NAVIGA SENZA RISCHI, LEGGI QUESTA GUIDA!

Ministero dello Sviluppo Economico

UNIONCAMERE
CAMERE DI COMMERCIO D'ITALIA

PROGETTO GIOVANI CONSUMATORI NEL WEB

NAVIGA SENZA RISCHI, LEGGI QUESTA GUIDA!

Introduzione

Qualunque sia la tua età, Internet è un gran posto da visitare.
Come probabilmente saprai, ti permette di essere sempre in contatto con tutte le persone che conosci e di accedere a una quantità enorme di informazioni. In Internet, come in una grande città, ci sono biblioteche, università, musei e luoghi per divertirsi; ci sono posti dove studiare, fare ricerche, imparare cose nuove e stare al passo con le cose che più ami: dalla musica ai film allo sport ai giochi on line. Sempre di più, puoi trovare e acquistare quello che più ti piace.
Eppure, esattamente come in una grande città, è necessario tenere sempre gli occhi aperti, saper riconoscere i pericoli ed evitarli adottando alcune precauzioni.
Lo scopo di questa guida è fare in modo che tu sia informato sui rischi che corri, attraverso una serie di consigli per aggirare sia i problemi più banali che le vere e proprie truffe. Così, potrai goderti solo il bello che la rete è in grado di offrire.

L'email. Comunicare bene ogni giorno.

La posta elettronica, universalmente conosciuta come email (dall'inglese *electronic mail*), è il corrispettivo digitale della posta ordinaria e cartacea. Oggi è tra i mezzi più veloci ed economici per comunicare, perché bastano un account, un indirizzo o una mailing list, e con un clic un messaggio parte e arriva a destinazione in una manciata di secondi.

La tua posta è piena di spazzatura? Si chiama spamming.

Sempre più spesso le persone e le aziende usano l'email per inviare messaggi a tutti i loro contatti, incoraggiandoli a comprare qualcosa, fare qualcosa, o visitare un sito web. E considerato che la posta elettronica è essenzialmente gratuita, inviare dieci, centinaia o migliaia di messaggi non fa nessuna differenza.
Questo fenomeno, molto noto a chi usa abitualmente l'email, viene chiamato *spamming*, e sta a intendere la spazzatura che periodicamente riempie la casella di posta elettronica, costringendo l'utente a svuotarla costantemente per evitare che si intasi impedendogli di ricevere le comunicazioni che realmente gli interessano.
La parola *spam* si può definire, quindi, come l'invio massiccio e au-

tomatico di posta elettronica a recapiti con i quali il mittente non ha mai avuto contatti diretti.
Ma come fanno le aziende o le persone che non conosciamo ad avere il nostro indirizzo email? Purtroppo oggi esistono numerosi software in grado di rastrellare indirizzi sul web prelevandoli da siti, *forum* e newsgroup e di immagazzinarli in banche dati che possono essere ingiustamente usate a scopi pubblicitari.
Per questo è consigliabile attivare nei propri indirizzi email un filtro anti-*spam* che nella maggior parte dei casi riesce a contenere il fenomeno.
Se riesci a individuare l'autore dello *spam* (per esempio visitando il sito Internet cui solitamente rimanda l'email dello *spammer*) puoi comunicare la tua opposizione al trattamento dei tuoi dati di posta elettronica e richiedere espressamente che vengano cancellati dagli archivi.
Se lo *spammer* continua ad inviarti email non richieste, puoi scrivere al Garante per la protezione dei dati personali che provvederà a farlo smettere (www.garanteprivacy.it).

La posta elettronica certificata, più sicura che mai!

La consegna dei messaggi inviati al destinatario non è sempre garantita. Puoi richiedere una conferma di consegna o di lettura dei messaggi inviati, ma il tuo destinatario è libero di scegliere se inviare o meno tale conferma. In caso di mancata consegna, generalmente, il server ti avverte automaticamente, ma questo non in tutti i casi.
Questi limiti della posta elettronica tradizionale possono essere

superati dalla Posta Elettronica Certificata (PEC). Se sei maggiorenne la puoi usare direttamente, altrimenti puoi consigliare ai tuoi genitori di farlo e, perché no, assisterli nel caso non siano pratici di Internet. A differenza della casella elettronica tradizionale, infatti, la PEC può fornire la precisa indicazione temporale del momento in cui l'email è stata inviata, rilasciando anche una ricevuta di avvenuta consegna, con l'indicazione del momento nel quale la consegna è stata effettuata. La PEC ha lo stesso valore di una tradizionale lettera raccomandata con ricevuta di ritorno.

I blog.
Diari personali, ma condivisi.

Un *blog* è una sorta di diario on line, un sito dove una o più persone (*blogger*) possono scrivere, pubblicare immagini e contenuti audiovisivi su qualunque argomento. Generalmente aggiornato con una certa periodicità, il *blog* serve a pubblicare in tempo reale notizie, informazioni, opinioni o storie, e dà la possibilità agli utenti che lo seguono di lasciare i loro commenti ai *post* (un *post* non è altro che il contenuto pubblicato).

I forum, piazze virtuali aperte a tutti.

Un *forum* è uno spazio virtuale di dibattito, generalmente frequentato da utenti con interessi comuni.

ctrl

Ogni iscritto al *forum* può "postare" messaggi in relazione ai temi proposti e ogni messaggio resta memorizzato nella discussione in cui è stato pubblicato. Generalmente frequentato da persone interessate a un determinato argomento, un *forum* diventa così non solo un luogo utile per lo scambio di idee e opinioni, ma anche un posto dove imparare dagli altri.
Alcuni *forum* sono luoghi di confronto totalmente liberi e sono aperti a tutti; molti altri, prima di concedere la possibilità di intervento nelle discussioni, richiedono all'utente di registrarsi.
I *forum*, così come i *blog*, sono un'occasione per approfondire la propria conoscenza di un argomento, confrontarsi e scambiare opinioni. Molti sono usati per risolvere piccoli problemi di vita quotidiana attraverso i consigli di altri utenti. In alcuni casi, vengono usati da aziende, società o enti che li utilizzano come strumenti di comunicazione. Sempre di più, sono un luogo dove scambiare utili pareri sui prodotti acquistati o confrontare i prezzi dei principali negozi on line.
Ogni *forum* ha degli amministratori e uno o più moderatori che si occupano di vigilare sullo sviluppo corretto e rispettoso delle discussioni. I gestori (detti amministratori) hanno invece anche la possibilità di chiuderlo, modificarlo e di espellere utenti indesiderati. Naturalmente, i protagonisti dei *forum* restano sempre gli utenti, che possono in qualunque momento pubblicare messaggi aprendo nuove discussioni, "postare" foto e immagini. Gli ospiti, infine, sono utenti che visitano il *forum* senza essere registrati.

Ricordati

Leggi con attenzione il regolamento del *forum*.
Se sei minorenne e vuoi aprire un *blog* o partecipare a un *forum* devi comunicarlo ai tuoi genitori. Generalmente, infatti, al momento dell'iscrizione è richiesto di dichiarare che i genitori ne sono al corrente.

- Controlla attentamente il materiale che intendi pubblicare. Anche informazioni apparentemente innocue possono diffondere notizie sensibili e delicate.
- Non fornire mai le tue informazioni personali, come l'indirizzo di casa, i numeri di telefono, il nome della scuola, i cognomi di amici o familiari.
- Non pubblicare immagini provocanti o oscene, tue o di altre persone, e accertati che le immagini pubblicate non rivelino alcuna informazione personale.
- Tieni presente che chiunque può stampare facilmente i contenuti di un *blog* o di un *forum* e salvarli su un computer.
- Evita di litigare con altri utenti, di insultarli o di usare un linguaggio inappropriato.

Sempre connessi con i social network.

Nati inizialmente all'interno di comunità di studenti, oggi i social network sono tra gli strumenti di comunicazione più diffusi. Alcuni dei principali social network, per fare alcuni esempi, sono Facebook, MySpace, Hi5, Flickr, Skyrock, Friendster, Tagged, LiveJournal, Orkut, Fotolog, Bebo.com, LinkedIn, Badoo.Com, Multiply, Imeem, Ning, Last.fm, Twitter, MyYearbook, Vkontakte, aSmallWorld, Windows Live e Xiaonei. Attraverso i social network le persone creano vere e proprie reti sociali basate su legami e interessi di varia natura: dai rapporti scolastici ai vincoli familiari, dalla conoscenza casuale ai rapporti di lavoro a quelli di amicizia e così via. I social network facilitano lo scambio di conoscenze ed espandono letteralmente la tua possibilità di comunicare. Ma considera anche che

quando ti iscrivi a un social network e inserisci i tuoi dati personali ne perdi il controllo. Le tue informazioni possono essere registrate da tutti i tuoi contatti e dai membri dei gruppi ai quali hai aderito, e possono essere rielaborate e diffuse anche a distanza di tempo. Per esempio, partecipando a un social network, puoi indirettamente concedere all'impresa che gestisce il servizio la licenza di usare senza limiti di tempo il materiale che inserisci on line (foto, pensieri, scritti, ecc.).

Se vuoi cancellare l'iscrizione a un social network, il più delle volte ti è concesso solo di disattivare il profilo, non di eliminarlo. E così, i dati e i materiali che hai pubblicato on line vengono comunque conservati nei server che li ospitano.

Questo perché le aziende che gestiscono i social network generalmente si finanziano attraverso la pubblicità on line e il valore di queste imprese è connesso anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni raccolte al miglior offerente.

Devi anche considerare che, a tutela della tua privacy, puoi limitare l'accesso al tuo profilo solo ad alcune persone.

Certamente, puoi iscriverti e partecipare ai social network senza correre nessun pericolo e divertendoti molto, ma seguire dei semplici accorgimenti può aiutarti a farlo con maggiore tranquillità.

Ricordati

- Leggi sempre l'informativa sulla privacy per avere la piena consapevolezza del controllo che il social network opera sui contenuti pubblicati dagli utenti.
- Usa le impostazioni per la privacy. Limita la visualizzazione del tuo profilo e dei tuoi dati personali solo agli amici che hai accettato o ai partecipanti di una delle reti sociali alle quali hai personalmente (e consapevolmente) aderito.
- Fai in modo di controllare come vengono utilizzati i tuoi dati per-

sonali da parte del fornitore del servizio. Se non desideri ricevere pubblicità, ricordati di rifiutare il consenso all'uso dei tuoi dati.

- Usa nomi account e password diversi da quelli utilizzati su altri siti web, sulla posta elettronica e per la gestione del conto corrente bancario.
- Prima di accettare nuovi amici, accertati di conoscerli. I ladri di identità possono creare falsi profili per ottenere informazioni più o meno riservate.
- Non pubblicare informazioni riservate come indirizzo e numero di telefono.
- Non scrivere o pubblicare niente che in futuro possa mettere in imbarazzo te o altre persone. Ricordati che quello che viene caricato on line difficilmente può essere eliminato.
- Scegli di rendere accessibili le tue foto personali solo ai contatti di cui ti fidi.
- Quando clicchi sui link ricevuti in messaggi inviati da parte di amici dei social network, fai attenzione come fai per quelli ricevuti per email.
- Per evitare di rivelare gli indirizzi email dei tuoi amici, non consentire ai servizi di social networking di analizzare la tua rubrica.
- Scegli accuratamente i contenuti che pubblichi, considera che chiunque potrà stampare o salvare foto, immagini e testi pubblicati nel tuo profilo, e che tu ne perderai il controllo.
- Fai attenzione prima di installare un'applicazione. Adotta le stesse precauzioni di sicurezza che utilizzi con qualsiasi altro programma o file scaricato dal web.
- Controlla i dettagli delle fotografie che pubblichi, evita le foto dove appaiono, per esempio, la targa della macchina di famiglia o dello scooter, il nome della strada dove abiti e così via.
- Quando decidi di pubblicare on line la foto di un tuo amico o di un parente, o quando lo "tagghi" (inserendo il suo nome e cognome su quella foto), domandati sempre se stai violando la sua privacy. Nel

dubbio, chiedi il suo consenso alla pubblicazione.

Tieni presente che i principali social network comunicano le novità agli utenti in inglese e senza rivolgersi direttamente al singolo utente.

Il phishing e i ladri d'informazioni.

Il *phishing* è un'attività illegale che si verifica quando i criminali on line (*phisher*) fingono di essere organizzazioni legittime, come banche e società di carte di credito, per spingere gli utenti a rivelare i loro dati personali (nome utente e indirizzo, ma anche numeri di carte di credito, codici e password di conti in banca, codice fiscale, ecc.) per poi usarli a scopo improprio.

I *phisher* di solito cercano di ingannare l'utente inviando un'email, o attraverso pop-up o siti web fraudolenti in cui chiedono di verificare o re-inserire le proprie informazioni personali.

Possono anche chiederti di compilare un modulo on line, promettendo in cambio qualcosa di attraente come una vincita di denaro o una vacanza.

Tipicamente, le email di *phishing* contengono false dichiarazioni finalizzate a creare l'impressione che ci sia una minaccia immediata o un rischio di disabilitazione del tuo account.

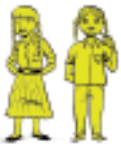
Ecco un esempio di *phishing* tra i più comuni: "Gentile utente, durante i regolari controlli sugli account non siamo stati in grado di verificare le sue informazioni. In accordo con le regole di [nome dell'azienda] abbiamo bisogno di confermare le sue reali informazioni. È sufficiente che lei completi il modulo che le forniremo. Se ciò non dovesse avvenire saremo costretti a sospendere il suo account."

Quasi tutti i *phisher* utilizzano un marchio, un nome e la grafica tipica dell'azienda imitata. Per questo, per non incorrere in spiacevoli situazioni, è sempre meglio diffidare di chiunque chieda informazioni su dati personali. Con le informazioni rubate, i *phisher* possono impersonare altri utenti e fare prelievi non autorizzati dal tuo conto in banca o utilizzarlo per acquisti on line. E possono anche vendere queste preziose informazioni a terzi.

Ricordati

- Tieni presente che nessuna banca ti chiederebbe mai via email la tua password.
- Diffida di qualunque email che richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento o altre informazioni simili.
- Diffida di email non personalizzate che contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento).
- Diffida di email che usano toni intimidatori, per esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente.
- Diffida di email che non riportano una data di scadenza per l'invio delle informazioni richieste.
- Non inserire mai i tuoi dati su finestre pop-up.
- Non cliccare su link presenti in email sospette o in pop-up che ti appaiono all'improvviso, perché potresti ritrovarti in un sito contraffatto, difficilmente distinguibile dall'originale, anche se sulla barra del browser l'indirizzo è apparentemente corretto.
- Modifica la password di accesso ai servizi on line almeno una volta al mese o al più presto se pensi che qualcuno ne sia a conoscenza.
- Quando inserisci dati riservati in una pagina web, assicurati che si tratti di una pagina protetta, diffidando da improvvisi cambiamenti nella modalità con cui viene chiesto di inserire i codici di accesso.

Occhio anche agli SMS. Il *mishing* (*SMS Phishing*) indica una truffa che viaggia con messaggi falsi via SMS. Il messaggio può invitare, per esempio, a collegarsi a un sito web, il più delle volte per scaricare qualcosa di gratuito. Una volta che ci si collega al sito falso o si scarica una suoneria o altro, il rischio di essere truffati è altissimo. Il *mishing* è spesso associato anche al *vishing* (*Voice Phishing*), la truffa attraverso chiamata telefonica: alcuni SMS, infatti, chiedono di comporre un numero telefonico dove una persona, o una voce registrata chiede informazioni personali e dati sensibili come la password per entrare nel servizio on line di gestione del conto corrente, della carta di credito o della prepagata.



Attenzione ai furti d'identità.

Rubare un'identità, su Internet, significa appropriarsi in modo subdolo di un'informazione individuale, per poi usare l'identità o i dati di una persona per compiere attività illecite.
Di solito il furto di identità avviene attraverso la ricezione di messaggi (SMS, email) che comunicano una vincita o invitano a collegarsi a un link che ti porterebbe a essere vittima di un'azione di *phishing* finalizzata ad acquisire i tuoi dati.
Per questo, in generale, non devi fornire le tue informazioni personali, soprattutto se non sei sicuro di sapere con chi sei in contatto, anche nel caso sostenga di essere incaricato dalla Polizia o da qualsiasi altra Organizzazione.
In questi casi devi chiedere sempre nome e recapito telefonico per poter effettuare tutte le verifiche del caso.

Ricordati

Diffida di qualunque email o sito web che ti offre qualcosa di troppo

bello per essere vero. Prima di fidarti, informati sulla credibilità del sito.

- Stai attento a dove lasci i dettagli della tua carta di credito on line o di quella dei tuoi genitori.
- Prima di cestinarli, distruggi i tuoi documenti personali come gli estratti conto della carta di credito e le bollette. Consiglia anche ai tuoi genitori di farlo.
- Monitora regolarmente il tuo conto in banca e l'estratto conto della carta di credito e segnala immediatamente eventuali attività sospette. Anche in questo caso, dai ai tuoi genitori questo pratico suggerimento.
- Prima di dare via o smaltire un vecchio computer o un telefonino, assicurati sempre che le informazioni siano state cancellate.
- Se trovi informazioni che ti riguardano pubblicate su Internet senza autorizzazione, richiedi che vengano rimosse.
- Se hai il sospetto che qualcuno abbia usato tue informazioni per acquistare qualcosa addebitandotene i costi, ricorda ai tuoi genitori che devono contattare il creditore, la banca, la compagnia telefonica e chiedere immediatamente di bloccare il conto e/o la carta di credito.
- Se qualcuno ha effettivamente usato in modo improprio le tue informazioni personali, informa i tuoi genitori. La cosa migliore da fare è rivolgersi a un consulente legale o alle associazioni difesa consumatori per ottenere consigli e assistenza su come agire per risolvere il problema, per verificare la tua situazione, ricevere informazioni e suggerimenti e, laddove necessario, anche tutela.

La parola d'ordine del download: scaricare? No, attenzione.

Non tutto quello che scarichi da Internet è sicuro al cento per cento. Per questo, per non incappare in pericoli, devi prestare attenzione anche ai tuoi *download*, perché alcuni file potrebbero danneggiare il tuo computer e intaccare i tuoi risparmi.

Bollette salate con le connessioni pirata.

Le connessioni pirata sono truffe ai danni di chi naviga su Internet realizzate attraverso programmi chiamati *dialer*. Questi programmi, a tua insaputa, fanno connettere automaticamente il computer con numeri a pagamento o con numeri internazionali o satellitari e naturalmente tutte le connessioni sono a carico dell'utente. Sono numeri a pagamento maggiorato quelli che iniziano con 892, 894, 895 e 899.
Senza che tu te ne renda conto, i *dialer* si possono installare nel tuo computer mentre navighi su molti dei siti Internet che propongono, per esempio, logo e suonerie, sfondi per il desktop, trucchi per videogiochi, foto e filmati, siti per adulti e, purtroppo, anche siti che invitano a scaricare gratuitamente programmi di musica.
Fai quindi sempre molta attenzione ai siti che promettono servizi gratuiti e che ti obbligano a installare software per poterli ottenere. In particolare devi controllare sempre i contenuti delle schermate che appaiono durante la navigazione e, nel dubbio, clicca su "no" o su "annulla", oppure cerca di uscire dal programma, soprattutto quando i messaggi non sono del tutto comprensibili.

Una volta che sospetti o scopri che un *dialer* si è installato nel tuo computer, utilizza i software disponibili nel tuo sistema operativo per individuarlo e rimuoverlo.

Occhio agli SMS.

Il pericolo di dover pagare bollette salate può arrivare anche via SMS. Il campanello d'allarme è sempre l'inizio del numero: quando in un messaggino ti chiedono di chiamare un numero che inizia con 89, devi essere consapevole che la tariffa sarà molto più cara di quella che applica il tuo operatore.

Ricordati

Diffida di messaggi simili a questi:

- "Abbiamo tentato di recapitarle una spedizione al suo indirizzo. Prego contattarci in orari d'ufficio al numero di telefono 89-9XX-XX-XX per nuova consegna".
- "Ti ho cercato alle ore 8.00 del xx/xx/20xx, è urgente. Per ascolto chiama da fisso al 89-9XX-XX-XX, info e costi su www.xxxxxx.biz".

Non lasciarti imbrogliare dagli spoofer.

Lo *spoofing* (dall'inglese *to spoof* che significa imbrogliare) è un attacco al tuo computer realizzato con una tecnica finalizzata a vincere le tue resistenze psicologiche, consentendo allo *spoofer* di entrare all'interno del sistema e di collocarci alcuni software dannosi.

Lo *spoofer* rinomina un file dandogli una doppia estensione. Quella reale (generalmente .exe, .hta, .bat, .hta, .ocx, .pif, .sys, .vbs e .wsf) che è quella dei file "eseguibili", ovvero dei file che contengono un programma che si installa una volta aperto il file, e una innocua tipo .gif, .jpg o .txt per far abbassare le tue difese e quelle dell'antivirus.
Vedendo allegato all'email un file che sembra un'immagine, un documento di testo o un semplice archivio *zip*, sarai spinto a scaricarlo, se non altro per curiosità. In questo modo, illudendoti di scaricare una innocua fotografia, potresti ritrovarti installato sul computer, per esempio, un *dialer* che ti farà inoltrare a tua insaputa chiamate verso numeri a tariffazione altissima.

Ricordati
Evita sempre di scaricare e aprire allegati inviati da sconosciuti.

Condividi con il file-sharing.

Letteralmente, il *file-sharing* (condivisione di file) è quel sistema che ti consente di condividere i tuoi file con altri utenti che si trovano sulla stessa rete o su Internet. Il *file-sharing* è la base di tutti quei programmi che permettono di scaricare file (mp3, video, programmi, immagini) dai computer di altre persone collegate a Internet. I programmi di *file-sharing* sono numerosissimi.
Nel linguaggio informatico, il *video-sharing* indica genericamente la condivisione di file video attraverso la rete per mezzo di programmi o siti Internet appositamente creati (per es: Youtube, Yahoo Video o Google Video).
Fai attenzione, perché i contenuti video protetti da diritto d'autore spesso non possono essere salvati direttamente sul computer, ma

solamente visualizzati con il proprio browser, e se ne sei in possesso, in molti casi non puoi diffonderli liberamente sul web.

Divertiti con i giochi on line.

I videogiochi in rete sono sempre più diffusi. Spesso, consentono di partecipare contemporaneamente allo stesso gioco con persone sparse per il mondo. In questi casi si parla di giochi in "modalità multiplayer", nei quali, effettivamente, l'elemento caratterizzante è rappresentato proprio dall'interazione con altri giocatori. Quando interagisci con giocatori sconosciuti, usa le cautele proprie della partecipazione a *blog*, *forum* e social network, perché puoi incappare negli stessi pericoli.
Nonostante il gran numero di giochi on line gratuiti, sono sempre più diffusi giochi (soprattutto per adulti) che prevedono l'uso di soldi, per esempio per acquisire nuove funzionalità o opzioni aggiuntive. In questi casi, ancora una volta, è necessario fare molta attenzione alle "modalità di pagamento".

Ricordati

- Non tutti i giochi sono accessibili ai minorenni. Se non lo sono c'è sempre un valido motivo, quindi prima di iniziare a giocare parlane con i tuoi genitori.
- Ricordati che non tutti i giochi sono gratis, nel caso i giochi siano a pagamento, i tuoi genitori devono esserne a conoscenza.

Proteggiti dai virus.

Su Internet, virus e programmi pirata sono estremamente diffusi. *Malware* (spesso utilizzato come semplice sinonimo del termine virus), *Trojan horse* (software che contengono istruzioni dannose che vengono eseguite nei computer all'insaputa dell'utente), *Backdoor* (letteralmente "porta sul retro", programmi che permettono un accesso "non autorizzato" al computer nei quali si autoinstallano) e *Hijacker* (in grado di far aprire l'apertura di pagine web non richieste) rappresentano tutti un pericolo. La caratteristica comune a questi programmi è quella di essere realizzati al solo scopo di creare danni all'interno del sistema informatico nel quale si annidano.
Per proteggere il tuo computer, riducendo notevolmente i rischi di infezione e salvaguardando tutte le tue informazioni, basta attenerti a una serie di semplici indicazioni.

Ricordati

- Installa e aggiorna regolarmente l'antivirus.
- Periodicamente, ricordati di scansionare il computer con l'antivirus per cercare di rimuove gli eventuali virus.
- Se il tuo software antivirus non include un software *anti-spyware*, installane uno separatamente e ricordati di aggiornarlo (gli *anti-spyware* sono software di protezione o di sicurezza in grado di rilevare e eliminare ogni eventuale minaccia al tuo computer).
- Accetta sempre gli aggiornamenti automatici dei principali software, assicurandoti che siano quelli originali.

- Usa estrema cautela quando apri allegati o clicchi su link contenuti in email, chat o social network. Se l'oggetto del messaggio o la domanda che ti viene posta ti suona strana, verifica che la persona in questione li abbia effettivamente inviati; se così non fosse, cancella gli allegati e chiudi la finestra della chat.
- Evita di fare clic su "Avanti", "Ok" o "Accetto" nei banner pubblicitari che ti promettono qualcosa, in pop-up o avvisi inattesi, in siti web che non sembrano regolari o in offerte sospette di rimozione di *spyware* o virus. Piuttosto chiudi subito la finestra o il browser (soprattutto quanto ti viene espressamente richiesto dai software di protezione del tuo computer).
- Stai attento alle offerte di musica, giochi, video e quant'altro ti sia offerto gratuitamente, perché potrebbe trattarsi di un'esca che contiene un virus.
- Fai attenzione ai falsi allarmi virus o a programmi gratuiti di scarsa affidabilità (anche se alcuni programmi gratuiti sono molto efficaci). Potrebbero garantire solo una protezione limitata o non offrirla affatto, o addirittura generare avvisi errati o fuorvianti tentando di attirarti in transazioni ingannevoli. Purtroppo non è facile individuarli e quindi, per essere sicuro, informati prima di scegliere e utilizza solo prodotti "originali", meglio se aggiornabili periodicamente (e in automatico) on line.
- Quando usi le USB cerca di essere cauto. Per ridurre al minimo il rischio di infettare il computer non devi collegare mai un'unità flash o una chiavetta USB di cui non conosci la provenienza o che è stata utilizzata da estranei. Soprattutto fai attenzione a non aprire file che ti sembrano sospetti.
- Proteggi la tua rete Internet: basta attivare una password o una chiave di protezione di rete in modo che gli estranei non possano accedere né alla rete né ai computer di casa.
- Se hai problemi con l'antivirus, prima di fare qualunque cosa ricordati di fare il backup dei dati che hai salvato sul disco fisso del computer.

Attenzione agli spyware.

Sono chiamati *spyware* i software in grado di monitorare ogni azione compiuta sul tuo computer: quali tasti hai digitato, le email che hai inviato, le tue conversazioni in chat, i file aperti ecc. Gli *spyware* registrano le informazioni relative alle tue scelte, ai tuoi gusti e alle tue preferenze senza che tu ne sia consapevole e senza che ti sia data la possibilità di concedere o negare il tuo consenso.
Queste informazioni vengono trasmesse, quasi sempre, a società che le riutilizzano per i più diversi scopi (prima di tutto commerciali).

Ricordati

Oltre ad accertarti di utilizzare programmi antivirus e *anti-spyware* affidabili, devi stare attento a non scaricare mai nulla in seguito a un avviso di un programma che non hai mai installato o che non riconosci. Se ti appaiono avvisi che ti promettono una maggiore protezione per il computer o di rimuovere virus, è molto probabile che succeda l'esatto contrario.

Difenditi con il firewall.

In rete ci sono tantissimi software *firewall* gratuiti che ti consentono di vigilare sullo scambio di dati tra il tuo pc, la tua rete locale e il mondo esterno.
Come un vero e proprio filtro, il *firewall* controlla il traffico della rete a cui sei connesso e consente di visualizzare sul tuo monitor i tentativi di intrusione e l'indirizzo telematico utilizzato per la violazione.

Ricordati

- Utilizza esclusivamente computer conosciuti e ritenuti affidabili e sicuri per eseguire alcune attività come per esempio l'accesso all'email.
- Usa un *firewall* Internet che si attivi automaticamente con l'accesso al sistema operativo.
- Ricordati di attivare nel tuo *firewall* Internet l'aggiornamento periodico automatico del programma.
- Non disattivare mai il *firewall*. Un *firewall* crea una barriera di protezione tra Internet e il tuo computer.
  Disattivandolo anche solo per un minuto, il computer rischia di essere infettato da malware.

Metti tutto al sicuro con il backup.

Il backup (e cioè la realizzazione di una copia di riserva o di sicurezza di tutti i dati presenti nella memoria del computer) è un'attività fondamentale: in caso di guasti, manomissioni, furti, sarai sempre sicuro di avere una copia dei dati.

Ricordati

- È buona norma eseguire periodiche operazioni di backup copiando almeno i dati più importanti su supporti ottici o magnetici (come CD-R e DVD), su hard disk portatili con collegamento esterno USB e su chiavette USB.
- Anche i telefonini e gli smartphone sono diventati strumenti importanti di archiviazione di dati perché contengono informazioni fondamentali come la rubrica telefonica e il calendario degli appuntamenti. È buona norma eseguire il backup anche su questi strumenti.

Il browser giusto per accedere a Internet.

Un browser è il software che ti consente di navigare sul web e rappresenta il primo filtro per proteggere la tua privacy on line e tutelare la tua sicurezza.
Sono browser, per esempio, Internet Explorer, Modzilla Firefox e Safari.
Il browser influenza la velocità con cui si apre una pagina su Internet, il livello di sicurezza durante la navigazione e la quantità dei dati condivisa sul web. In sintesi, influenza il tuo modo di usare il web.

Ricordati

Prima di scaricare un browser, verifica se è supportato dal tuo computer, tieni in considerazione la sicurezza che ti offre e le sue potenzialità d'uso e di adattamento alle tue esigenze.

Il pharming. Siti uguali, ma molto diversi.

Il *pharming* consiste nel far comparire sul browser di un utente una pagina web diversa da quella richiesta. In sostanza il *pharming* è una tecnica che consiste nel realizzare pagine web identiche a siti già esistenti (banche, assicurazioni, software-house, ecc.) in modo che l'utente sia convinto di trovarsi, per 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, i cyber criminali le recupereranno facilmente per poi utilizzarle ai propri fini.

Connessioni protette? Occhio all'https.

L'"http" (cioè l'*Hypertext Transfer Protocol*, letteralmente protocollo di trasferimento di un ipertesto) è il principale sistema per la trasmissione "in chiaro" d'informazioni sul web, gestito dal *World Wide Web Consortium* (W3C). Dal momento che tutto il traffico "http" è visibile a tutti, sono state sviluppate diverse alternative per garantire differenti livelli di sicurezza, in termini di cifratura del linguaggio, verifica di integrità del traffico, autenticazione del server e autenticazione dell'utente. L"https" è invece usato proprio nei casi in cui è necessario trasferire dati riservati impedendo l'intercettazioni dei contenuti. È importante usare questo sistema proprio per situazioni che richiedono particolari esigenze in ambito di sicurezza come per esempio il pagamento di acquisti on line o l'accesso alla posta elettronica.

Ricordati

- Ricordati che i filtri *anti-phishing* segnalano i siti web sospetti e quindi ti proteggono anche dal *pharming*.
- Se necessario verifica che il sito usi sistemi di crittografia, e cioè misure di sicurezza che codificano i dati che attraversano Internet. Sono indicatori di un sito crittografato il simbolo di un lucchetto chiuso (il lucchetto potrebbe trovarsi anche nell'angolo in basso a destra della finestra) e l'indirizzo che compare nella barra degli indirizzi del browser che comincia con "https://" e non con "http://".

Le tue informazioni, un bene prezioso.

Tutte le volte che crei un account, acquisti qualcosa on line, ti iscrivi a un concorso, partecipi a un sondaggio, scarichi un software gratuito o semplicemente navighi sul web, sei costretto a trasmettere informazioni. Nella maggior parte dei casi, queste informazioni sul tuo conto vengono raccolte dalle aziende semplicemente per indagini di mercato o per conoscere meglio i gusti dei propri utenti. Alcuni siti, invece, tengono traccia delle pagine web che visiti e dei tuoi clic, ma senza collegare il dato al tuo nome. Purtroppo, però, ci può essere anche chi raccoglie i tuoi dati per venderli o usarli per macchiare la tua immagine, molestarti, o rubarti l'identità.

Ricordati

- Non condividere più informazioni del necessario.
- Evita di "postare" on line qualcosa che non vuoi rendere pubblico.
- Riduci al minimo i dettagli che identificano te o il luogo in cui ti trovi.
- Tieni segreti i tuoi nomi utente e password.
- Condividi l'indirizzo email o l'identità di messaggistica istantanea principale solo con persone che conosci o con organizzazioni affidabili.
- Evita di indicare il tuo indirizzo di casa.
- Nei moduli di iscrizione inserisci solo le informazioni obbligatorie (spesso contrassegnate con un asterisco).

L'importanza della password.

La password è solitamente associata ad uno specifico nome utente (in inglese *username*) e serve per identificare in modo inequivoco

un soggetto (comunemente si parla di *login*). È sempre consigliabile scegliere di utilizzare password complesse lunghe almeno 14 caratteri, formate da lettere (maiuscole e minuscole, numeri e simboli) facili da ricordare per te ma difficili da indovinare per gli altri. È consigliabile aumentare il più possibile la varietà dei caratteri presenti nella password, utilizzando l'intera tastiera, non solo le lettere e i caratteri usati più frequentemente.

Ricordati

- Non creare password utilizzando: parole di senso compiuto; parole scritte al contrario e abbreviazioni; sequenze o caratteri ripetuti (per es: 12345678, 222222, abcdefg) o lettere adiacenti sulla tastiera (per es: "qwerty"); informazioni personali (nome, compleanno, numero di patente o informazioni analoghe).
- Tieni segrete le tue password a tutti, anche agli amici. Registrale o annotale, ma custodiscile con attenzione.
- Non utilizzare la stessa password per tutti i siti. Se qualcuno dovesse impadronirsene, tutte le altre informazioni che protegge saranno a rischio.
- Non conservare le password in zaini o portafogli. Non lasciare traccia delle password in luoghi in cui non si lascerebbero mai le informazioni riservate. Non memorizzare le password in file sul computer. È il primo posto in cui vanno a guardare i criminali.
- Non inviare la password tramite posta elettronica, anche se in risposta a una richiesta arrivata via email. Eventuali messaggi di posta elettronica che richiedono la password o richiedono di visitare un sito web per verificare la password possono rappresentare una truffa.

Impara a usare i computer pubblici.

Scuole, biblioteche, Internet cafè, aeroporti e copisterie sono luoghi nei quali capita spesso di connettersi a un computer pubblico e quindi accessibile a tutti. Per utilizzarlo in sicurezza basta seguire alcune semplici regole, perché non è possibile sapere se un computer pubblico è protetto o al contrario è già affetto da un virus. Inoltre, i dati del *login* potrebbero restare memorizzati sul computer e un altro utente dopo di te potrebbe accedere con i tuoi account.

Ricordati

- Non salvare mai i tuoi dati di accesso. Esci sempre dai siti web facendo clic su "chiudi sessione" o "esci". Chiudere il browser o digitare un altro indirizzo non è sempre sicuro.
- Disabilita la funzionalità di memorizzazione delle password. Molti programmi (soprattutto i siti di social networking, web mail e i programmi di messaggistica istantanea) includono funzionalità di accesso automatico che salvano il tuo nome utente e password.
- Non lasciare incustodito il computer con informazioni sensibili sullo schermo. Se devi allontanarti dal computer pubblico, esci da tutti i programmi e chiudi tutte le finestre.
- Elimina i file temporanei e la cronologia Internet.
- Fai attenzione a chi osserva il monitor o la tastiera mentre scrivi le tue password.
- Evita di fare acquisti da un computer pubblico o con qualsiasi dispositivo (per esempio, un laptop o un telefono cellulare) collegato a una rete *wireless* pubblica usando una carta di credito.

Paga on line in tutta sicurezza

Per acquistare su Internet, scegliere le carte prepagate al posto delle carte di credito riduce il rischio che qualcuno possa prelevare i tuoi soldi. Le carte prepagate possono essere di due tipi: usa e getta e ricaricabili. Il meccanismo di queste ultime è simile a quello delle ricaricabili dei cellulari: acquistata la carta la prima volta, è possibile in seguito ricaricarla tutte le volte che si desidera e con il credito che ti serve. Puoi effettuare le ricariche anche allo sportello automatico e, in alcuni casi, a distanza (via Internet o telefono) o in alcune ricevitorie autorizzate. Se la carta di credito o la prepagata viene persa o rubata il proprietario può bloccarla e renderla inutilizzabile in qualunque momento, chiamando un numero verde e comunicando il furto alla banca. È sempre oppurtuno denunciare immediatamente il furto o lo smarrimento alle Forze dell'Ordine. Perdere una carta di credito è molto rischioso, perché non è necessario digitare nessun PIN per effettuare pagamenti.

I contratti possono essere stipulati da minorenni?

I contratti stipulati da minorenni sono validi ma annullabili. Ciò dà il diritto ai genitori di pretendere il rimborso della somma spesa. Questo principio non trova però applicazione nei casi in cui il minorenne abbia taciuto o falsificato la propria età. Il semplice fatto di non indicare l'età corretta non viene considerato come elemento sufficiente per annullare il contratto d'acquisto.

Cosa devi sapere se sei minorenne?

Ricorda che non puoi acquistare on line e che, se lo fai, devi sempre concordare l'acquisto con i tuoi genitori.
Quando compri on line, il venditore naturalmente non ha la possibilità di vederti e di verificare se hai più di 18 anni. Deve fidarsi delle informazioni che gli dai, ma questo lo tutela anche dai tuoi eventuali inganni. Se compri qualcosa all'insaputa dei tuoi genitori, la restituzione della cifra pagata sarà quasi impossibile (soprattutto se hai falsificato il tuo nome usando la carta di credito di un adulto).

Attento alle aste on line!

Attratto dalla possibilità di risparmiare o di acquistare qualcosa che vicino casa o in altri negozi on line non si trova facilmente, è facile lasciarti affascinare dai siti di aste on line dove puoi trovare veramente di tutto. Il funzionamento è semplice ed è lo stesso delle aste tradizionali: un oggetto viene messo all'asta a un prezzo minimo fissato, la cosiddetta "base d'asta", al di sotto della quale non sarà assegnato. Da quel momento si comincia a rilanciare, e chi conclude con l'offerta più elevata rispetto alla "base d'asta" risulta vincitore e si vede assegnato l'oggetto. Oltre a un valore minimo, esiste anche un altro vincolo nelle contrattazioni rappresentato da un tempo massimo di durata dell'asta, superato il quale le contrattazioni si fermano e vengono valutate le condizioni d'assegnazione. Il prodotto, naturalmente, dovrebbe essere corredato anche da un'esauriente descrizione con i dettagli utili per valutarlo in modo adeguato e quindi fissare il prezzo della tua offerta. Il sistema informatico di contrattazione, general-

mente, crea messaggi di posta elettronica automatici per informare i partecipanti sullo stato dell'asta. Alla chiusura della contrattazione ti verranno forniti tutti gli elementi per concludere l'acquisto e redigere un contratto alle condizioni stabilite dall'asta (prezzo, quantità, caratteristiche del prodotto). Le aste on line sono una realtà ormai consolidata in tutto il mondo. Come in quelle tradizionali è l'acquirente a decidere il prezzo che è disposto a pagare per un oggetto, quindi avviene una vera e propria contrattazione.
Ma anche in questo caso, soprattutto per i meno esperti, è bene prestare grande attenzione per non incappare in fastidiosi inconvenienti.

Ricordati

- I minorenni non possono comprare on line. Se vuoi fare un acquisto, informa sempre almeno un genitore e se chiedi di utilizzare la sua carta di credito, paga sempre in sua presenza!
- Prima di partecipare all'asta, insieme a uno dei tuoi genitori controlla sempre le condizioni di contrattazione, quelle relative alla chiusura dell'asta, i tempi di svolgimento e ogni altra caratteristica determinata dal venditore o prevista dal sistema.
- Leggi attentamente anche tutte le clausole del regolamento dell'asta, i tipi di pagamento, la percentuale che andrà alla casa d'aste, il metodo di spedizione e i tempi di consegna che dovrà essere almeno indicativamente segnalato.
- Prima di procedere all'acquisto è consigliabile richiedere sempre ulteriori foto, proprio perché in un'asta via Internet non è quasi mai consentito esaminare l'oggetto di persona.
- Avvisa gli altri utenti lasciando un commento di feedback sincero.
- Non acquistare o vendere oggetti contraffatti.
- Se non ricevi l'oggetto acquistato o l'oggetto ha caratteristiche diverse rispetto a quello descritto on line, puoi inviare un reclamo allo spazio sicurezza presente nel sito.

Cosa sono i gruppi di acquisto on line?

Si tratta di siti dove più persone hanno la possibilità di comprare, a prezzi scontati, oggetti o servizi, come cene, massaggi, trattamenti estetici, abbonamenti in palestra e così via. Ogni giorno sono presentate offerte suddivise per città e che mostrano il valore dello sconto. Affinché l'offerta si concretizzi, è necessario che un numero minimo di persone la sottoscrivano entro un certo periodo di tempo definito dal venditore. Se si raggiunge la soglia minima richiesta dall'offerta, si paga il prezzo del coupon e lo si riceve on line, acquisendo il servizio acquistato. Al di là dei principali operatori esistono, però, una gran varietà di siti clone non tutti caratterizzati dalla stessa sperimentata affidabilità.

Ricordati

- Se sei minorenne, ricorda che non puoi acquistare on line e che, se lo fai, devi sempre avere il permesso dei tuoi genitori.
- Per fare acquisti o operazioni su Internet, di solito ti viene richiesto dal sito interessato solo il numero della carta di credito (o della prepagata), la relativa data di scadenza e il codice "CVV" e mai le password del numero di conto o della carta.
- Stai attento alle offerte che sembrano troppo convenienti per essere vere, alle false proposte di lavoro, ai messaggi che ti annunciano la vincita di una lotteria, o a richieste di aiuto da parte di uno sconosciuto che ha bisogno di trasferire dei fondi.
- Se compri su Internet fallo su siti conosciuti e che godono di credibilità.
- Dubita di siti sconosciuti che promuovono sconti troppo allettanti.
- Verifica che i siti in questione utilizzino protocolli di sicurezza che permettano di identificare l'utente. Il più diffuso è il Secure Socket Layer (SSL).
- Fai uso, per quanto possibile, delle soluzioni on line o via SMS che

le banche mettono a disposizione per controllare - quasi in tempo reale - le tue spese, in modo da bloccare tempestivamente la carta qualora non dovessi riconoscere una spesa addebitata.

- Nei casi dubbi contatta i numeri telefonici verdi (gratuiti) delle banche o delle società che hanno emesso la carta di credito.
- Prediligi il computer di casa perché uno pubblico potrebbe essere meno sicuro nel proteggere i dati della tua carta.
- Controlla che il venditore, oltre all'indirizzo di posta elettronica, abbia anche una sede con un indirizzo reale e un numero di telefono a cui rivolgersi in caso di problemi legati all'acquisto del prodotto.
- Cerca sempre di pagare con carte prepagate.
- Verifica che sulla proposta di contratto siano presenti le informazioni sul diritto di recesso e sulle modalità per esercitarlo.
- Salva e stampa la pagina di riepilogo dell'acquisto compiuto.
- Prima di acquistare un prodotto o di usufruire di un servizio in Internet, verifica le politiche di vendita e le condizioni di recesso (tramite le informazioni evidenziabili sulle caratteristiche del prodotto), i tempi di consegna, i costi e le spese di spedizione.
- Verifica che si tratti di una vendita a prezzo fisso. Nel caso di aste le garanzie per chi acquista sono minori.
- Presta particolare attenzione quando compri su un sito straniero, in quanto le condizioni di acquisto potrebbero essere differenti e i tuoi diritti meno tutelati.
- Controlla che ci siano garanzie per il trattamento dei dati personali.
- Non fornire i tuoi dati personali se non sei sicuro dell'uso che ne sarà fatto e di quanto saranno protetti.

Cosa si può fare in caso di uso fraudolento della carta di credito o prepagata?

Se pensi che qualcuno non autorizzato abbia usato la tua carta di credito devi immediatamente informare i tuoi genitori e fare una segnalazione alla tua banca per ottenere il rimborso. Contestualmente i tuoi genitori dovranno presentare una denuncia presso il più vicino posto di Polizia o presso una stazione dei Carabinieri.

Cosa si deve fare se non si riconoscono alcune spese addebitate?

Se pensi di non dover pagare somme di denaro addebitate da un venditore, riferiscilo subito ai tuoi genitori e suggerisci loro di contestare le spese inviando un reclamo alla banca.

A chi segnalare i comportamenti scorretti in rete?

Siti web dai contenuti illeciti o contatti con persone dai comportamenti sospetti devono essere segnalati alla Polizia delle Comunicazioni (www.poliziadistato.it). Nella maggior parte dei casi il tentativo di truffa inizia con l'invio di una email alla potenziale vittima.

I navigatori più esperti usano molta cautela nell'interagire con gli sconosciuti evitando così brutte sorprese. In ogni caso, se sospetti un tentativo di truffa, informa immediatamente la Polizia delle Comunicazioni.

A chi rivolgersi per tutelare la privacy in Internet?

La normativa vigente in materia di tutela della privacy prevede che i tuoi dati personali possano essere trattati da altri solo dopo aver ricevuto il tuo consenso esplicito. Per saperne di più puoi consultare il sito www.garanteprivacy.it.

Sempre

- Assicurati di installare un programma antivirus e aggiornalo regolarmente.

- Tieni aggiornato il sistema operativo del tuo computer.

- Assicurati che le tue password restino segrete e conservale in un luogo sicuro. Cambiale regolarmente.

- Ricordati di fare regolarmente il backup dei dati più importanti e archiviali in un posto sicuro.

- Assicurati di usare una connessione protetta quando fai shopping on line. Accertati di poterti fidare dell'azienda da cui acquisti.

Mai

- Non aprire allegati inviati da persone che non conosci, anche quelli apparentemente innocui potrebbero danneggiare il tuo computer.

- Non rispondere alle email in cui ti chiedono informazioni personali e riservate. Nessuna azienda onesta ti chiederebbe mai di farlo.

Glossario

Account (profilo o identità) insieme dei dati personali e dei contenuti caricati su un sito Internet o su un social network.

Anti-spyware programma realizzato per prevenire e rilevare i programmi *spyware* indesiderati e per rimuoverli dal computer.

Antivirus software software che analizzano tutti i file e i programmi individuando i virus e rimuovendoli dal computer.

Banda larga connessione che garantisce alta velocità di accesso e di *download* su Internet.

Browser software che consente di visualizzare le pagine Internet e quindi di navigare in rete.

Chat sistema di messaggistica testuale istantanea. Il dialogo on line può essere limitato a due persone o coinvolgere un ampio numero di utenti.

Condizioni d'uso *(user agreement o terms of use)* regole contrattuali che l'utente deve accettare per accedere a un servizio.

Dialer particolare tipo di virus che nei collegamenti non ADSL, disconnette la normale connessione modem per riconnettersi, a nostra insaputa, a un numero telefonico a pagamento.

Email virus un virus che viaggia per email come allegato ai messaggi e che una volta aperto si replica da solo inviandosi auto-

maticamente a tutti i contatti della rubrica.

Fake falsa identità assunta su Internet.

Firewall come un muro di protezione, impedisce ai programmi malevoli di entrare nel computer mentre si è connessi a Internet.

Loggarsi (autenticarsi) accedere a un sito o servizio on line inserendo le proprie credenziali (*username* e password).

Malware termine generico per "software malevolo", che comprende virus, *worm*, Trojan horse e *spyware*.

Meccanismo di pagamento sicuro metodo di pagamento che assicura che i dati personali che intercorrono tra l'acquirente e il commerciante on line siano protetti.

Nickname pseudonimo.

On line stato del computer connesso a Internet.

Password sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo a una risorsa infomatica.

Pharming truffa che consiste nel far comparire sul browser di un utente una pagina web identica a quella richiesta ma non originale, allo scopo di rubare informazioni e dati personali dell'utente (vedi *phishing*).

Phishing attività illegale che si verifica quando i criminali on line (*phisher*) fingono di essere organizzazioni legittime per spingere gli utenti a rivelare i loro dati personali (tra cui numeri di carte

di credito, password di conti in banca, codice fiscale, ecc.) per usarli a scopo improprio.

Postare pubblicare un messaggio (*post*) - non necessariamente di solo testo - all'interno di un *blog*, *forum*, ecc.

Privacy policy (tutela della privacy o informativa) pagina esplicativa predisposta dal gestore del servizio contenente informazioni su come saranno utilizzati i dati personali inseriti dall'utente, su chi potrà usare tali dati e quali possibilità si hanno di opporsi al trattamento.

Reti senza fili *(Wi-Fi o Wireless LAN)* reti che consentono ai computer di comunicare tra loro utilizzando un collegamento radio simili ai telefoni cordless.

Router dispositivo che collega il computer alla connessione a Internet.

Scaricare (fare il *download*) salvare sul proprio computer o su una memoria esterna documenti presenti su Internet.

Server computer connesso alla rete utilizzato per offrire un servizio. Sono noti come "client" i computer che gli utenti utilizzano per collegarsi al server e ottenere il servizio.

Sistema operativo base software del computer su cui tutti i programmi vengono eseguiti.

Sito web sicuro sito web crittografato in modo tale da assicurare che i dati che intercorrono tra l'utente e il sito web restino riservati. Sono siti sicuri, per esempio, quelli in modalità https.

Spamming invio indiscriminato di messaggi non richiesti, generalmente tramite posta elettronica.

Spyware software che raccoglie segretamente dati, informazioni e dettagli personali sul tuo computer trasmettendoli, sempre a tua insaputa, attraverso la tua connessione Internet.

Tag "etichetta virtuale", parola chiave associata a un contenuto digitale.

Taggare connotare un file, un contenuto ecc. con una "etichetta virtuale" (*tag*) a un file.

Trojan Horse software che fingendo di essere un innocuo programma (per esempio un gioco), danneggia il computer e i dati nel momento in cui viene eseguito sul computer.

Uploadare caricare un documento di qualunque tipo (audio, video, testo, immagine) on line.

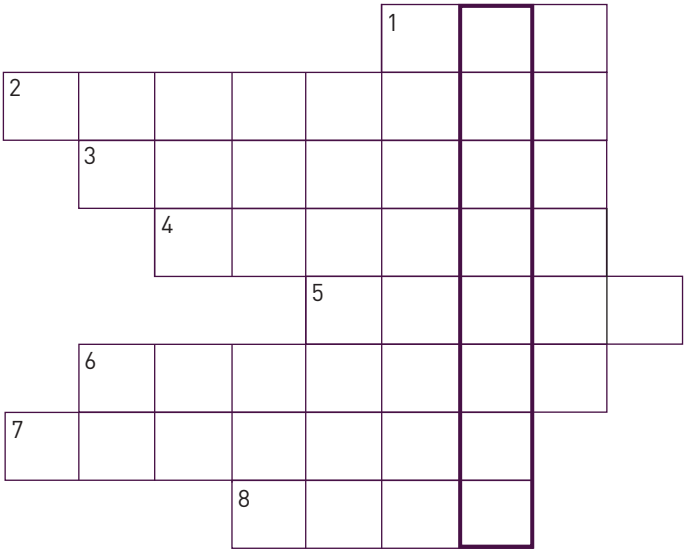
Virus piccole parti di software che attaccano i programmi sul computer, sono in grado di replicarsi per infettare altri computer danneggiando, copiando o rubando dati.

Vishing combinazione di voce e *phishing*, in cui la vittima riceve un messaggio di testo per email o una telefonata in cui qualcuno, fingendo di essere la sua banca o la società di carte di credito, chiede di fornire informazioni personali.

VoIP (Voice Over Internet Protocol) modo di comunicare usando Internet al posto della linea telefonica tradizionale.

WPA (Wi-Fi Protected Access) standard di protezione wireless che impedisce agli utenti non autorizzati di connettersi alla rete wireless.

Cruciverba



1 Personal Identification Number 2 La manipolazione di indirizzi web 3 La "carta" utilizzata negli acquisti 4 Connessioni pirata 5 Luoghi virtuali di discussione 6 Condivisione di file 7 Virus che raccoglie segretamente dati, informazioni e dettagli personali sui pc 8 Un messaggio all'interno di un blog o social network

1 pin 2 pharming 3 credito 4 dialer 5 forum 6 sharing 7 spyware 8 post

Finito di stampare a gennaio 2012
presso la tipografia Graficart s.n.c. - Formia (LT)