Test Noi Consumatori - Periodico settimanale di informazione e studi su consumi, servizi, ambiente. Anno XXIX - numero 3 del 5 Gennaio 2017
Direttore: Walter Meazza - Direttore responsabile: Ester Crea - Amministrazione: Adiconsum, Largo Alessandro Vessella n. 31, 00199 Roma
Reg. Trib. Roma n. 350 del 09/06/88 - Iscriz. ROC n. 1887. Questo periodico è associato all'Unione Stampa Periodica Italiana

Spesa finanziata dal Ministero dello Sviluppo Economico ai sensi del Decreto 6 Agosto 2015

ADICONSUM
Associazione Difesa Consumatori e Ambiente promossa dalla CISL

no problem
servizi ai consumatori

NAVIGARE NELLA RETE SENZA AFFONDARE

Consigli pratici per una corretta connessione ad internet

GUIDA ADICONSUM: NO PROBLEM
Il diritto a conoscere i tuoi diritti

Questa Guida nasce nell'ambito del progetto *"No problem - Assistenza, informazione, incontri con le Associazioni dei consumatori"*, finanziato dal Ministero dello Sviluppo Economico e realizzato in collaborazione dalle Associazioni dei Consumatori Adiconsum, Unione Nazionale Consumatori, Centro Tutela Consumatori e Utenti e U.Di.Con., con l'obiettivo di rafforzare la relazione tra i consumatori e le associazioni di tutela e rafforzare il ruolo stesso del consumatore, rendendolo così protagonista attivo attraverso la maggiore consapevolezza e conoscenza dei propri diritti.

Al lettore intendiamo offrire un breve ma essenziale percorso di conoscenza ed orientamento all'esercizio dei diritti che la normativa nazionale e comunitaria hanno sancito per lui, nei confronti dei fornitori di beni e servizi operanti sul mercato unico, inclusi i servizi pubblici.

Senza la pretesa di fornire informazioni esaustive, per ciascun diritto o procedura diamo informazioni di base e indicazioni pratiche di comportamento, in modo che il consumatore possa agevolmente comprendere la situazione in cui si trova ed attivarsi in modo efficace per ottenere assistenza, se necessario, o interloquire correttamente con la controparte in modo autonomo.

L'obiettivo primario di questa pubblicazione è quello di fornire informazioni utili su come navigare in internet in maniera consapevole e sicura, proteggendo i propri dati e difendendo i propri diritti.

Per informazioni più dettagliate e per accedere a risorse utili come fac-simile di lettere di reclamo, guide specifiche, link ai servizi istituzionali ecc., vi rimandiamo al sito internet dell'Associazione www.adiconsum.it, che ospita una sezione informativa sul progetto e le sue attività, oltre a numerose sezioni tematiche.

Buona lettura!

NAVIGARE NELLA RETE SENZA AFFONDARE
Consigli pratici per una corretta connessione ad internet

INDICE:

INTERNET

Internet è la sintesi di “INTERconnection of NET”, una comunità di utenti che sono interconnessi tramite i loro apparati, superando i confini tradizionali. È una fitta rete di calcolatori (pc, tablet, smartphone) e altre macchine (qualsiasi oggetto connesso alla rete) che parlano il medesimo linguaggio di comunicazione. I device collegati ad Internet possono comunicare con qualsiasi altro device, indipendentemente dal tipo di macchina e dal sistema operativo che utilizzano. Questo è possibile mediante un protocollo di comunicazione TCP/IP. Oggi si stimano almeno 3 miliardi e mezzo di persone collegate! E questo numero tenderà ancora a crescere. Una volta collegati si comincia a navigare e si può accedere ad una serie di servizi che la rete mette a disposizione come file testo, immagini, suoni, filmati, posta elettronica, Messaggeria, News, ecc...

Internet è la modalità che gli umani (e anche le cose) hanno per connettersi fra loro. Un sistema primario di comunicazione mondiale che si estende a tutta la popolazione terrestre. Uno strumento che allarga le nostre conoscenze e il nostro sapere. Un potente strumento di creazioni e/o erogazione servizi.

Per usare internet è necessario disporre di una connessione altamente veloce (ultra banda larga) per collegare gli apparati nella rete; dei protocolli che unificano i criteri e stabiliscono una certa omogeneità nella trasmissione dei dati pur utilizzando macchine differenti; degli indirizzi IP, che permettono di identificare ogni singola macchina connessa alla rete (un po’ come gli indirizzi postali identificano ogni singola cassetta postale).

In questa guida vorremo dare alcune indicazioni su come navigare nella rete in sicurezza, difendendo la nostra identità senza subire intromissioni non volute e senza rischiare di affondare.

NAVIGARE SENZA AFFONDARE

Aggirandosi per la rete dobbiamo sempre prestare molta attenzione a proteggere le informazioni che ci riguardano. Siamo noi, infatti, che dobbiamo decidere in che modo vogliamo "farci conoscere". Il diritto alla privacy, ritenuta come la "sovranità su se stessi", nasce proprio dalla necessità di garantirci di non subire intrusioni indesiderate nella nostra sfera privata che potrebbero farci *affondare* definitivamente.
Nella vita reale, tra noi e gli altri, c'è il nostro corpo che media e protegge la nostra identità, facendoci accorgere con facilità e istinto se altri stanno "violando i nostri confini".
Navigando in rete è tutta un'altra musica. In assenza di un corpo "fisico" diventa molto più complicato riconoscere le varie identità che possiamo incontrare, che potrebbero essere identità inventate se non si usano idonei sistemi di identificazione. In rete, quindi, può essere difficile scoprire se altri vogliono impossessarsi di informazioni che ci appartengono e che ci identificano.
Lo sviluppo tecnologico, la semplicità di utilizzo dei nuovi **apparati**, la presenza continua *on line*, la crescita dei ***social network***, nonché la spinta dei governi tesa a creare sempre più "cittadini digitali", hanno, ormai, permesso l'integrazione tra reale e virtuale, offrendo molte nuove opportunità ma modificando le modalità di protezione della propria identità.
In questa guida avremo sempre presente che la nostra è un'unica vita (senza differenza tra virtuale e reale) che utilizza, però, varie opportunità comunicative, compresa quella digitale. Forniremo le informazioni utili per continuare a navigare in rete senza rischiare troppo, accrescendo in noi la consapevolezza dei rischi in cui possiamo incorrere se navighiamo in modo superficiale e inesperto.
L'accesso alla rete è ormai possibile con una molteplicità di apparati: PC, CELLULARI, SMARTPHONES, TABLET, CONSOLE GIOCHI, DECODER DIGITALI, TELEVISORI. La difficoltà nell'utilizzo degli apparati

oggi non può più ritenersi un ostacolo. Le aziende costruttrici offrono sul mercato sistemi operativi "*user friendly*" (semplicità d'uso); lo stesso sistema operativo può essere utilizzato su più devices (PC, cellulare, tablet), ed è possibile eseguire azioni complesse con un semplice "clic" su un pulsante (app), facilitando in tal modo, enormemente, il compito ai consumatori. In ogni angolo del mondo qualcuno sta navigando e potremmo incontrarlo ma, l'estrema semplicità con cui si accede a questo nuovo mare comunicativo, non ci garantisce di essere al riparo da possibili minacce.

LE MINACCE DEL MONDO CONNESSO

Quando accendiamo un apparato connesso alla rete, siamo nella rete anche se non facciamo nulla. Un apparato connesso alla rete, in relazione al livello di vulnerabilità del sistema operativo in uso, è come una barca in balia delle onde che può subire arrembaggi da parte di altri naviganti che potrebbero impossessarsi del nostro natante (FURTO D'IDENTITÀ). Ciò significa che, se non mettiamo in atto una *corretta prevenzione*, i pirati informatici, attraverso **Virus, Worm**, **Spyware** e "tecniche di **phishing**", possono essere in grado di realizzare vere e proprie *truffe online* appropriandosi illegalmente di dati sensibili o di indurre, con l'inganno, a divulgare i nostri dati personali.

PROTEGGIAMO IL NOSTRO APPARATO, PROTEGGIAMO LA NOSTRA IDENTITÀ

I devices di ultima generazione utilizzano sistemi operativi che integrano protezioni in grado di limitare le minacce e gli attacchi provenienti dalla rete ma potrebbero non bastare, perché determinate difese sono attivabili solo tramite precise azioni sulle impostazioni del sistema operativo. Occorre, inoltre tenere presente che i cellulari e gli smartphones, le console per videogiochi o i televisori, hanno sistemi

operativi più leggeri, che richiedono una maggiore attenzione in termini di sicurezza e comportamenti particolarmente virtuosi da parte dei consumatori.

Per i soli PC occorre dotarsi di:

***Firewall**: può essere un apparato, quindi un hardware o un firewall personale, cioè un programma installato sul PC. Nei sistemi operativi che lo incorporano il firewall è già abilitato all'origine, pertanto è necessario solamente prestare attenzione a che lo stesso non sia stato disabilitato da qualche programma malevolo. Il firewall è 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.*

***Connettersi con un ROUTER:** è preferibile connettersi alla rete con un ROUTER, che, se di buon livello, riesce a sopportare i possibili attacchi e a proteggere il PC (gli attacchi, infatti, sono rivolti al router e non agli apparati a lui connessi). Il discorso non è attuabile anche alle connessioni che utilizzano direttamente un **modem** (anche da telefono).*

Per PC e altri apparati:

***Utilizzare software antivirus**, facilmente reperibili e scaricabili in rete, che è necessario mantenere sempre aggiornati.*

***Prestare attenzione ai siti Web che si visitano**: se viene segnalato che i contenuti non sono attendibili è opportuno uscire dalla pagina che si sta visitando e cercare pagine alternative.*

COMPORTAMENTI VIRTUOSI

Navigando dobbiamo adottare comportamenti virtuosi, tali da impedire la sottrazione di informazioni importanti. È fondamentale evitare di lasciare nella memoria (del PC, dello smartphone e dei nostri apparati connessi) i propri dati sensibili. Sono molte le persone che, ad esempio, conservano la propria carta d'identità scannerizzata, il cedolino del proprio stipendio, le password utilizzate e le credenziali

bancarie, permettendo in tal modo ai malintenzionati di usufruirne per il compimento di attività illecite. Purtroppo, qualsiasi sistema di sicurezza può essere eluso; il modo migliore per proteggere seriamente la nostra identità consiste quindi nell'eliminare all'origine, dalla memoria presente nell'apparato, tutti i dati sensibili. Oggi, per fortuna, la tecnologia ci viene incontro, permettendo di salvare tutte le nostre cose nel cloud, cioè in parti delle memorie presenti nella rete. Molti operatori offrono questo servizio (Drive, dropbox sono alcuni esempi). Basta un collegamento internet e, con qualsiasi apparato, possiamo recuperare e utilizzare le nostre cose digitali protette da login e password.

CELLULARI O SMARTPHONE

Oltre a telefonare attraverso la rete cellulare (aspetto marginale) le principali funzioni di uno smartphone possono essere utilizzate solo se si è connessi alla rete. Addirittura l'aggiornamento dello stesso smartphone, cioè del suo sistema operativo, avviene attraverso la rete. Con il tempo, uno smartphone non connesso alla rete vedrà ridursi notevolmente le sue capacità e le sue applicazioni, diventando inutilizzabile. Con uno smartphone possiamo messaggiare, inviare e ricevere posta elettronica, discutere nei social, fare acquisti on line, visionare siti, farci localizzare, farci condurre da un navigatore, fare foto e video da condividere, leggere libri, possiamo controllare cam, gestire la propria auto, ascoltare musica, vedere programmi televisivi, e tanto altro ancora. Con uno smartphone si accede ad uno store di applicazioni dove trovare e scaricare applicazioni gratuite e a pagamento (App), per aggiungere funzionalità all'apparato. Il cellulare, quindi, con la sua sim e la sua memoria diventa il custode di tutte le attività della nostra vita e della nostra identità. In caso di furto o smarrimento del dispositivo, tali informazioni possono cadere in mano a

soggetti estranei. *Proteggere il telefono con una password o un codice PIN o meglio ancora con l'impronta digitale sicuramente aiuta.*
Di seguito alcune modalità per migliorare la sicurezza dei telefoni mobili e proteggere lo smartphone.

I rischi che si corrono
Chi possiede tali dispositivi lo sa bene: basta sfiorare lo schermo per ritrovarsi su una pagina che non si voleva assolutamente visitare o cancellare dati che non si volevano cancellare, ecc..
È grazie a questa facilità nel toccare lo schermo inavvertitamente, che società disoneste possono mettere a segno pratiche commerciali scorrette attivando abbonamenti per servizi non richiesti.

I fatti
Grazie a **banner** che si aprono mentre si sta consultando, ad esempio, una **app** a volte, si attivano abbonamenti anche solo cliccando per chiuderli. Nel migliore dei casi, contestualmente all'attivazione, si riceve un messaggio in cui si avverte che il servizio è stato attivato e viene fornita una mail o un numero da chiamare per disattivarlo. In altri casi, invece, l'abbonamento non richiesto viene scoperto solo quando arriva la bolletta o quando si esaurisce il credito.
Attenzione: anche disattivando immediatamente l'abbonamento l'importo vi viene comunque addebitato sul conto telefonico. Occorre fare reclamo e chiedere il rimborso.

Come comportarsi in questi casi?
1. ***Installare*** *solo applicazioni provenienti da fonti attendibili; (Così come accade per il computer, è utile e opportuno installare tutti gli aggiornamenti disponibili per il sistema operativo del cellulare e per le applicazioni installate)*
   Nel caso di attivazione involontaria per sfioramento del touchscreen

o per un abbonamento caricato in maniera scorretta in bolletta:

2. ***contattare** il proprio operatore telefonico e chiedere la disattivazione del servizio; si può anche chiedere la sospensione **definitiva** di tutti i servizi a valore aggiunto;*
3. ***chiedere** il rimborso di quanto pagato e non dovuto;*
4. ***rivolgersi** alle sedi territoriali Adiconsum per ricevere l'adeguata assistenza ed ove necessario accedere alla conciliazione paritetica.*

Furto e smarrimento

È utile verificare che il cellulare disponga di una funzionalità che aiuti a ritrovarlo in caso di furto o smarrimento. Se tale funzionalità non è presente, è opportuno scaricare un'**applicazione** apposita che aiuti a ritrovare il telefono smarrito. In ogni caso è buona norma APPUNTARE IL **CODICE IMEI** del proprio dispositivo, di norma presente sulla scatola, nel vano batteria e nella memoria del telefono (il libretto di istruzioni del cellulare indica dove reperirlo). Il codice è necessario per le opportune comunicazioni all'operatore telefonico e alle Forze dell'Ordine in caso di furto o smarrimento, per bloccare o eventualmente rintracciare il cellulare smarrito.

POSTA ELETTRONICA

L'e-mail rimane uno degli strumenti più diffusi per comunicare online, anche se ora la messaggistica istantanea è sempre più utilizzata. La posta elettronica ci consente di scambiare messaggi con altri titolari di indirizzo di posta elettronica, nonché di inviare e ricevere allegati rapidamente. Le informazioni e i dati contenuti nelle e-mail sono, però, potenzialmente esposti ad attacchi di pirateria informatica; per questo motivo è importante proteggere il proprio **account** utilizzando una password di accesso complessa (combinando numeri e lettere), che è consigliabile modificare frequentemente. Con le mail viaggiano

anche i virus e per non infettare gli apparati è meglio evitare di aprire messaggi o allegati provenienti da mittenti sconosciuti. **Per difendersi utilizziamo solo operatori di posta elettronica che garantiscono sistemi antispam (Spam: messaggi inviati con modalità massiva e non richiesto) e soprattutto leggiamo la posta solo sul sito del nostro operatore di posta, direttamente sul server dove risiede l'account, attraverso il Web.**
I sistemi antispam possono sbagliare è quindi opportuno verificare frequentemente il contenuto della cartella spam, al fine di recuperare la posta che invece interessa e indicare i mittenti considerati sicuri, in modo tale che le email provenienti da questi non finiscano più nella cartella spam.

Non scaricate automaticamente i dati esterni all'e-mail
Attenzione agli allegati. Tramite i file allegati, infatti, moltissime società effettuano il cosiddetto TRACCIAMENTO dei dati personali, o la verifica dell'esistenza di un determinato indirizzo e-mail al quale poi inviare messaggi pubblicitari. Scaricare, quindi, nella memoria del proprio apparato solo gli allegati di cui siete certi della provenienza.

Il furto di identità, principale rischio dell'e-mail
Il furto dell'identità consiste nell'acquisire illegalmente dati sensibili e informazioni personali per poi venire successivamente utilizzati, ad esempio, per effettuare acquisti online con carta di credito o realizzare trasferimenti di denaro tramite il servizio di Internet banking; il tutto, ovviamente, sempre all'insaputa del titolare dei dati utilizzati.
Tale procedura fraudolenta, definita *phishing,* fa sì che nella casella di posta elettronica arrivino e-mail con loghi contraffatti che invitano a visitare determinate pagine Web (anche queste contraffatte), accedendo alle quali verrà poi richiesto l'inserimento di dati personali

o ad esempio le password della carte di credito. Esempio tipico è quello di una banca che, con un qualsiasi pretesto (aggiornamento del sistema, offerta commerciale, ecc.), invita il destinatario della e-mail a visitare la relativa pagina Web ed inserire i dati del proprio profilo.
Diventa quindi fondamentale saper riconoscere i casi di phishing.
I messaggi "truffaldini" normalmente:

- ***chiedono*** *di inserire le proprie credenziali in un* ***sito Web*** *(falso), del quale forniscono il collegamento (link);*
- ***utilizzano*** *un tono intimidatorio;*
- ***non sono*** *personalizzati;*
- ***presentano*** *errori di ortografia.*

Nel caso in cui, sfortunatamente, la pagina Web indicata nella e-mail sia stata aperta e siano stati inseriti i propri dati personali, è indispensabile informare immediatamente la banca, nonché segnalare l'accaduto alla Polizia di Stato.

CONSOLE GIOCO, TELEVISORI E DECODER

La console giochi è diffusa in tantissime case e viene connessa alla rete per sfidare giocatori sparsi nel mondo. Con il passaggio alla tv digitale anche televisori e decoder sono in grado di collegarsi alla rete, facendo sì che ogni spettatore televisivo possa ricercare tra i molteplici contenuti multimediali presenti in internet. Anche questi apparati comportano gli stessi rischi sopra descritti ma, purtroppo, per questi specifici apparati non esistono ancora programmi appositi o apparati dedicati alla difesa dalle minacce. Diventa, quindi, indispensabile, fare un uso virtuoso degli apparati stessi, limitandosi solo alla visione di contenuti multimediali e fornendo limitatamente dati relativi alla propria identità.

NAVIGARE IN INTERNET

Messi in sicurezza gli apparati e l'account di posta elettronica possiamo cominciare a navigare in Internet dove è possibile praticamente fare tutto ciò che si fa normalmente nella vita reale e forse anche di più. Internet è una fonte inesauribile di informazioni e contenuti relativi a qualsiasi argomento; una vera e propria enorme biblioteca per apprendere senza limiti. Ovviamente anche le minacce sono presenti e *raggruppabili in tre categorie:*

- ***attacchi alla persona,*** *ovvero truffe e inganni, noti come "ingegneria sociale", cioè la modalità che i cyber criminali, agendo sull'ingenuità delle persone - e non sul software - utilizzano per accedere agli apparati delle stesse;*
- ***attacchi al device****, al browser o alle applicazioni;*
- ***attacchi ai siti Web****, ad esempio il cross-site scripting.*

I pirati informatici (cyber criminali) navigano in rete come ognuno di noi e vanno alla ricerca di eventuali vulnerabilità nel codice dei siti Web, per inserirvi script dannosi in grado di raccogliere informazioni private relative a coloro che visitano tali siti. In questo modo riescono a manomettere gli account Web, monitorare ciò che si digita e anche compiere, a nome di ignari naviganti, azioni indesiderate. Qualsiasi attività si esegue in internet può essere minacciata ma non per questo si deve rinunciare al suo uso. La percentuale di possibilità di subire un attacco informatico è molto inferiore a qualsiasi possibilità di subire una minaccia nella vita quotidiana. Dobbiamo quindi essere solo attenti e non sprovveduti, come, in fondo facciamo ogni giorno uscendo da casa.

BROWSER

Per navigare nel Web è necessario usare uno specifico programma definito **browser**, se ne trovano molti, tutti gratuiti e spesso legati ai

vari sistemi operativi. L'elevato livello di concorrenza fa sì che i diversi browser tendano sempre a migliorare e ciò rappresenta anche un'importante garanzia per il consumatore. I criteri di scelta sono soggettivi e legati alle proprie modalità d'uso. Per ottenere il massimo della sicurezza occorre sempre operare nelle impostazioni del programma, impostando i settaggi appropriati per tutelare la propria identità e attivare sempre gli aggiornamenti automatici quando proposti, in modo tale da essere garantiti anche dalle minacce più recenti. Comunque è importante che la scelta non ricada solo su quelli che garantiscono la maggiore velocità di navigazione, bensì su quelli in grado di assicurare all'utente la massima sicurezza (informazioni verificabili facendo una ricerca su internet).
La velocità di navigazione dipende dal browser, ma soprattutto dal comportamento dell'utilizzatore, il quale può installare estensioni utili ad attivare nuove funzioni, chiamati *plugin.* Tali estensioni, però, rallentano l'esecuzione. Per mantenere alta la velocità di esecuzione è quindi consigliabile l'utilizzo di browser che consentano di gestire i vari plug in abilitandoli o disabilitandoli all'occorrenza.

TRACCIAMENTO
Quando navighiamo in rete il nostro "percorso" viene tracciato a nostra insaputa. Le tecniche utilizzate per il tracciamento, tuttavia, non configurano dirette violazioni della privacy, in quanto non identificano dati personali o sensibili. Ogni apparato che si connette alla rete viene identificato in Internet con una sorta di "*numero di targa*", detto **Indirizzo IP**. Senza un'identificazione, infatti, l'utente non potrebbe navigare. Qualsiasi azione si fa sull'apparato è in realtà una richiesta a qualcuno (il server) e quanto richiesto ritorna precisamente all'indirizzo IP dal quale la richiesta è partita. È bene precisare che nessuno (tranne la Magistratura, in determinati casi) può accoppiare un indirizzo IP alle generalità del suo utilizzatore. Quando si naviga in un sito

Web, accade che terze parti (società specializzate), diverse dal sito nel quale ci troviamo ed interessate al comportamento di un determinato indirizzo IP, sono in grado, con particolari tecniche, di tracciarlo. I dati raccolti vengono poi utilizzati per scopi pubblicitari, facendo in modo che allo stesso device arrivino messaggi pubblicitari rispondenti agli interessi dell'utilizzatore. Tutto ciò, tuttavia, avviene all'insaputa di chi naviga in rete. Alcuni browser permettono di bloccare il tracciamento ma occorre essere consapevoli che non tutto potrebbe funzionare integralmente in quanto molti dei servizi che sembrano gratuiti sono sostenuti dalla pubblicità.

SOCIAL NETWORK

I Social Network sono diffusissimi e di vario tipo, ma sfortunatamente questi servizi, che sembrano di facile utilizzo, non sono altro che siti Web e come tali presentano i rischi sopra menzionati. I social network, inoltre, necessitano di maggiore attenzione perché è lo stesso utente che, all'atto dell'iscrizione, sceglie volontariamente di comunicare informazioni relative alla propria identità, facilitando il compito dei malintenzionati. È importante ricordare sempre di proteggere il proprio account modificando spesso la password e offrire la propria amicizia solo alle persone delle quali ci si può certamente fidare.

QUANDO CI SI ISCRIVE AD UN SOCIAL NETWORK E AD OGNI SUO AGGIORNAMENTO È IMPORTANTE VISUALIZZARE LE IMPOSTAZIONI, PONENDO ATTENZIONE ALLE FUNZIONI RELATIVE ALLA PRIVACY, ATTIVANDO QUELLE CHE GARANTISCONO L'ESPOSIZIONE DELLE PROPRIE INFORMAZIONI SOLO AD UNA CERCHIA RISTRETTA.

Anche se attiviamo le impostazioni in modo perfetto, bisogna essere consapevoli che tutto ciò che è postato in un profilo di qualsiasi social network è disponibile a chiunque lo voglia ed è quindi sempre pubblico.

NON BISOGNA MAI DIMENTICARE CHE TUTTO CIÒ CHE È IN RETE PUÒ ESSERE COPIATO, SALVATO E REDISTRIBUITO DA TERZI, senza peraltro che l'interessato se ne accorga. **Il modo migliore per tutelare la propria identità e tutelare la propria reputazione è avere, sempre, la consapevolezza di ciò che si decide di far sapere a tutti riguardo la propria sfera personale**. Per fortuna l'immenso numero di informazioni personali presenti in rete rende bassissime le probabilità che siano carpite proprio quelle che ci riguardano. Particolare ATTENZIONE deve essere rivolta ai minori (grandi utilizzatori dei social) rendendoli edotti dei rischi che corrono utilizzando i social network con superficialità e scarsa protezione.

Ricapitoliamo gli atteggiamenti virtuosi da mantenere nei social network:

- ***controllare sempre*** *le impostazioni di sicurezza;*
- ***selezionare*** *con cura gli amici e accettare la loro amicizia solo se si conoscono veramente;*
- ***controllare*** *ciò che gli amici scrivono su di noi, e se sono cose spiacevoli chiederne subito la rimozione ed annullare l'amicizia;*
- ***usare*** *password complesse, sicure ed efficaci, modificandole spesso;*
- ***personalizzare*** *le impostazioni della privacy rendendo disponibili i contenuti personali solo ad amici fidati;*
- ***negare*** *alle applicazioni che si utilizzano la possibilità di accedere ai propri dati;*

- ***non rendere*** *pubblici foto e video con contenuti particolarmente personali e che riguardano i minori;*
- ***selezionare*** *il materiale che viene postato evitando di diffondere informazioni troppo personali;*
- ***verificare sempre*** *le notizie che vengono diffuse da altri (fidarsi solo di profili autenticati) consultando fonti attendibili. Nei social sono pubblicate molte "bufale".*

MESSAGGISTICA ISTANTANEA

La messaggistica istantanea (*instant messaging)* è molto diffusa grazie all'uso dello smartphone collegato alla rete. Le applicazioni più famose sono WhatsApp, Telegram, Viber e Messenger Facebook. Grazie a queste App e internet è possibile la comunicazione immediata, soprattutto di messaggi brevi, fra utenti in modo sincrono e in alcuni casi anche criptato. L'evoluzione di quest'applicazione permette ormai di comunicare tra persone qualsiasi cosa (messaggi di testo, conversare tramite scambiare video, foto, suoni e allegati). La grande diffusione è dovuta al fatto che l'uso delle applicazioni di *instant messaging* è gratuita e che l'unico costo per l'utente è la connessione ad internet. La tecnologia usata è complessa e varia per ogni applicazione ma il principio di base è peer-to-peer, permettendo alle applicazioni di comunicare direttamente tra loro. **Per far funzionare e quindi utilizzare questo tipo di applicazioni è necessario fornire ai server del gestore del servizio la propria rubrica di contatti,** (numeri di cellulari o dei contatti sui social) che in tal modo riconoscerà chi fra i propri contatti fa uso dell'applicazione mettendoli in contatto ma avendo anche una copia di questi. È il vero costo che paghiamo a chi ci offre il servizio, cioè far conoscere un'infinità di contatti. Occorre inoltre essere consapevoli che molto spesso i proprietari di *instant messaging* sono anche proprietari di

social o altre società di servizi che possono creare specifiche pubblicità. **Non è a rischio la sicurezza dell'identità degli utilizzatori perché non è possibile associare ai numeri di telefono le generalità dell'utente** ma, come per i social, dobbiamo tener presente che quando utilizziamo le applicazioni di messaggeria istantanea, con le condizioni contrattuali accettiamo di fornire i nostri dati e che ci assumiamo la responsabilità della sicurezza del dispositivo e dell'account.
Per proteggerci quindi occorre sempre avere consapevolezza di cosa utilizziamo e proteggere gli apparati. **Non va dimenticato che tutto ciò che comunichiamo lascia traccia nella memoria del proprio apparato ed essendo notizie personali dovrebbero essere eliminate per proteggersi da possibili intrusioni.**

E-COMMERCE

Il commercio elettronico (**eCommerce**), consiste nell'acquisto di beni o servizi tramite Internet, utilizzando anche apparati con connessione mobile. Per acquistare si accede ad un sito predisposto alla vendita, si sceglie il prodotto o servizio desiderato visionandolo e leggendone le caratteristiche, si inserisce il prodotto scelto in un carrello virtuale, si conferma l'acquisto con un clic e parte la propria richiesta di acquisto. Il pagamento avviene in rete, normalmente con moneta elettronica (carte di credito o sistemi di pagamento elettronici paypal e similari), in uno specifico sito dotato di trasmissione criptata e sistemi alta sicurezza (**nella URL appare la dicitura https e un lucchetto chiuso**). Raramente viene utilizzato il contrassegno postale che ha un costo supplementare. Fate attenzione a chi richiede il bonifico bancario, metodo sconsigliato perché non garantisce il consumatore in caso di mancata consegna. Nel periodo indicato al momento dell'acquisto, la merce viene recapitata nel luogo indicato dal consumatore.

Il tutto è facilissimo e fa risparmiare tempo e denaro, ma farlo in sicurezza è una necessità che non dobbiamo mai trascurare.

Come tutelarci

Oltre a mettere in pratica i suggerimenti già indicati in questa guida, occorre verificare che il sito di eCommerce non sia truffaldino e che non venda merce contraffatta. Prima di acquistare on line, verificare se le recensione presenti in internet di altri acquirenti sono positive altrimenti è meglio desistere. Leggere le condizioni di contratto, essere certi che venga applicato il diritto di recesso entro 14 giorni dall'acquisto, appurare che sia indicato il luogo della sede legale dell'azienda e della sua iscrizione alla camera di commercio, che sia garantito il servizio di post vendita con metodi reali e diffidare da chi propone prezzi troppo stracciati.

LE REGOLE DA NON DIMENTICARE

Ci sono alcune semplici regole che, se osservate, permettono di ridurre notevolmente i rischi.

1. **Mantieni l'apparato ben protetto:**
- usa sempre gli aggiornamenti automatici dei software e del sistema operativo;
- utilizza sempre firewall, antivirus e antispam.

2. **Custodisci le tue informazioni personali:**
- inserisci dati personali su Internet solo in pagine con la scritta **https** nell'indirizzo e il simbolo del lucchetto;
- Non lasciare le proprie informazioni o documenti d'identità nelle memorie dei dispositivi;
- utilizza password *che siano lunghe (almeno 8 caratteri), contengano lettere maiuscole e minuscole, numeri e simboli.*

3. **Pensa prima di cliccare:**
- quando ricevi un allegato alla posta elettronica aprilo solo se certo

del mittente. Non scaricare il contenuto di e-mail pubblicitarie o di sospetto spam.

4. **Non fornire informazioni via e-mail:**

- cognome, nome, indirizzo, numero di telefono, foto, età, ecc..

5. **Attenzione ai falsi:**

- diffida da messaggi allarmistici, richieste di aiuto, segnalazioni di virus, offerte imperdibili, richieste di dati personali, ecc..

6. **Sui social network con prudenza:**

- controlla bene le impostazioni relative alla privacy e ricorda che tutto ciò che viene postato può diventare pubblico anche se non si vuole. È importante ricordare che ciò che viene pubblicato rimane spesso di proprietà della piattaforma che raccoglie le pubblicazioni, anche laddove poi si decida di cancellarle.

7. **Rispetta la netiquette:**

- è opportuno essere educati, la netiquette è un insieme di regole da osservare nei social network, nei forum e nelle community.

GLOSSARIO PERICOLI

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.

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

Spyware e Adware: programmi informatici usati per raccogliere informazioni dal sistema sul quale sono installati e trasmetterle ad un destinatario interessato. I PROGRAMMI FREE, che si scaricano dalla rete, possono contenere spyware o adware. È BENE CONTROLLARE, QUANDO SI SCARICA UN SOFTWARE GRATUITO, CHE SIA ESPRESSAMENTE CERTIFICATA L'ASSENZA DI ADWARE E SPYWARE. 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.

Trojan horse: è un programma informatico apparentemente utile che, tuttavia, contiene al suo interno un malware.

Virus: è un programma che si autodiffonde, cioè infetta autonomamente o sfruttando la vulnerabilità di altri programmi (ad esempio i software di posta elettronica) o dei sistemi operativi.

Worm: è un malware che modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo fino a che il computer non viene spento. Scopo del worm è rallentare il sistema con operazioni inutili e dannose. Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica.

VOCABOLARIO MINIMO

ACCOUNT - Informazioni che identificano l'utente e gli consentono di accedere alle risorse a cui è autorizzato. Un account è formato da un nome utente (username) e da una parola d'ordine necessaria per accedere al sistema (password). Esistono diversi tipi di account, che vanno dal semplice account per l'utilizzo di una macchina a quelli forniti dai provider per l'accesso a Internet e al servizio di posta elettronica.

ADSL - Acronimo di Asymmetric Digital Subscriber Line. Tecnologia che permette la trasmissione di dati a velocità elevate su linee telefoniche tradizionali, utilizzabile per la connessione ad Internet. ADSL è una tecnologia asimmetrica, cioè fornisce velocità differenti in trasmissione (fino a 640 Kbps) e in ricezione (fino a 7 Mbps).

ANTIVIRUS - Programma atto a identificare e rimuovere eventuali virus presenti in un computer. Gli antivirus più recenti sono in grado di controllare anche gli allegati di posta elettronica ricevuti via rete e di controllare automaticamente ogni dischetto inserito nel computer. Un antivirus deve essere tenuto costantemente aggiornato, scaricando periodicamente dal sito Internet del produttore le definizioni dei virus scoperti nelle ultime settimane.

APPLICAZIONE (App) - Usato anche come sinonimo di "programma", indica in realtà solo i programmi di tipo applicativo, cioè quelli che vengono fatti partire dall'utente per eseguire un determinato lavoro (videoscrittura, disegno, contabilità, giochi). Vedi anche Programma.

Banda larga - Identifica un vasto insieme di tecnologie accomunate da una peculiarità: quella di consentire il collegamento a In-

ternet e alle Reti locali ad una velocità di trasmissione dei dati largamente superiore a quelle supportate dai modem tradizionali.

BANNER - Striscione pubblicitario elettronico inserito in una pagina Web. Consiste in un'immagine, spesso animata, solitamente in formato GIF o JPEG. Il banner contiene un link al sito dell'inserzionista.

BROWSER - Programma utilizzato per la navigazione su Internet. I browser attuali permettono di sfogliare le pagine presenti sulla Rete (World Wide Web), di inviare e ricevere posta elettronica, di partecipare a gruppi di discussione (newsgroup) e di scaricare file dalla rete, salvandoli sul proprio computer. Con alcuni di essi è inoltre possibile creare semplici pagine in HTML e pubblicarle in Rete.

CODICE IMEI - (International Mobile station Equipment Identity) è un codice numerico che serve a identificare i dispositivi mobili (telefonini, smartphone, tablet) e alcune tipologie di telefoni satellitari. Può essere utilizzato, quindi, per scoprire le caratteristiche tecniche del dispositivo in uso. Solitamente si trova stampato all'interno del comparto batteria (nelle vicinanze del tray per la scheda SIM); nel caso in cui il dispositivo abbia la batteria non estraibile, il codice IMEI sarà stampato o all'interno del carrellino estraibile della scheda SIM o sulla cover posteriore del dispositivo. In alternativa, il codice IMEI può essere visualizzato anche sul display de dispositivo utilizzando dei codici particolari o andando a spulciare nei menu di sistema dello smartphone.

CLIENT - In generale è un computer collegato ad un server ma un client è anche il programma che, in un sistema client/server, inoltra le richieste dell'utente ad un programma server. L´esempio più comune

è sicuramente il browser che l'utente utilizza per inviare richieste ai web server cosi da poter visionare le pagine che interessano.

COMMUNITY - Comunità di utenti Internet che condividono un interesse specifico e che frequentano un medesimo sito Internet per il Content (notizie, descrizione prodotti/servizi, formazioni) e le aree di interazione (forum, chat, sondaggi, opinioni sui prodotti e servizi) relativi a tale interesse.

DEVICE - Appartengono a tale famiglia i componenti elementari dell'elettronica. Per estensione, vengono anche chiamati così i componenti più complessi.

DNS - Acronimo di Domain Name System. Sistema che assegna ad ogni indirizzo IP un nome mnemonico (del tipo www.microsoft.com), più facile da ricordare e da digitare.

DOMINIO - Parte finale di un URL che identifica il tipo di sito Internet presente ad un determinato indirizzo.

E-COMMERCE - Operazioni commerciali effettuate on-line. L'acquirente può essere un consumatore finale (c.d. Business to Consumer o B2C) ovvero un soggetto esercente attività commerciale o professionale (c.d. Business to Business o B2B).

FTP - Acronimo di File Transfer Protocol (protocollo per il trasferimento di file). Protocollo di comunicazione adatto per il trasferimento di file fra due computer connessi attraverso una rete TCP/IP.

HOME PAGE - Pagina d'apertura di un sito Web che viene caricata per prima quando si accede al sito. Dalla Home page è possibile accedere a tutte le pagine/file che compongono il sito.

HOST - Si definisce host o end system (terminali) ogni terminale collegato ad Internet. Gli host possono essere di diverso tipo, ad esempio computer, palmari, dispositivi mobili e così via, fino a includere web TV, dispositivi domestici e thin client.

HOTSPOT - Un Hot Spot é un luogo in cui è presente una rete Wi-Fi aperta al pubblico, attraverso la quale è possibile connettersi ad Internet: vi si può accedere con un notebook, un PDA, un telefono cellulare o qualunque dispositivo in grado di utilizzare una rete wireless.

HTML - Acronimo di HyperText Markup Language, il linguaggio per computer con il quale vengono create le pagine Web.

HTTP - Acronimo di HyperText Transfer Protocol (protocollo per il trasferimento di ipertesti). È il protocollo utilizzato su Internet (o, meglio, sul World Wide Web) per l'accesso a pagine HTML.

INTERNET - Rete di computer, costituita dall'unione di reti locali, metropolitane e geografiche in ogni continente. Le origini di Internet risalgono alle ricerche dell'organismo militare statunitense DARPA (Defence Advanced Research Project Agency), che sviluppò il protocollo di connessione a pacchetti TCP/IP (Transmission Control Protocol - Internet Protocol) e lo utilizzò per creare una rete di computer in grado di operare senza interruzioni anche in seguito alla distruzione di parte di essa.

INDIRIZZO IP - Numero a 32 bit, che identifica univocamente ogni macchina presente su una rete. Viene rappresentato sotto forma di quattro numeri da 8 bit (da 0 a 255), separati da un punto (per esem-

pio 192.168.0.1). Ogni computer (host) connesso ad una rete deve avere un indirizzo IP permanente (statico), mentre quando un utente si connette ad Internet tramite un provider gli viene assegnato generalmente un indirizzo IP temporaneo per la durata della connessione.

LAN - Una LAN (Local Area Network) è una rete locale, che collega computer compresi in un'area limitata (al limite in edifici vicini fra loro, come per esempio quelli di un'università) allo scopo di permettere la comunicazione e la condivisione di risorse.

LINK - In una pagina HTML, un link è un collegamento ad un'altra pagina. I link permettono la navigazione fra le pagine Internet con semplici clic del mouse.

MODEM - Dispositivo in grado di mettere in comunicazione due computer tramite una linea telefonica. Il modem converte (modula) i segnali digitali in uscita in impulsi sonori analogici, che vengono convogliati sulle tradizionali linee telefoniche. I segnali analogici in entrata sono riconvertiti invece in forma digitale (demodulati).

NEWSGROUP - I newsgroup (gruppi di discussione) sono "bacheche elettroniche" dove gli utenti possono leggere e scrivere messaggi, diretti a tutti i frequentatori del gruppo.

PASSWORD - Parola d'ordine che un sistema informatico richiede per l'accesso a servizi personali. Vedi Account.

PHISHING - Storpiatura della parola inglese che significa pescare, usa spesso finte email come una vera e propria esca. Si avvale infatti di un messaggio e-mail dall'aspetto ufficiale in apparenza proveniente da un istituto di credito o di una società che fornisce servizi a mezzo Internet.

POP3 - Acronimo di Post Office Protocol-3, protocollo utilizzato per recuperare la posta da una casella postale remota. POP3 viene utilizzato quando un utente si collega ad Internet tramite un provider e richiede il trasferimento sulla propria macchina dei messaggi di posta elettronica in attesa sul server.

PORTALE - Sito Web, solitamente concepito per essere la prima pagina caricata dal browser, che offre una vasta gamma di servizi e contenuti.

POSTA ELETTRONICA - Servizio che consente lo scambio di messaggi fra due host collegati ad Internet. Ai messaggi possono essere anche allegati dei documenti (immagini, documenti di Word, etc.).

RETE - Con il termine "rete" (indicato in minuscolo) si indica un insieme composto da un certo numero di computer (host) collegati fra di loro per scambiarsi informazioni e condividere risorse (file, periferiche, applicazioni), e dall'hardware utilizzato per realizzare i collegamenti (ad esempio, instradatori o router, concentratori o hub, gateway, switch e firewall.

ROUTER - Il termine **router** assume in italiano il significato di *instradatore.* Il router, infatti, è un dispositivo che si occupa di instradare i dati fra molteplici e differenti reti. È possibile utilizzare un router per collegare in Rete più personal computer, anche in assenza di una connessione a Internet. Nel caso si intenda distribuire una linea Adsl su molteplici dispositivi, il router assume il ruolo di apparecchio deputato a condividere l'indirizzo Ip fornito dal provider attraverso il modem.

SITO WEB - Singola destinazione sul Word Wide Web, contraddistinta da un indirizzo. Un sito è composto da una Home page e, so-

litamente, da un certo numero di altri documenti (detti anche “pagine”) o file alle quali si accede dalla Home page.

SMS - Acronimo di Short Message Service, un servizio che consente di inviare, da un telefono cellulare o da Internet, brevi messaggi di testo ad un altro cellulare.

SMTP - Acronimo di Simple Mail Transfer Protocol (semplice protocollo per il trasferimento di posta). Protocollo utilizzato per la consegna della posta elettronica su reti TCP/IP (Internet).

Social Network -Sito Internet che fornisce agli utenti della rete un punto d’incontro virtuale per scambiarsi messaggi, chattare, condividere foto e video, ecc.

TCP-IP - Transmission Control Protocol/Internet Protocol. È il protocollo utilizzato da Internet e da molte reti locali. In particolare, il TCP si occupa della suddivisione dei messaggi in “pacchetti”, mentre l’IP pensa ad inviarli al corretto destinatario.

URL - Acronimo di Uniform Resource Locator, è un metodo per identificare univocamente ogni file (incluse le pagine HTML) presente in Internet. Un URL è formato da tre parti: il protocollo da utilizzare per accedere al file, il nome DNS della macchina sulla quale si trova il file e il nome del file stesso.

USERNAME - Nome che identifica l’utente di una macchina o di un servizio.

VIRUS - Programma che si installa su un computer all’insaputa dell’utente, ed è potenzialmente in grado di eseguire azioni maligne. I virus sono in grado di autoreplicarsi e attaccarsi ai programmi, propagandosi attraverso lo scambio di file.

Wi-Fi - Wi-Fi è stato pensato per collegare dispositivi senza fili e reti locali, ma molto spesso è utilizzato per fornire accesso ad internet.

WORLD WIDE WEB - www è l'acronimo di World Wide Web. Si tratta di un'applicazione progettata all'inizio degli anni novanta che, tramite il linguaggio HTML per la creazione di pagine Internet e il primo browser Mosaic, ha reso Internet facile da utilizzare e capace di visualizzare contenuti in forma testuale contenenti suoni, immagini fisse e in movimento e collegamenti (link) ad altre pagine, attivabili con un semplice clic del mouse. Per estensione, "www" è diventata poi la sigla che si trova all'inizio di ogni indirizzo Internet che mostri contenuti di questo tipo.