si sta assistendo ad una crescita smisurata del fenomeno del furto d'identità, inteso come appropriazione indebita di informazioni personali di un soggetto con lo scopo di commettere in suo nome atti illeciti a fini di guadagno personale.
L'apertura alla rete, l'uso massiccio della posta elettronica, la diffusione delle transazioni telematiche e l'utilizzo crescente di social network e chat al fine di condividere informazioni, contenuti ed esperienze, ha, infatti, favorito e incrementato la circolazione di dati personali, rendendo i navigatori sempre più vulnerabili rispetto alla possibilità di essere vittime di questo pericolo, con conseguenti gravi danni economici e sociali.
In assenza di una precisa definizione normativa, per furto d'identità, si può intendere ogni azione intrapresa al fine di ottenere in modo fraudolento un'informazione individuale, relativa sia a persone fisiche che ad aziende, con l'intento di utilizzare identità o dati personali altrui per scopi illeciti.

Come avviene

Negli ultimi anni abbiamo assistito ad un cambiamento di abitudini e stili di vita che hanno sicuramente contribuito al moltiplicarsi delle occasioni in cui è possibile raccogliere, immagazzinare, processare, aggregare, collegare, analizzare e trasferire vaste quantità di dati. Internet, è ovviamente il canale per eccellenza in cui è più facile per i malintenzionati carpire i dati sensibili di utenti poco cauti.

Ad ogni modo, è bene spezzare una lancia a favore di Internet, perché non è solo lui la causa dei furti d'identità. Anche i comportamenti sbagliati perpetrati al di fuori della rete concorrono a facilitare il lavoro dei criminali: una bolletta del gas gettata nell'immondizia, per esempio, può essere trovata da un malintenzionato che utilizzerà le informazioni su di essa per compiere illeciti.

Nel mondo virtuale invece, la tecnica più comune con la quale avviene il furto d'identità è il cosiddetto phishing: il nome è una storpiatura della parola inglese che significa pescare, infatti usa spesso finte email come una vera e propria esca. Si avvale di un messaggio e-mail dall'aspetto ufficiale, in apparenza proveniente da un istituto di credito o da una società che fornisce servizi a mezzo Internet. Nel testo del messaggio i truffatori presentano improcrastinabili esigenze di sicurezza che si traducono nell'invito a modificare i codici di accesso personali ai conti online, cliccando su di un link. Accedendo a tale link, l'utente vedrà configurarsi davanti a sé una pagina Web uguale a quella del proprio istituto di credito. Il correntista in buona fede inserisce i propri dati d'accesso e i phisher portano a segno il colpo perché "rubano l'identità digitale" del malcapitato utilizzando i dati inseriti in questo sito fittizio per prelevare denaro dai conti correnti della vittima, fare acquisti o transazioni a suo nome.
È importante saper riconoscere i casi di phishing. Tali messaggi sovente:

- non sono personalizzati;
- utilizzano un tono intimidatorio;

- chiedono di inserire le proprie credenziali in un sito Web (falso) del quale inseriscono il link;
- presentano errori di ortografia.

È importantissimo ricordare che né banche, né la posta né altri istituti affini richiedono MAI l'invio di informazioni sui dati personali tramite email. Diffidate sempre, e in caso di dubbi, è opportuno verificare con la propria banca o l'organismo in oggetto che il messaggio sia autentico.

Altre tecniche che si accompagnano al phishing per il furto di identità sono:

- **Vishing**, è l' ultima evoluzione del phishing legato all'utilizzo del Voip, ovvero le telefonate via Internet. Può succedere che il cyber criminale si spacci per una banca, facendo addirittura comparire il vero numero dell'istituto di credito sul display dell'utente, spingendo, l'utente a comunicare i propri dati di accesso per risolvere fantomatici problemi o rendere di nuovo sicuro il proprio account.

- **Pharming** è una tecnica ancora più occulta del phishing. La truffa consiste nel realizzare pagine Web identiche ai siti già esistenti (banche, assicurazioni...) in modo che l'utente sia convinto di trovarsi, ad esempio, nel sito della propria banca e sia indotto a compiere le normali transazioni sul proprio conto on-line. Una volta digitate le credenziali (password e user ID) del proprio conto, sarà semplice recuperarle, tramite keylogger o trojan, per utilizzarle a fini fraudolenti.

Come prevenire il furto d'identità

La prima regola fondamentale da seguire per prevenire al meglio i furti d'identità è la seguente: non sottovalutare la furbizia dei "ladri" d'identità. Questa nuova tipologia di criminali ha trovato nel Web una fonte inesauribile di possibili "prede" oltre ad una serie di strumenti tecnologici sempre più efficaci per portare a termine il proprio scopo. Se nel mondo reale possiamo riuscire a comprendere se qualcuno ci sta truffando, in quello virtuale è molto più difficile. Le nostre credenziali potrebbero già essere a disposizione di malintenzionati senza che noi ne sappiamo nulla.

La protezione dell'identità è direttamente collegata con quella del computer: antivirus, firewall, antispamming, antiphishing, certificati digitali sono alcuni tra i metodi oggi sempre più utilizzati per prevenire questo tipo di frodi.

Quando riceviamo un'e-mail e non sappiamo da chi ci proviene non dovremmo neppure aprirla soprattutto quando ci accorgiamo che è scritta in un pessimo italiano. E' buona norma, dunque, cancellare immediatamente, anche dal cestino , qualunque tipo di e-mail proveniente da sconosciuti perché può dar luogo a uno scambio di informazioni tra il nostro computer e quello di chi ci ha inviato l'amo per farci abboccare.

Non riutilizzare mai la password di account importanti (come quella del conto bancario on line) per e-mail, siti di social network e siti commerciali e cambiare la password periodicamente soprattutto quando si sospetta che uno degli account sia a rischio. Non memorizzare alcun PIN, alcuna password, alcun "nome utente" o altri parametri per l'accesso ai servizi delle banche (online o stradali, come i Bancomat, che siano) all'interno dei propri cellulari. Non annotare password in nessun luogo, né cartaceo né elettronico, ma cercare di imparle bene a memoria.

Non limitarsi inoltre, quando si cambia password, a modificare solo un paio di lettere o numeri della combinazione precedente ma crearne una nuova ogni volta e non utilizzare mai password intuibili come nomi dei figli,

proprio nome, data di nascita propria o dei propri famigliari; queste sono facilmente individuabili, a scapito della privacy e della sicurezza nelle comunicazioni via e-mail. Ed ancora non utilizzare mai computer pubblici (di biblioteche, Internet point, Internet café, etc.) per controllare la vostra e-mail o i vostri conti bancari on line o per effettuare transazioni finanziarie. Infatti, non è possibile sapere se su un computer pubblico siano state installate le patch di protezione appropriate o se il computer sia già affetto da un virus. Anche se il computer è aggiornato, le informazioni immesse potrebbero restare memorizzate sul computer e un altro utente potrebbe accedervi successivamente. Può essere rischioso. È bene cercare di mantenere la propria e-mail confidenziale e privata e non usarla per iscriversi a forum, siti Web sconosciuti o social network.

Cosa fare se si sospetta di un furto di identità ?

1. Innanzitutto bloccare le carte di credito e tutti i conti correnti interessati La prudenza non è mai troppa: è preferibile congelare o cambiare subito i conti evitando di perdere tempo in seguito per contestare acquisti effettuati in modo illecito dal criminale informatico.
2. Contattare il dipartimento di sicurezza o antifrode delle banche o degli istituti finanziari con i quali intercorrono rapporti, comprese le società di emissione di carte di credito, le aziende di servizi pubblici, i provider di servizi Internet e tutti i luoghi in cui la carta di credito viene utilizzata regolarmente, per segnalare eventuali accessi o usi fraudolenti del proprio conto.
3. Dare seguito alla telefonata con una lettera raccomandata con ricevuta di ritorno.
4. Modificare le password di tutti i conti on-line.
5. Se avete il sospetto che la vostra posta sia stata rubata o che sia stata inoltrata una richiesta di variazione di indirizzo a vostro nome, contattate subito le Poste Italiane;

... e quando si diventa una vittima

- Immediatamente dopo aver subito un furto o uno scippo, denunciate l'accaduto al Pronto Intervento (112 per i Carabinieri, 113 per la Polizia di Stato). Recatevi poi negli uffici dell'Autorità di Polizia Giudiziaria e presentate la denuncia, fornendo gli estremi dei documenti che vi sono stati sottratti; se sospettate che qualcuno abbia usato il vostro nome o altre informazioni per effettuare un acquisto a credito o richiedere un prestito contattate la vostra banca per segnalare l'accaduto e valutate se è necessario bloccare tutte le carte di credito;
- Presentate una denuncia agli organi competenti. Idealmente la denuncia dovrebbe essere fatta nel luogo dove il crimine si è verificato. Anche se non si è in grado di fornire alla polizia informazioni sufficienti per la cattura del criminale, puoi utilizzare una copia o il numero della denuncia per i creditori nel caso venga richiesta una prova. È possibile che non ce ne sia mai bisogno ma potrebbe anche fare la differenza.
- Se sono stati rubati il numero della patente di guida o il codice fiscale sarà necessario contattare, rispettivamente, l'ufficio della Motorizzazione e l'Agenzia delle Entrate. È comunque consigliabile denunciare il furto anche alla propria assicurazione e a qualsiasi organizzazione professionale di settore.
- Contattate il creditore, la banca, la compagnia telefonica e l'azienda di servizi pubblici e congelate immediatamente i relativi conti.
- Rivolgetevi alle associazioni dei consumatori per ottenere consigli e consulenza su come agire per risolvere il problema, per verificare la propria situazione ed eventualmente per riconfermare la propria affidabilità creditizia. Le associazioni dei consumatori potranno fornire informazioni, suggerimenti e offrire tutela legale.

Il mondo degli acquisti online

Una delle grandi opportunità offerte da Internet è la possibilità di fare acquisti comodamente dalla poltrona di casa. Questo però non significa essere esenti da rischi o truffe, anzi, nell'e-commerce è bene fare molta più attenzione che negli acquisti "normali", perché in rete "non è tutto oro quello che luccica".

L'e-commerce

Il commercio elettronico, o e-commerce, consiste nell'acquisto di beni o servizi tramite Internet, senza quindi la presenza simultanea di professionista e consumatore.
Invece di passeggiare tra le vetrine dei negozi, si scorrono innumerevoli siti online e una volta scelto il prodotto o servizio desiderato si compila l'ordine e, cliccando sul tasto di conferma, si invia la propria richiesta di acquisto.
Le modalità di pagamento sono svariate e dipendono da ciò che offre il professionista, sovente però la più semplice e immediata è il pagamento tramite carta di credito/debito o tramite Paypal.

Cos'è Paypal?

È una società che offre servizi di pagamento online e permette di effettuare transazioni senza condividere i dati della carta di credito con il destinatario finale del pagamento. Registrandosi gratuitamente sul sito della società è possibile aprire il proprio conto per effettuare i pagamenti. Al conto si può associare una carta di credito o prepagata o caricarlo tramite bonifico. L'invio di denaro è gratuito mentre la ricezione è soggetta a tariffe.

L'e-commerce si configura come "contratto di acquisto a distanza" ed è regolamentato dal D.Lgs 206/2005 (Codice del Consumo) dagli articoli 45 e seguenti.
Trattandosi di una modalità d' acquisto a distanza, l'informativa che dev'essere fornita al consumatore prima dell'acquisto è regolamentata per legge e deve includere:

- identità del professionista e, in caso di contratti che prevedono il pagamento anticipato, l'indirizzo del professionista;
- caratteristiche essenziali del bene o del servizio;
- prezzo del bene o del servizio, comprese tutte le tasse e le imposte;
  spese di consegna;
- modalità del pagamento, della consegna del bene o della prestazione del servizio e di ogni altra forma di esecuzione del contratto;
- esistenza del diritto di recesso o di esclusione dello stesso;
- modalità e tempi di restituzione o di ritiro del bene in caso di esercizio del diritto di recesso;

- costo dell'utilizzo della tecnica di comunicazione a distanza;
- durata della validità dell'offerta e del prezzo;
- durata minima del contratto in caso di contratti per la fornitura di prodotti o la prestazione di servizi ad esecuzione continuata o periodica;
- informazione sulle condizioni e sulle modalità di esercizio del diritto di recesso;
- indirizzo geografico della sede del professionista a cui il consumatore può presentare reclami;
- informazioni sui servizi di assistenza e sulle garanzie commerciali esistenti;
- condizioni di recesso dal contratto in caso di durata indeterminata o superiore ad un anno.

L'accesso a tutte queste informazioni non solo vi permetterà di effettuare un acquisto in modo consapevole, ma vi aiuterà anche a valutare l'affidabilità del venditore e a proteggere i vostri soldi evitando le truffe.

Buone regole per acquistare online in sicurezza

" Non è tutto oro quello che luccica". Alla vastità di scelta che offre Internet corrispondono anche grandi possibilità di cadere vittime di truffe. Su Internet si può comprare di tutto e a qualunque prezzo, è bene però ricordare che le cose "troppo belle per essere vere" di solito non lo sono: diffidare sempre di siti che propongono la vendita di oggetti di marca a prezzi stracciati, perché spesso si tratta di truffe.
Qui di seguito alcuni consigli per acquistare online in sicurezza:

- prima di acquistare un bene o un servizio verificare sempre le politiche di vendita, le condizioni di recesso, i tempi di consegna e i costi di spedizione;
- verificare che sul sito siano presenti tutti i dati relativi al venditore. Devono essere indicati chiaramente il nome e l'indirizzo dell'azienda. Il sito rappresenta la "faccia" del venditore, quindi è come se avessimo di fronte una persona e le si potessero fare domande e ricevere risposte: verifichiamo che il sito risponda a tutte le nostre domande;
- verificare l'esistenza della certificazione, cioè di un attestato che comprovi la corrispondenza tra un dato sito e una persona fisica o giuridica. È possibile fare questa verifica aprendo la voce "visione certificati" nella finestra del browser;
- è preferibile scegliere siti con l'indicazione di un marchio di qualità rilasciato da un ente esterno che certifica che il sito svolga la sua attività nel rispetto dei diritti dei consumatori. I marchi più diffusi in Italia oggigiorno sono: Webtrader, E-quality mark e QWeb;
- evitare un utilizzo improprio delle carte di credito in rete: verificare che al momento del pagamento il sito presenti un sistema di protezione della trasmissione dei dati SSL (socket secure lock). Lo si può capire verificando la presenza di un lucchetto chiuso sulla parte bassa dello schermo (se è aperto vuol dire che la transazione non è sicura.) Assicurarsi inoltre che le informazioni relative alla carta siano criptate in maniera sicura prima di essere inviate, controllando che l'indirizzo del sito inizi con https:// anziché con http://;
- prestare attenzione alla normativa sulla privacy: i dati richiesti dovrebbero essere unicamente quelli finalizzati a consentire l'acquisto;
- evitare, se possibile, mezzi di pagamento che non permettano di essere bloccati e/o contestati (bonifico o money transfer);
- conservare con cura una copia degli ordini fatti e di tutte le comunicazioni intercorse.

Internet e minori

Quali rischi

Negli ultimi anni è cresciuta in maniera esponenziale l'utenza domestica della rete ed è aumentato con essa il numero di bambini e ragazzi che utilizzano Internet. Questo aumento ha sollevato la lecita domanda: Internet è a misura di bambino?

Il computer non può essere considerato come un mezzo di intrattenimento passivo, alla stregua della televisione, perché non lo è, soprattutto quando ha un collegamento ad Internet.
Il Web è un eccezionale strumento che può essere usato da bambini e ragazzi ai fini di studio e di divertimento, ma è importante essere consapevoli che il "lato oscuro" del Web può avere effetti particolarmente deleteri sui minori. Non si può ignorare che i nostri figli possano facilmente imbattersi in contenuti inappropriati, quali ad esempio siti pornografici, pedopornografici, siti con contenuti violenti e in grado di suscitare paura nei bambini…

I minori nel mondo virtuale di Internet coltivano amicizie, grazie soprattutto all'utilizzo dei social network (Facebook, Twitter, MySpace…), perché il fatto di non vedersi o sentirsi direttamente diminuisce la timidezza e riduce le inibizioni. Questa è una delle belle possibilità offerte dal Web, che però può anche nascondere risvolti negativi, perché coloro che conosciamo in rete, nella realtà possono essere persone totalmente differenti. È bene, infatti, che i minori siano accompagnati nell'uso di tali strumenti, per ridurre al minimo il rischio di entrare in contatto con malintenzionati. Bisogna scegliere con accortezza le informazioni personali da condividere e stare in guardia dalle relazioni con i cosiddetti falsi profili, ovvero persone che dichiarano età, sesso e identità diversi dalla realtà; è fondamentale sapere sempre con chi ci si sta relazionando!

Nel mondo delle relazioni virtuali, i rischi maggiori per i minori sono:

- **sexting:** crasi delle parole inglesi sex e texting, è un termine usato per indicare l'invio di immagini sessualmente esplicite o di testi sul sesso;
- **cyberbullismo:** indica atti di bullismo e di molestia effettuati tramite mezzi elettronici (email, blog, siti Web…). A differenza del bullismo, quello cibernetico è ancora più subdolo, perché spesso l'identità del molestatore è nascosta. Alcuni esempi di cyberbullismo sono il flaming (invio di messaggi violenti o volgari) e il cyberstalking (forme di molestie reiterate che utilizzano il web e le tecnologie delle comunicazione);
- **adescamento online (grooming):** Si tratta di una tecnica usata dai pedofili per avvicinare i minori attraverso mezzi elettronici, con dialoghi in chat o forum, tramite social... I pedofili costruiscono un legame di fiducia con la vittima che viene indotta a dare informazioni personali e a volte ad accettare un incontro. L'adescamento online è molto insidioso, perché può durare anche a lungo e, sebbene non implichi necessariamente un contatto fisico, può indurre il minore a considerare come normali atti sessuali tra adulti e bambini.

Come difendersi

Nel caso dei minori, gli accorgimenti tecnologici da soli non sono sufficienti a difendersi dai pericoli. A volte, infatti, non sono vittime passive, ma i primi a fare un uso inadeguato di Internet. È quindi fondamentale e indispensabile il ruolo educativo della famiglia, che è tenuta ad intervenire nella sfera affettiva del minore. In particolar modo è bene far capire al minore quanto è importante la privacy nella nostra società e in particolare nella navigazione in rete, perché le informazioni personali messe online diventano pubbliche e come tali possono essere utilizzate per scopi illeciti.

Per assistere i minori nella navigazione in rete è bene ricordar loro alcune semplici regole:

- non fornire mai agli estranei informazioni quali nome, cognome, indirizzo di casa o scuola;
- non inviare mai foto o video tramite posta elettronica;
- non utilizzare la chat come unica alternativa alle conversazioni dal vivo;
- non fissare mai incontri con persone conosciute online;
- segnalare ai genitori i siti che arrecano disagio o paura, nonché ogni richiesta di incontro o invio di foto o video;
- non fornire il proprio numero di telefono a sconosciuti;
- non pubblicare mai foto provocanti, che potrebbero attirare malintenzionati;
- ricordarsi sempre di non girare, commentare, linkare messaggi che possono essere offensivi o causare dispiacere ad altri.

Aldilà dell'educazione che ogni genitore deve dare al proprio figlio, prima di mettere a disposizione dei bambini un computer, è molto importante adottare tutte le precauzioni necessarie affinché gli stessi siano tutelati e usare ciò che la tecnologia ci fornisce per farlo.
Ad esempio è possibile personalizzare i settaggi dei browser con i quali il bambino effettua l'accesso ad Internet. La maggior parte dei browser conosciuti consente, infatti, di limitare l'accesso a determinati siti, oltre che di controllare i contenuti che vengono visualizzati.
Anche un corretto utilizzo del router può essere di aiuto alla sicurezza dei minori in rete; quelli attualmente in commercio, infatti, dispongono di settaggi di blocco dei domini. È possibile impostare il router inserendo nei settaggi, tra i siti bloccati, l'indirizzo (url) del sito rispetto al quale si vuole vietare l'accesso. Così facendo si impedisce l'accesso a tali siti non solo dal singolo PC, ma da tutti gli apparati presenti all'interno dell'abitazione (per esempio i cellulari che si collegano tramite wi-fi alla rete di casa).
Qualora si fosse comunque vittime di comportamenti illeciti o si incappasse in materiale illegale, è bene contattare immediatamente la Polizia delle Comunicazioni per segnalare la fonte
(www.commissariatodips.it).

Il problema della navigazione sicura in rete per i bambini è un tema su cui ha lavorato anche l'Unione Europea istituendo il Programma Internet Sicuro
(http://ec.europa.eu/information_society/activities/sip/index_en.htm) .

Tale programma, volto a migliorare la sicurezza dei minori nell'ambiente in linea, verte su due obiettivi:

- approfondire la conoscenza delle modalità adottate dai minori per utilizzare le nuove tecnologie;
- identificare e lottare contro i rischi a cui essi sono esposti.

Il programma sarà attuato seguendo le quattro linee d'azione seguenti:

- **Sensibilizzazione del pubblico**. Le azioni di sensibilizzazione si rivolgono soprattutto ai bambini, ai loro genitori ed agli educatori. Hanno lo scopo di informare adeguatamente il maggior numero possibile di utenti in merito ai rischi ed ai metodi di prevenzione. ;

- **Lotta contro i contenuti illeciti ed i comportamenti dannosi**. Si tratta di azioni destinate a ridurre il volume dei contenuti illeciti online ed a combattere la distribuzione di materiale pedopornografico, le pratiche di cyberbullismo e di grooming. Il programma mette a disposizione del pubblico alcuni punti di contatto accessibili a livello europeo per segnalare efficacemente tali abusi. Inoltre promuove la cooperazione sul piano nazionale, comunitario ed internazionale, incoraggiando le parti interessate a condividere informazioni e migliori prassi;

- **Promozione di un ambiente online più sicuro**. Queste attività sono intese ad incoraggiare l'attuazione di iniziative di autoregolamentazione tra le parti interessate.

- **Creazione di una base di conoscenze**. In questa base verranno inseriti gli usi esistenti ed emergenti dell'ambiente in linea da parte dei minori, come pure i rischi e le conseguenze inerenti a tali usi.

Il Programma sponsorizza anche i due eventi annuali dedicati al tema: Safer Internet Day e Safer Internet Forum.

Centro Europeo Consumatori Italia

ECC-Net

Come contattarci

Il Centro **ECC-Net**, in Italia, è, dal 2005, gestito da **Adiconsum** – sede centrale – insieme al **CTCU di Bolzano** – sede transfrontaliera –, e assiste sia i consumatori italiani che abbiano acquistato beni e servizi da imprese e professionisti di un altro Stato membro dell'Ue che i consumatori degli altri Stati membri Ue che abbiano invece acquistato beni e servizi da imprese e professionisti italiani.

È possibile contattare il Centro Europeo Consumatori per richiedere tutte le **informazioni** sui propri **diritti di consumatore europeo**, e per ricevere **consulenza e assistenza gratuita** sia in fase di presentazione dei reclami che di gestione delle controversie, nel caso in cui il reclamo già presentato non abbia avuto risposta o la risposta sia stata non soddisfacente.

Per maggiori informazioni: **http://www.ecc-netitalia.it**

Sede centrale

Viale Degli Ammiragli, 91
00136 Roma

Tel. +39 06 44238090
Fax. +39 06 44170285
info@ecc-netitalia.it

Sede transfrontaliera di Bolzano

Via Brennero, 3
39100 Bolzano

Tel. +39 0471 980939
Fax +39 0471 980239
info@euroconsumatori.org

Progetto gestito da:

ADICONSUM
Associazione Difesa Consumatori e Ambiente promossa dalla CISL

Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti

cofinanziato da:

Ministero dello Sviluppo Economico

AUTONOME PROVINZ BOZEN SÜDTIROL
PROVINCIA AUTONOMA DI BOLZANO ALTO ADIGE
PROVINZIA AUTONOMA DE BULSAN SÜDTIROL

European Commission

Centro Europeo Consumatori Italia
ECC-Net