GUIDA ALLA SICUREZZA INFORMATICA

NET & WEBBY

IN VIAGGIO PER LA RETE

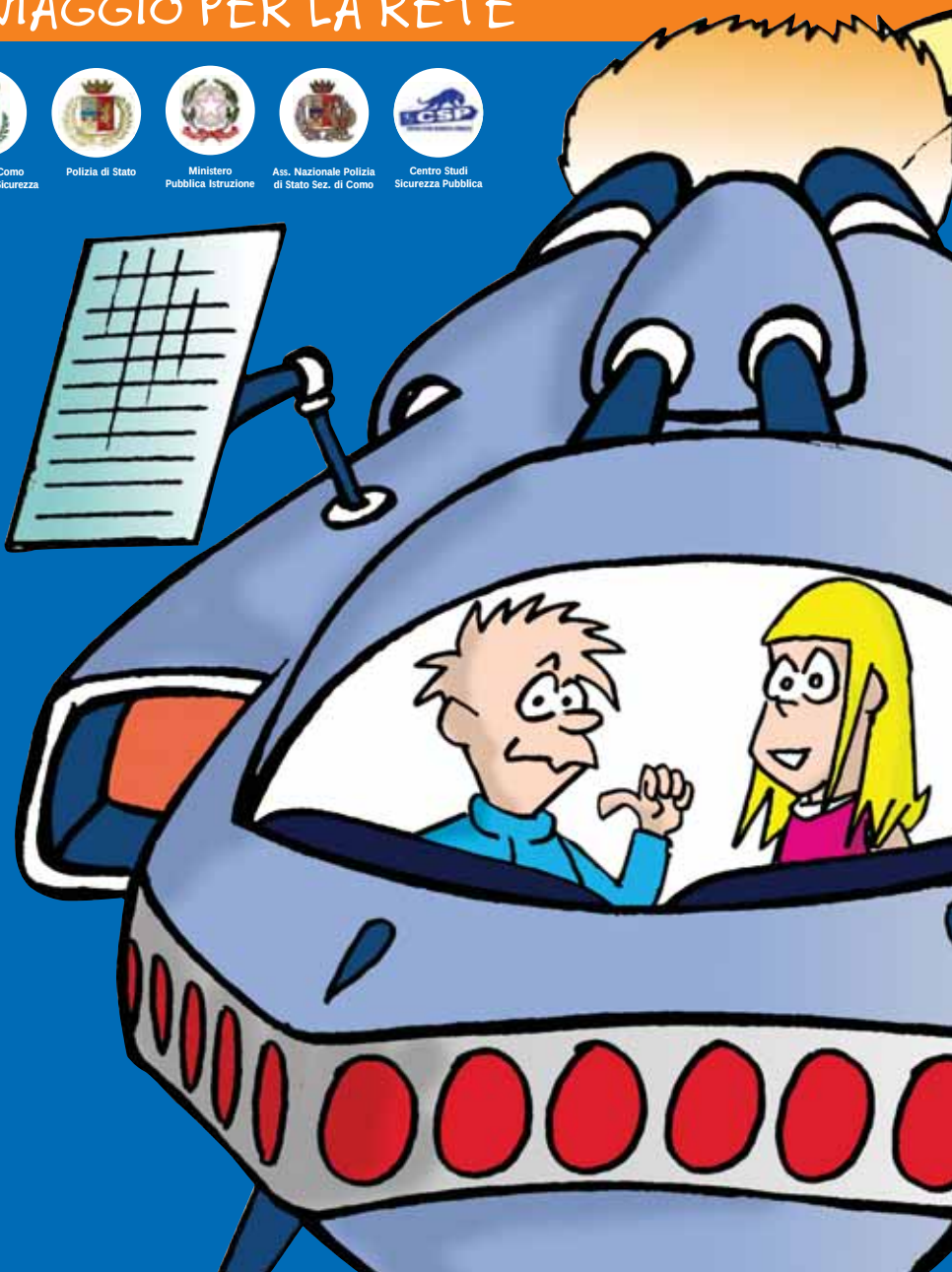
Provincia di Como
Assessorato alla Sicurezza

Polizia di Stato

Ministero
Pubblica Istruzione

Ass. Nazionale Polizia
di Stato Sez. di Como

Centro Studi
Sicurezza Pubblica



PUBBLICAZIONE REALIZZATA DA:

PROVINCIA DI COMO
ASSESSORATO ALLA SICUREZZA E POLIZIA LOCALE

POLIZIA POSTALE E DELLE COMUNICAZIONI
COMPARTIMENTO PER LA LOMBARDIA

Presentazione

Negli ultimi anni la Provincia di Como ha svolto una crescente azione mirata sia al finanziamento delle tecnologie applicate alla pubblica amministrazione (c.d. e-government), che alla realizzazione di infrastrutture al passo coi tempi, in grado di offrire servizi avanzati e collegamenti a "banda larga" anche nelle aree che tradizionalmente ne erano prive.

Il rapido diffondersi di nuovi strumenti tecnologici, tuttavia, se da un lato ha consentito processi inimmaginabili solo qualche anno addietro, dall'altro lato, ha offerto nuove opportunità criminali, figlie di quelle stesse tecnologie che rendono la vita di ogni giorno estremamente comoda.

Tale considerazione ha offerto lo spunto per ideare e realizzare la presente guida per la sicurezza informatica.

I nostri due protagonisti, Net & Webby, offriranno ai lettori informazioni utili e consigli preziosi circa gli imprevisti ed i rischi che l'uso di alcuni strumenti tecnologici può comportare.

Il percorso che si intende seguire è tracciato nel solco dell'approccio di carattere preventivo alla lotta alla criminalità, di cui per prime le Forze di Polizia a competenza generale si sono fatte promotrici rinnovando profondamente alcune strategie di intervento operativo, e che, si ritiene, possa essere efficacemente perseguito anche grazie ad interventi realizzati attraverso la collaborazione tra le diverse Istituzioni.

La Polizia Postale e delle Comunicazioni dal canto suo, forte dell'importanza della sicurezza partecipata, garantisce il corretto funzionamento del-

le reti di telecomunicazioni con un'organizzazione moderna e capillare presente sul territorio, con operatori ad alto livello di specializzazione e con l'istituzione di unità funzionali dedicate ad aspetti singoli del crimine informatico (CNAIPIC-Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, Centro Nazionale per il Contrasto della Pedopornografia sulla Rete Internet ed il Commissariato online).

L'impegno di questa specialità della Polizia di Stato è rivolto anche all'analisi ed alla ricerca di strumenti investigativi del tutto innovativi, sia in termini di hardware che di software, che consentano all'operatore di individuare, enucleare e vanificare le forme di criminalità emergenti delle quali le nuove tecnologie costituiscono purtroppo una parte essenziale.

Le strategie di intervento prevedono la suddivisione degli utenti-vittima nelle tre categorie principali di "utenti-infrastrutturali" (enti pubblici o privati detentori di risorse critiche per il paese), "utenti-qualificati" (aziende della Net Economy) e "utenti singoli" (utilizzatori finali), a cui corrispondono peculiari attività investigative.

Tuttavia le azioni si basano sempre sul presupposto che è impossibile presidiare Internet senza la collaborazione degli attori che vi partecipano e che diminuirne i rischi vuol dire aumentare il livello di coinvolgimento di coloro che usano la Rete per fini sociali, politici e remunerativi.

Questa guida è pienamente aderente a questi principi e permetterà sicuramente di aumentare la cultura della sicurezza informatica.

Anche l'A.N.P.S. (Associazione Nazionale Polizia di Stato di Como) e il C.S.P. (Centro Studi Sicurezza Pubblica di Brescia) hanno sostenuto con forza questa iniziativa perché credono molto nello sviluppo e nell'evolu-

zione nell'era del computer, ma nello stesso tempo, per esperienza, conoscono i rischi e le insidie che si nascondono dietro ad ogni collegamento ad Internet e soprattutto le difficoltà che incontrano i giovani e adulti quando utilizzano la Rete.

Entrambi si adopereranno con sinergia affinché la famiglia, la scuola e le istituzioni preposte si impegnino fino in fondo a diffondere la cultura della legalità, sensibilizzando i giovani di questa società postmoderna, promuovendo incontri e confronti atti a prevenire questi tipi di reati.

É opinione di tutti gli enti coinvolti in questa iniziativa che la guida debba essere un manuale esplicativo da divulgare in ogni nucleo familiare e che ogni insegnante la potrà utilizzare quotidianamente come strumento idoneo non solo per prevenire i reati informatici, ma soprattutto, per educare alla legalità e ad un migliore utilizzo dello strumento tecnologico.

Insomma, prevenire significa anche informare ed intervenire positivamente sull'opinione pubblica in modo che non avverta più la scoraggiante sensazione di insicurezza che sovente attaglia gli animi dei consociati, ed è questo l'obiettivo ultimo che si propone il presente lavoro.

Auguriamo pertanto una proficua lettura.

Dott. Roberto Zanetti

Dott. Salvatore Rossi

Cons. Naz. Marcello Chirulli

Dott. Maurizio Marinelli

INDICE

1

INIZIARE BENE

I computers e più in generale gli strumenti tecnologici perfezionati negli ultimi anni, quotidianamente ci permettono di fare con semplicità cose inimmaginabili solo qualche tempo addietro, quando i nostri genitori erano ragazzi come noi.

Oggi attraverso Internet possiamo trovare informazioni su qualunque argomento ci appassioni, come ad esempio un viaggio o un luogo ove trascorrere un periodo di studio o, più banalmente, un oggetto da acquistare. Possiamo creare un sito o un blog tutto nostro, o semplicemente surfare il web.

La tecnologia ci permette di comunicare con chi si trova dall'altro capo della Terra offrendoci persino la possibilità di vedere con chi stiamo parlando; basta un'email per scambiare in un clic con chi vogliamo libri interi o le nostre canzoni preferite; sul web possiamo conoscere tanta gente simpatica, chattare, scambiarci mille idee o giocare online con ragazzi che chissà quale lingua parlano.

Oggi possiamo anche portare nella tasca dei pantaloni un'intera collezione di dischi da ascoltare in qualunque momento, telefonare senza gettoni ovunque siamo, o fare fotografie da trasmettere in un istante a chi ci pare.

Possiamo liberamente cogliere tutte le opportunità che ci vengono offerte da queste incredibili tecnologie, tuttavia è importante sapere che insidie e pericoli reali sono presenti anche nel mondo virtuale.

Questa breve guida da condividere con gli adulti ha lo scopo di offrire una serie di consigli che, se osservati, possono scongiurare il rischio di rimanere vittima di situazioni spiacevoli o di vero e proprio pericolo.

Sfoglia le pagine che seguono e Net e Webby ti aiuteranno a scoprire quali!

COLLOCARE IL COMPUTER

...ma attenzione alla postura

Il computer non deve essere inteso come un semplice giocattolo, magari solo più costoso di tutti gli altri, ma come uno strumento a disposizione di tutta la famiglia.
Per questa ragione è meglio collocarlo in un ambiente comune della casa e non isolarlo nella nostra cameretta. In questo modo potremo condividerlo con mamma e papà ed imparare con loro ad usarlo al massimo delle sue potenzialità.
Il computer è uno strumento complesso che deve essere utilizzato rispettando alcune semplici ma importanti regole.

PRESTATE ATTENZIONE A

Il computer, che passione!!
A volte capita di passarci le giornate intere! E poi che mal di testa...
L'uso eccessivo e prolungato di computer o videogiochi può essere causa di malesseri fisici, quali stanchezza visiva, bruciore agli occhi, mal di testa, dolore al collo o alla schiena, che sono tutti sintomi che possiamo accusare dopo una prolungata permanenza davanti al monitor o al televisore.
Per questo motivo, è essenziale creare un ambiente adatto alla loro collocazione ed è necessario assumere una postura corretta mentre li si utilizza.

CONSIGLI PER I RAGAZZI

- Usa una sedia che sostenga la parte bassa della schiena
- Evita di stare sdraiato per terra
- Non mettere sotto la scrivania oggetti che impediscano i movimenti delle gambe
- I piedi devono appoggiare per terra, altrimenti usa un supporto
- Sistema tastiera e mouse alla stessa altezza dei gomiti
- Stai a 50-70 cm dal monitor
- Fai delle frequenti pause (anche se brevi)

CONSIGLI PER I GENITORI

- Colloca il computer in una stanza comune della casa, evitando di isolarlo nella cameretta; così potrai vedere come viene utilizzato
- Non considerare il computer come un gioco del tuo ragazzo, non lo è. Fai sì che diventi uno strumento condiviso da tutta la famiglia
- Impara il più possibile ad utilizzare il computer ed apprendi il linguaggio delle nuove tecnologie. Per poter dare consigli devi sapere di cosa si sta parlando, altrimenti non ti verrà dato ascolto
- Sistema le apparecchiature su di una scrivania chiara, preferibilmente non bianca
- È bene schermare la luce esterna con delle tende, mentre la luce artificiale non deve creare riflessi sullo schermo

CONFIGURARE IL COMPUTER

Antivirus e firewall

Il computer è uno strumento prezioso che utilizziamo quotidianamente per studiare o giocare e che i nostri genitori utilizzano per lavorare.
Come tutte le cose preziose deve essere custodito con il massimo riguardo.
A quanti sarà capitato di fare una complessa ricerca o di lavorare alacremente per lungo tempo al computer, per poi veder svanire in un attimo ore ed ore di faticoso lavoro a causa di una distrazione, di un mancato salvataggio o di un crash del sistema.
Molto spesso, al di là delle intenzioni dei soliti burloni o dei veri criminali informatici, siamo vittime di situazioni spiacevoli a causa della nostra stessa disattenzione.
Il primo potenziale aggressore informatico siano dunque noi stessi.

PRESTATE ATTENZIONE A

È importante tenere il sistema operativo sempre aggiornato, installare un buon programma antivirus e configurare adeguatamente i firewall.
Le impostazioni di sicurezza non devono essere modificate nemmeno a seguito dell'installazione di programmi p2p, poiché questi software incrementano l'esposizione al rischio di "infezioni" elettroniche.
Eventuali connessioni wi-fi devono essere protette per evitare accessi di persone non autorizzate.
Piccoli accorgimenti possono garantire un migliore funzionamento complessivo del computer ed assicurare la sicurezza dei dati in esso immagazzinati.

CONSIGLI PER I RAGAZZI

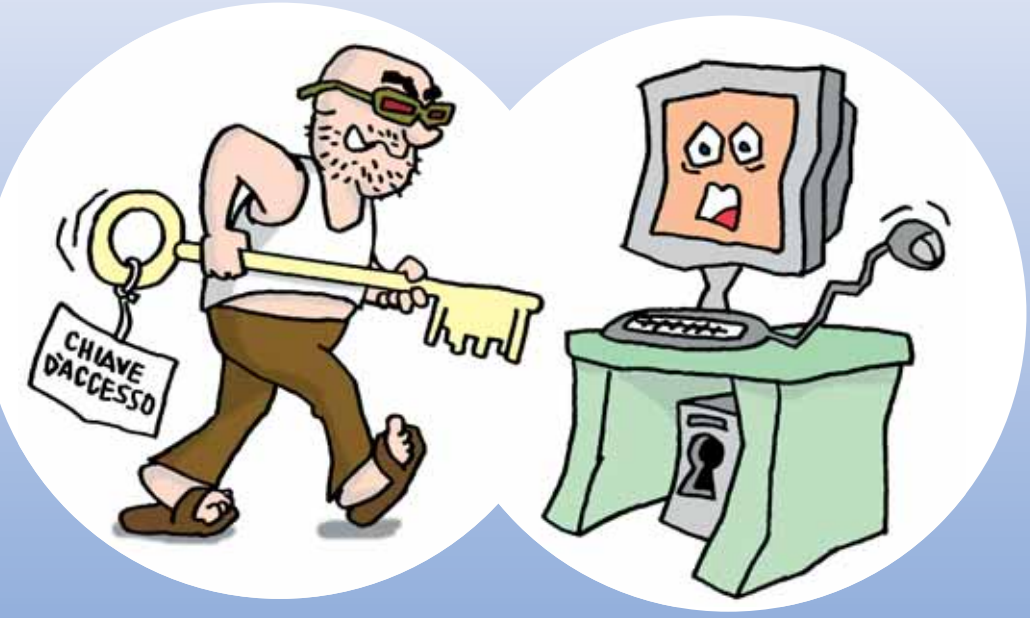
- Non eseguite file che non conosci
- Ricordati di salvare frequentemente il tuo lavoro, specie quando stai facendo qualcosa a cui tieni particolarmente
- Quando scarichi o condividi musica lascia sempre attiva la protezione del firewall e dell'antivirus
- Non eseguire procedure delle quali non conosci perfettamente gli effetti

CONSIGLI PER I GENITORI

- Ricorda di installare e tenere ben aggiornati i software antivirus e antispyware, oltre che il sistema operativo
- Se è presente una rete senza fili assicurati che sia protetta
- Se il computer di casa è anche utilizzato per lavorare, non lasciarlo utilizzare ai ragazzi senza supervisione
- Se necessario proteggi il computer con una password complessa
- Organizza i dati in modo da ridurre al minimo il rischio di perderli
- Esegui il backup periodico

PROTEGGERE I PROPRI DATI

La scelta di una password



Le caselle di posta elettronica, ma anche alcuni servizi presenti all'interno di siti, blog o forum, i servizi di telefonia e quelli bancari, così come i servizi erogati dalle scuole, sono solo alcune delle applicazioni informatiche protette da password.

Troppo spesso sottovalutiamo l'importanza della password e ne scegliamo una con superficialità, magari solo perché una certa parola è più facile da ricordare. Raramente sentiamo la necessità di modificare periodicamente quelle che utilizziamo tutti i giorni, nella convinzione che mai nessuno sarà in grado di scoprirle.

Questo accade a causa dell'inconsapevolezza delle implicazioni e delle responsabilità che derivano da un cattivo uso delle proprie parole chiave e degli effetti che una loro cattiva gestione comporta in termini di sicurezza.

PRESTATE ATTENZIONE A

I pericoli che si corrono a causa di una cattiva gestione delle password sono numerosissimi. Si pensi, solo per fare un esempio, se qualcuno violasse la nostra privacy leggendoci la posta elettronica o se la utilizzasse il nostro indirizzo, magari per inviare messaggi truffaldini o di minaccia ad una terza persona.

E dunque, come scegliere una buona password?

Nella sua individuazione evitiamo innanzitutto i nomi comuni (come quello dei genitori, del fratellino o della sorellina, della fidanzata/o o dell'animale domestico) e le date di nascita (vostre e delle persone più care).

Una buona password può essere poi individuata deformando una o più parole. Si possono ad esempio modificare alcune lettere di una parola che ben conosciamo. Proviamo a cambiare le "s" con dei "5", le "i" con degli "1", le "o" con degli "0", e il gioco è fatto.

Spazio alla fantasia!

CONSIGLI PER TUTTI

- Non trascrivere mai la password in agende, diari e non salvarla nel telefonino, perché sono i primi luoghi ove il malintenzionato la cercherà
- Non digitarla mai in presenza di persone estranee
- Osserva sempre dove stai digitando la password. Solo negli appositi spazi essa non sarà leggibile a chi ti sta intorno
- Utilizza più di una password per i diversi servizi e graduane la complessità in relazione alla tipologia di servizio
- Non aver timore di creare password lunghe o complesse

TRUFFARE CON IL TELEFONO

I Dialer

Il dialer è un programma informatico che consente di comporre via modem i numeri telefonici necessari per collegare il computer ad un fornitore di servizi telematici. Il collegamento viene stabilito attraverso la tradizionale linea telefonica ed i costi della connessione vengono addebitati nella bolletta.

Solitamente il dialer viene utilizzato per collegarsi ad Internet e navigare a costi contenuti.

Alcuni tipi di dialer ci permettono di accedere a diversi siti commerciali che, a fronte di una connessione telefonica molto più costosa, forniscono gadget elettronici di varia natura, come ad esempio suonerie per il telefonino, oppure consentono l'accesso a contenuti particolari.

Tuttavia molto spesso questo tipo di connessioni non sono desiderate e si corre il rischio di ricevere bollette da capogiro.

PRESTATE ATTENZIONE A

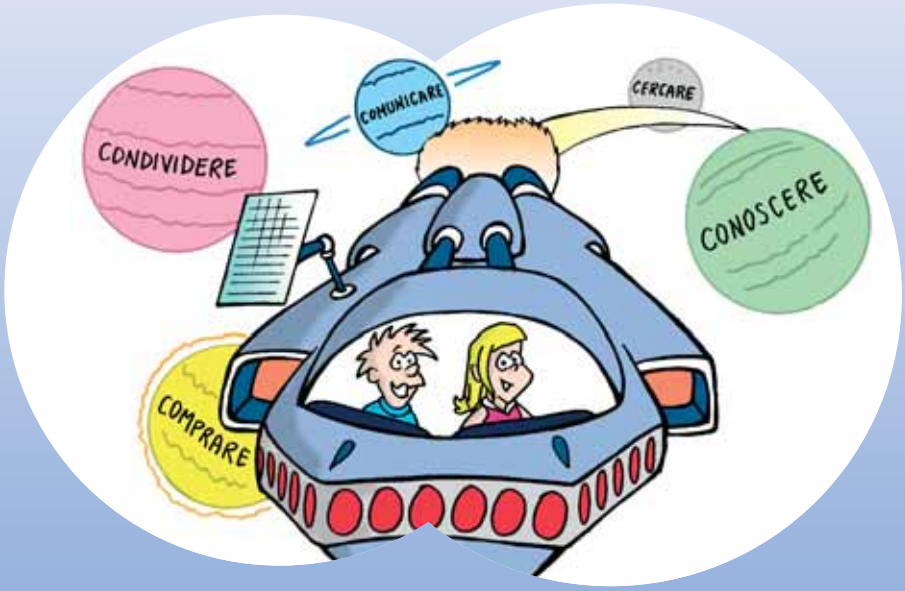
Un download disattento oppure un file allegato ad una email potrebbe installare nel computer un dialer truffaldino che effettua chiamate a numeri remoti costosissimi, senza il nostro consenso e a nostra insaputa.
Il fenomeno dei dialer ha colpito migliaia di utenti che, ignari, effettuavano chiamate dai costi esorbitanti. La Polizia di Stato ha calcolato che sono oltre 25.000 gli italiani che hanno presentato denuncia per le connessioni a tramite le numerazioni 709, dopo aver ricevuto bollette salatissime ed incongruenti rispetto al normale traffico telefonico.
Grazie anche alla diffusione dei collegamenti a "banda larga", il numero delle truffe attraverso i dialer si è notevolmente ridotto, ma è ancora necessario prestare la massima attenzione.

CONSIGLI PER TUTTI

- Installa un software anti-dialer
- Controlla periodicamente la tua connessione di accesso ad Internet
- Imposta un livello di sicurezza del tuo browser medio/elevato e se necessario disattiva il download di file Activ-X
- Impedisci l'apertura di pop-up
- Disabilita i codici 709, 899 e, se non sono necessarie, le numerazione internazionali contattando il tuo operatore di telefonia
- Leggi con attenzione gli avvisi e le comunicazioni che appaiono quanto scarichi file

2

LA POTENZIALITÁ DEL WORLD WIDE WEB



Oggi si cresce online. L'accesso ad Internet è disponibile attraverso la scuola, la biblioteca, il computer di un amichetto o quello di casa. Il numero dei ragazzi connessi ed il tempo speso per questo intrattenimento è in costante crescita. Allo stesso modo diminuisce l'età alla quale vengono effettuati i primi collegamenti.

Lo strumento utilizzato non è più esclusivamente il computer. La maggior parte delle consolle sono in grado di navigare sul web, chattare o giocare online. Ci si può connettere anche con apparati mobili, come i telefoni cellulari o le agende elettroniche.

La rete può essere assimilata ad un enorme biblioteca che cataloga un'inesauribile fonte di conoscenza, messa a disposizione in molteplici formati. Al tempo stesso è come un quotidiano che cambia faccia di giorno in giorno, offrendo contenuti sempre nuovi.

Internet è anche una risorsa formativa e didattica. Sono sempre più

numerosi i siti che offrono corsi online nelle materie più disparate e gli istituiti scolastici che offrono la possibilità di approfondire gli argomenti trattati in classe attraverso ricerche individuali o di gruppo da fare attraverso la rete.
La naturale propensione dell'essere umano alla socializzazione ha trovato poi nella rete un veicolo inesauribile di contatti. Coltivare vecchie amicizie, intrecciarne di nuove o mantenere i legami con parenti lontani attraverso Internet è un gioco da ragazzi. Gli strumenti disponibili sono numerosissimi: dalle email alle chat, dall'instant messaging alla webcam. C'è solo l'imbarazzo della scelta.
Inoltre, attraverso Internet è possibile scambiarsi testi scritti, suoni, immagini, software e qualsiasi altra cosa possa essere trasformata in un file digitale.
Per di più, la rete è come un immenso supermercato dove si può acquistare qualsiasi oggetto, molto spesso a prezzi convenienti.
Nelle pagine che seguono, i nostri due amici Net e Webby ci illustreranno alcune delle enormi ricchezze della rete, indicandoci al contempo i rischi più diffusi ed alcuni preziosi sconsigli su come scongiurare le situazioni di pericolo.
Infatti, proprio come abbiamo imparato fin da piccoli a guardare da entrambi i lati prima di attraversare la strada o a non dare confidenza agli estranei fuori da scuola, è necessario apprendere alcune nozioni basilari prima di andare online.
Non serve essere un esperto di informatica e non serve nemmeno che lo siano mamma o papà, ma l'importante è condividere con loro ciò che facciamo con il computer e soprattutto seguire i loro preziosi consigli.

CERCARE

...e trovare di tutto un po'

Internet è un'incredibile risorsa sulla quale si può trovare un pò di tutto. Si possono fare ricerche online per completare i compiti che vengono assegnati a scuola o per apprendere qualcosa in più circa un argomento che ci interessa particolarmente.
Conoscenze, cultura, sport, viaggi, giochi e passioni di ogni genere possono essere coltivate ed arricchite online.
Si dice che il world wide web esprima l'idea stessa di libertà e esso sia il luogo ove ogni l'iniziativa individuale possa essere intrapresa, ed ogni idea espressa in qualunque forma.

PRESTATE ATTENZIONE A

Su Internet non esiste alcuna censura e questa incontrollata libertà di espressione fa sì che non tutto quello che è disponibile sulla rete sia adeguato alla nostra età. La naturale curiosità per alcune tematiche rischia di farci imbattere in argomenti o contenuti indesiderati.
Espressioni di razzismo, immagini violente o pornografiche sono soggetti che sicuramente non vorremmo vedere.
In secondo luogo, navigando tra un link e l'altro ci può capitare di perdere la cognizione del tempo, sottraendo così importanti risorse alla studio, alle amicizie ed allo sport. È importante non esagerare!

CONSIGLI PER I RAGAZZI

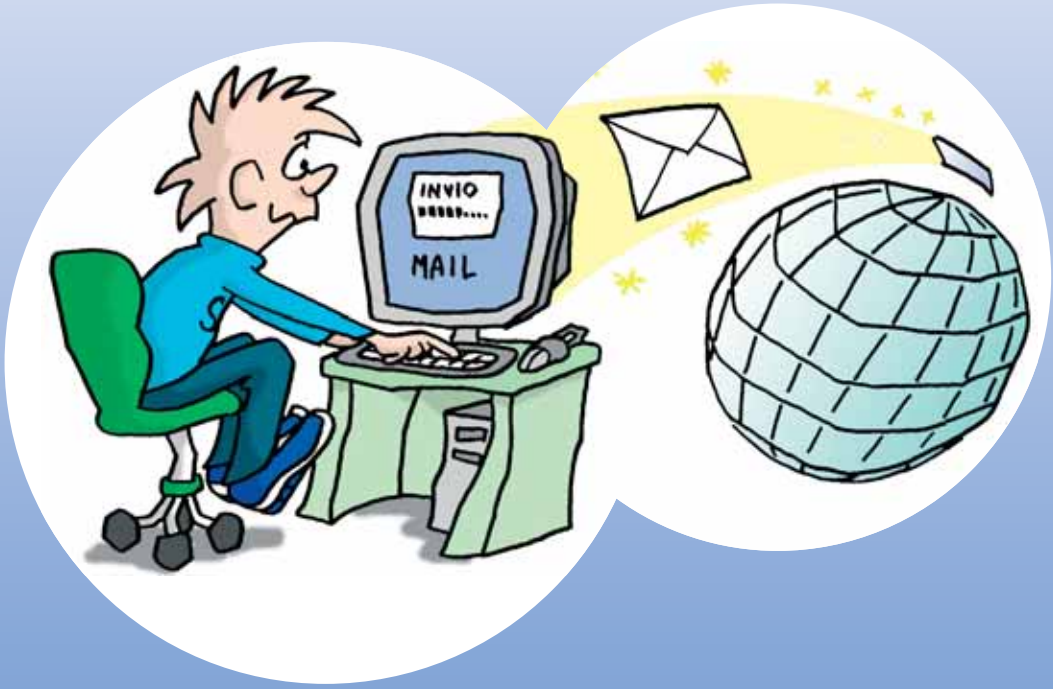
- Privilegia l'utilizzo di motori di "ricerca sicura"
- Se incontri un sito con l'indicazione "vietato ai minori", rispetta l'indicazione
- Segnala i contenuti inadatti agli adulti e discutine con loro
- Non passare più di un'oretta al giorno davanti al computer
- Concorda con i genitori il tempo di utilizzo del computer

CONSIGLI PER I GENITORI

- Discuti con i tuoi figli dei benefici e dei rischi di Internet e prova ad andare online con loro
- Fatti mostrare i loro siti preferiti, i giochi online e le chat che frequentano più spesso
- Se i tuoi figli ti raccontassero di aver visto cose inappropriate, non rimproverarli e non punirli. La tua reazione avrà effetto sulle cose che i tuoi figli decideranno di condividere in futuro
- Controlla frequentemente la cronologia dei siti visitati e la cache di navigazione
- Valuta la possibilità di usare un sistema di filtro o di blocco delle ricerche online

COMUNICARE

Via Internet è veloce, semplice ed economico



Comunicare via Internet è veloce, semplice ed economico.
L'email è l'applicazione Internet più conosciuta ed utilizzata; consente di comunicare con chi vogliamo e in qualunque luogo del mondo esso si trovi. È sufficiente disporre di un computer collegato ad Internet.
Via email si può trasmettere del semplice testo, ma anche pressoché qualunque "oggetto elettronico" sotto forma di allegato. Musica, filmati, fotografie e software sono solo alcuni esempi di ciò che può volare da un computer ad un altro grazie ad un messaggio di posta elettronica.

PRESTATE ATTENZIONE A

I principali rischi connessi alle email sono quelli che derivano dall'uso improprio che altri ne fanno. Bombardamenti pubblicitari, trasmissione di virus o tentativi di truffa sono alcuni dei rischi che arrivano con la posta elettronica. È bene quindi prestare attenzione ai mittenti dei messaggi che vengono incasellati al nostro indirizzo, perché le insidie sono sempre dietro l'angolo.

CONSIGLI PER I RAGAZZI

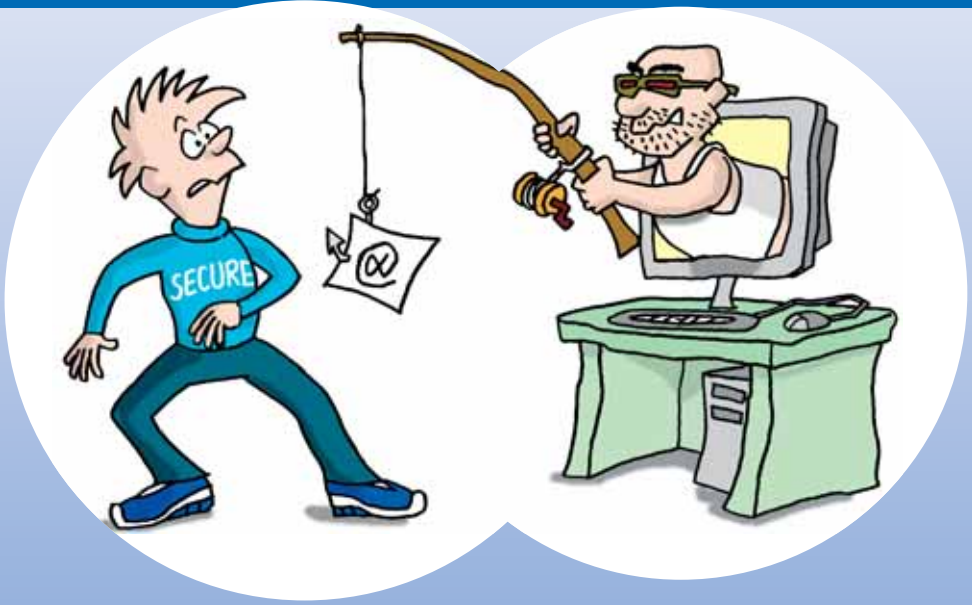
- Non trasmettere mai nessuna informazione personale
- Non condividere mai la password della tua casella di posta, neanche con gli amici
- Se ti arrivano messaggi da sconosciuti cestinali subito senza eseguire gli allegati
- Non salvare o copiare file allegati ad email, senza aver verificato che siano privi di virus

CONSIGLI PER I GENITORI

- Se i tuoi figli ricevono spam o posta indesiderata o vengono bombardati da messaggi pubblicitari, dì loro di eliminare queste mail senza dare importanza ai contenuti
- Insegna ai tuoi figli a non accettare inviti, non concordare mai appuntamenti e non inviare dati personali o immagini ad altre persone, a meno che tu non sia d'accordo
- Insegna ai tuoi figli ad informarti quando ricevono messaggi offensivi o volgari
- Cancella spesso i messaggi di posta elettronica memorizzati o spostati nel cestino

COMUNICARE

Phishing e spamming



Le truffe che vengono innescate da una email sono numerosissime, molto insidiose ed in numero sempre crescente.
Il phishing è un tipo di truffa online che utilizza le email allo scopo di "pescare" (fish) con l'inganno informazioni private. La phishing email solitamente contiene un collegamento ad un sito illegale che appare pressoché identico ad un sito noto, inducendo così in errore il malcapitato cybernauta.
Lo spamming invece consiste nell'inviare email non desiderate a qualcuno che non si conosce e che sicuramente non desiderava il massaggio. La spam mail è solitamente utilizzata per vendere qualcosa, ma spesso cela insidiose truffe.
Un modo senz'altro efficace per diffondere un messaggio alla velocità del web sono le Catene di Sant'Antonio. Anche in questo caso, spesso i messaggi nascondono pericolosi trabocchetti.

PRESTATE ATTENZIONE A

È importante valutare con attenzione le email che riceviamo ogni giorno.
Nome utente, password, riferimenti di un account o dati relativi ad una carta di credito non vengono mai richiesti via email, pertanto messaggi di posta elettronica con i quali vengono pretesi tali dati nella maggior parte dei casi nascondono una frode informatica.
È importante essere prudenti e mantenere sempre la riservatezza dei propri dati, diffidando delle email sospette.

CONSIGLI PER I RAGAZZI

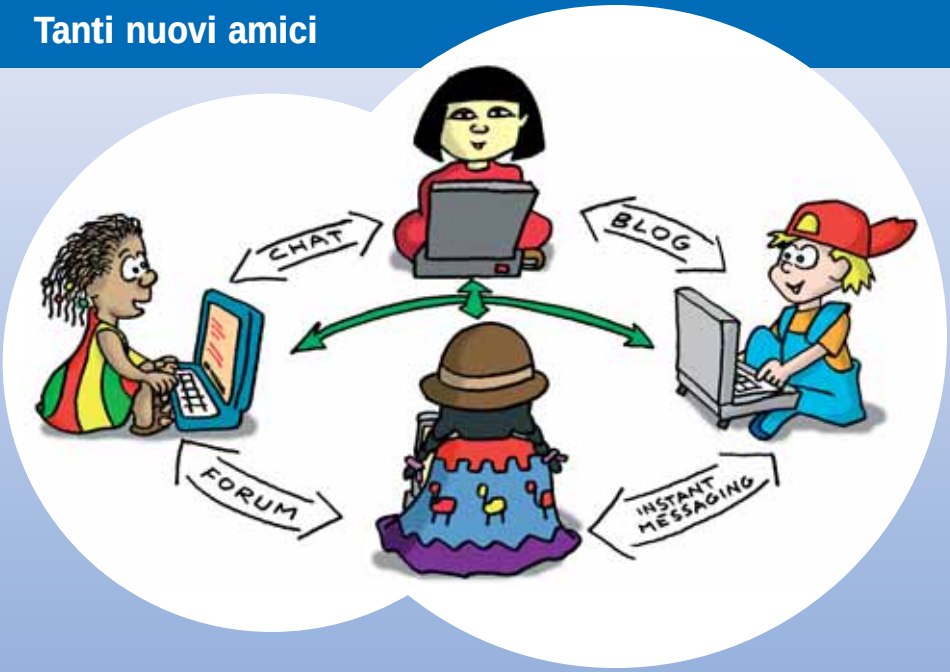
- Non farti attrarre da proposte di vendita di prodotti a prezzi eccessivamente scontati, di farmaci senza prescrizione medica o di prodotti discutibili
- Non aprite link riguardanti materiale pornografico o inadatto
- Non farti attrarre da prodotti finanziari che promettono guadagni elevati e rapidi
- Fare un'opera di bene è sicuramente un gesto prezioso, ma alle volte dietro alle richieste di aiuto ci sono persone senza scrupoli ed è bene prestare attenzione

CONSIGLI PER I GENITORI

- Utilizza le impostazioni di bloccaggio e filtraggio della posta indesiderata presenti nelle caselle di posta elettronica più diffuse
- Insegna ai tuoi figli che non esistono guadagni facili e che qualora desiderassero rispondere a qualche email ricevuta da persone sconosciute è importante che prima si confrontino con voi
- In caso di avvisi di malfunzionamenti o di problemi particolari con un proprio account, verifica che il problema sia reale

CONOSCERE

Tanti nuovi amici



La grande diffusione delle chat, dei servizi di messaggistica istantanea e dei blog ha influenzato il nostro modo di incontrarsi e di interagire. Sempre più utenti di Internet si conoscono sulla rete e alcuni di questi contatti si trasferiscono nel mondo reale con incontri “dal vivo”, a volte con soddisfazione (ci sono anche matrimoni fra persone conosciute in chat), a volte con profonde delusioni, altre volte con situazioni pericolose.

Insomma in Internet, come nella vita e nelle attività di tutti i giorni, possiamo altrettanto facilmente incappare in “brutte sorprese”.

Questo avviene perchè negli utenti delle chat c’è la mancanza di un’identità certa.

Dobbiamo essere coscienti di questa situazione e non dimenticare mai che l’interlocutore, per motivi vari, può essere diverso (o diversa) da quello che dichiara di essere, con tutto ciò che ne consegue.

PRESTATE ATTENZIONE A

La chat è un servizio aperto a tutti, previa registrazione di un nick name. Il nick name nasconde il vero nome agli altri partecipanti della chat. Se non sarà il chatter a comunicare la sua vera identità, questa rimarrà anonima. Tuttavia è possibile denunciare chi infrange le regole all'interno della chat, dato che nessuno resta del tutto anonimo sulla rete. Ogni nick name è associato in modo univoco a un numero IP per tutto il tempo che l'utente resta in chat e questo permette all'amministratore del sistema di rintracciare la vera identità dell'utente in caso di necessità.

CONSIGLI PER I RAGAZZI

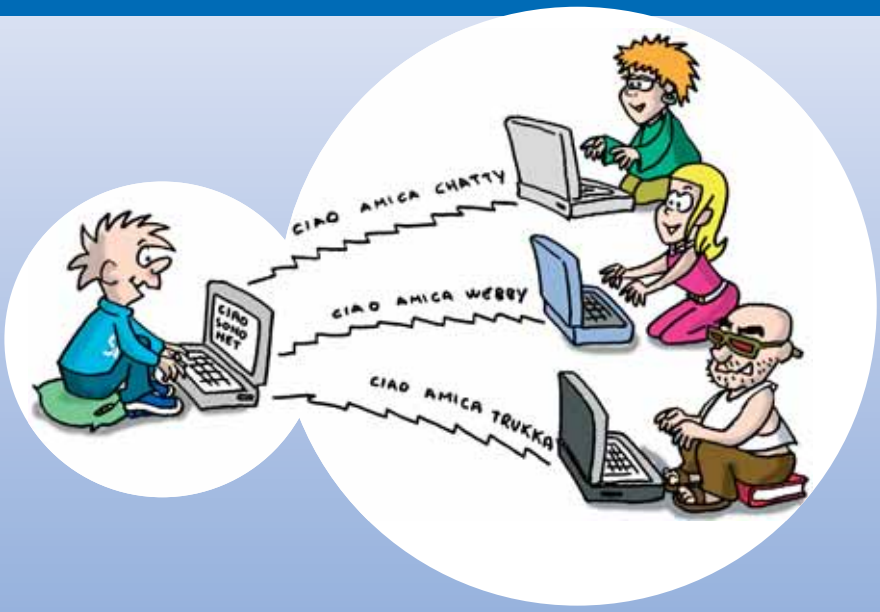
- Non scegliere particolari nick name, che possano attirare l'attenzione o che contengano allusioni all'età (ad es. "lolita", "tispakkolafaccia" o "lucia 1995")
- Nel modulo di registrazione della chat non fornire per nessun motivo informazioni personali vere o hobby particolari (per es. con allusioni sessuali)
- Durante le conversazioni non indicare dati personali
- Ricorda che non tutto quello che leggi o vedi su Internet è vero

CONSIGLI PER I GENITORI

- Scegli il nick name insieme a tuo figlio e divertiti a compilare il modulo di registrazione insieme a lui
- Utilizza le chat insieme a lui, fallo come se fosse un gioco ovvero fatti raccontare quello che è avvenuto e commenta con lui quello che ha visto
- Verifica periodicamente che tuo figlio usi i nick name scelti insieme e che non ne abbia altri
- Supervisiona le attività online chiedendo spesso che cosa sta facendo al pc e con chi è collegato

CONOSCERE

...ma non tutti sono buoni amici



Sulle chat incontriamo persone di tutti i tipi. Ci sono individui a posto e brutti soggetti, nella stessa identica percentuale di una strada affollata o di qualsiasi altro luogo pubblico.
Troviamo cultura, informazione, dibattito politico, amore, arte, solidarietà, ma anche mercati di pornografia, truffatori, terroristi, pedofili, maniaci come, del resto, sperimentiamo nel territorio reale. Vediamo anche i cyber bulli, ovvero utenti che insultano le persone pubblicamente, li prendono in giro in maniera feroce, rendono pubbliche le confidenze in rete o che in virtù di privilegi particolari posseduti sulla chat, "buttano fuori" le loro "vittime" dalla "stanza" in cui si sta chiacchierando.
Insomma le persone "cattive" ci sono anche in Internet!
Questo non vuol dire che dobbiamo rinunciare ad usare le chat. Usiamo sempre cautela e manteniamo alta la naturale diffidenza nei confronti di chi non conosciamo.

PRESTATE ATTENZIONE A

Nella chat ogni utente parla contemporaneamente con tutti gli altri oppure può "appartarsi" con un altro in uno spazio privato. Spesso le cattive intenzioni si manifestano durante le conversazioni "private". I sistemi di instant messanging e le chat permettono di scambiarsi links, da cui è facile importare virus sul proprio pc, e di trasferire con grande velocità files, che potrebbero riguardare anche aspetti illeciti o pericolosi. Soprattutto se inviati nell'ambito di scambi "privati", il loro contenuto può essere rischioso.

CONSIGLI PER I RAGAZZI

- Verifica le tematiche indicate nelle chat e evita quelle di tipo particolare o illecite.
- Stai attento al materiale che scarichi sul pc attraverso le chat o i servizi di istant messanging.
- Non rispondere alle provocazioni.
- Sii diffidente nei confronti di chi vuole sapere troppe cose.

CONSIGLI PER I GENITORI

- Insegna a tuo figlio che per evitare contrasti sulla rete, la prima cosa da fare è non accettare le provocazioni e ignorare il cyberbullo.
- Segnala sempre i comportamenti ritenuti scorretti all'amministratore del servizio, per far escludere il "bullo" dalla comunità frequentata.
- Presta attenzione all'utilizzo delle chat in modalità private: il rischio di cattivi incontri aumenta notevolmente!
- Cerca di conoscere gli amici online di tuo figlio.

CONOSCERE

I malintenzionati ci sono anche sulla rete

Molte chat riservano delle “stanze” per le questioni di nostro interesse e noi ci ritroviamo al loro interno a chiacchierare. È proprio in queste aree che più facilmente si muove un maleintenzionato.
Chi tenta di avvicinarsi a noi lo fa gradualmente, guadagnando prima la nostra fiducia per poi sviluppare con noi una “relazione”. L’aggressore passa da conversazioni su argomenti di nostro interesse nelle chat room pubbliche a comunicazioni più intime in stanze private e cerca poi di ottenere un indirizzo email, un contatto di istant messanging o il numero di cellulare. La fase finale del processo di adescamento prevede un incontro con noi.
La riposta da dare è sempre una sola: “No, grazie!” e bisogna sempre avvisare i genitori.
Ricordati che il maleintenzionato non è facilmente identificabile e non si distingue da altri visitatori delle chat. Perciò occhio a non farti imbrogliare!

PRESTATE ATTENZIONE A

Per avvicinare i minori un cyber-pedofilo a volte nasconde la propria età, mascherandosi con un nick name apposito; altre volte mantiene la sua identità e fa leva sui minori facendoli sentire importanti e "speciali" perchè conoscono persone più grandi. Talvolta sfrutta la loro curiosità nei confronti della sessualità, per stimolare l'interesse su tematiche sessuali ed il bisogno di scoprirle, ed invia fotografie pedo-pornografiche - per convincerli che tali comportamenti sono normali e che gli altri bambini sono sessualmente attivi - oppure pornografiche, indicando di essere se stesso.

CONSIGLI PER I RAGAZZI

- Parla subito con un adulto se vengono proposti incontri reali o situazioni "strane" o se ti fanno complimenti e/o regali
- Non rispondere mai a email fastidiose o allusive, specie se di argomento sessuale, e avvisa i tuoi genitori se vedi fotografie di persone adulte o di bambini nudi
- Non prendere mai appuntamenti con persone conosciute su Internet, anche se dicono di essere coetanei, senza avere prima il permesso dei tuoi genitori, e fai venire anche loro al primo incontro

CONSIGLI PER I GENITORI

- Verifica che nella chat nessuno dica qualcosa di strano o preoccupante (per esempio discorsi sul sesso)
- Leggi e visiona le email insieme a tuo figlio
- Controlla l'iscrizione a chat verificando che siano garantite per i minori e meglio se con moderatore
- Valuta se è necessaria l'installazione di web-cam e verifica come vengono usati web-cam e/o videotelefoni
- Configura opportunamente il computer per registrare le sessioni di chat intrattenute e controllale periodicamente

APPROFONDISCI ONLINE www.guidaallasicurezza.it

CONOSCERE

Inviare proprie fotografie

Un malintenzionato con cautela arriva a parlare della sessualità, inviando immagini pornografiche di se stesso ritraenti bambini nudi e chiedendo di compiere atti sessuali da riprendere con web-cam o videotelefoni.

A volte le nostre immagini, prima in costume e poi senza, sono richieste con la falsa promessa di partecipazione a provini nel mondo della moda. In alcune occasioni questa scusa si trasforma in minaccia di diffonderle sulla rete se non vengono inviate altre fotografie ancor più piccanti.

Talvolta filmati in atteggiamenti intimi fra consenzienti sono diffusi su Internet da ex-fidanzati dopo litigi o da terze persone per motivi di gelosia.

Dobbiamo proteggere la nostra intimità e privacy e non farci riprendere mai in situazioni private: le persone possono tradire la nostra fiducia ed approfittarsi della nostra ingenuità!

PRESTATE ATTENZIONE A

Il telefono cellulare costituisce un collegamento "privato" - pertanto non facilmente vincolabile - fra il minore e il pedofilo, dopo il preliminare incontro su Internet. Infatti la ricarica della sim card potrebbe essere uno strumento per adescare un minore. Bisogna altresì valutare quali servizi (SMS, MMS, bluetooth, accesso a Internet) disabilitare nei cellulari di ultima generazione.
Riguardo a Internet è preferibile disattivare tale opportunità non solo per evitare costi elevati dovuti alla connessione, ma anche per proteggere il telefono da eventuali virus e lo stesso minore dai rischi legati a una navigazione non controllata.

CONSIGLI PER I RAGAZZI

- Non inviare le tue immagini a nessuno e non farti vedere in webcam, a meno che non ti autorizzino i tuoi genitori
- Non farti ritrarre in atteggiamenti intimi da nessuno
- Ricorda che le proposte troppo belle non sono mai vere (per esempio quelle relative a facili provini nel mondo della moda)
- Non dare il tuo numero di telefono agli sconosciuti e non prestare il cellulare a nessuno

CONSIGLI PER I GENITORI

- Controlla i file salvati sul computer e sul cellulare
- Acquista un cellulare che sai usare o comunque, impara il suo funzionamento, magari facendoti spiegare da tuo figlio
- Valuta quali servizi del cellulare è opportuno disabilitare
- Attiva la sim del telefono a tuo nome, per controllare il traffico telefonico effettuato tramite Internet
- La ricarica telefonica deve essere fatta esclusivamente da te
- Definisci regole abbastanza rigide sull'uso del cellulare in base all'età del minore

CONDIVIDERE

Filmati, musica e tanto altro: il file sharing

I sistemi di file sharing, di per sé pienamente leciti, ci possono agevolare nel ricercare contenuti particolari. Tuttavia dobbiamo prestare attenzione al tipo di materiale condiviso. Per esempio diffondere immagini pedo-pornografiche è illecito. Anche scaricare e distribuire file musicali, film o programmi non è legale, perché vietato dalle norme sui diritti d'autore.

L'avvento delle nuove tecnologie informatiche e telematiche ha aperto nuovi orizzonti alle strategie della "pirateria". Per contrastarle molteplici comportamenti che violano i diritti d'autore hanno rilevanza penale. L'aspetto più complesso è però legato alla mancata percezione della reale lesività del fenomeno.

Scaricare programmi e file audiovisivi o venderli dopo averli copiati sono reati come una truffa o un furto e non devono essere consentiti!

PRESTATE ATTENZIONE A

Il rischio più grosso nell'adoperare le tecnologie di file sharing è l'arrivo sul PC di materiale non desiderato o pericoloso (per esempio immagini pedo-pornografiche o pornografiche) poiché talvolta questo si cela dietro indicazioni di altro genere. Inoltre i files si aprono direttamente sul computer non appena il programma termina le operazioni di scarico. Ricordiamoci anche che molti programmi di file sharing mettono in condivisione in automatico i files prima che venga completato il download sul proprio computer.

CONSIGLI PER I RAGAZZI

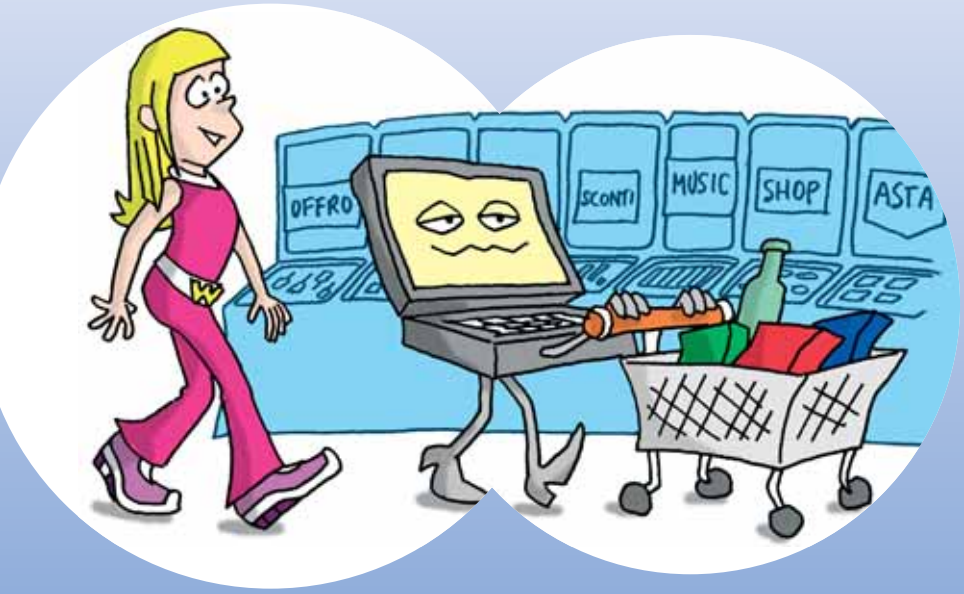
- Non diffondere con i file sharing film, mp3 musicali o programmi: è illegale!
- Presta attenzione a quello che scarichi. Talvolta nei files si nascondono dei virus
- Valuta insieme ai tuoi genitori la cartella di condivisione ed il suo contenuto
- Effettuare una copia di back up dei tuoi supporti originali è consentito

CONSIGLI PER I GENITORI

- Valuta se installare i file sharing sul PC di tuo figlio
- Configura opportunamente i programmi di file sharing
- Verifica costantemente quale materiale viene condiviso e che cosa viene scaricato
- Stai accanto a tuo figlio quando scarica files e controlla, magari prima di lui, il risultato della ricerca
- Non permettere che tuo figlio scarichi musica e film tramite i file sharing
- Sensibilizza tuo figlio a non duplicare illegalmente musica, film o programmi

COMPRARE

Consigli per gli acquisti



L'era di Internet, oltre ad aver introdotto nuove le forme di socializzazione che, come abbiamo visto, hanno rivoluzionato le modalità di comunicazione tra le persone, ha profondamente modificato gli scambi commerciali tra gli individui.
L'e-commerce è una forma sistema transazionale ove gli acquisti e le vendite di beni e servizi vengono effettuate attraverso comunicazioni elettroniche e non scambi fisici e contatti diretti.
Grazie al commercio elettronico, oggi è possibile fare acquisti comodamente seduti sulla poltrona di casa, molto spesso con risparmi considerevoli rispetto ai negozi reali ed avendo a disposizione l'immensa varietà di prodotti reperibile su Internet.

PRESTATE ATTENZIONE A

È bene però considerare alcuni fattori. In primo luogo, davanti al computer non si tocca con mano il prodotto acquistato e, a meno che non lo si abbia visto altrove, non se ne conoscono le caratteristiche. Spesso, poi, sottovalutiamo gli aspetti legati alla restituzione della merce che dovesse rivelarsi difettosa o guasta, o semplicemente non rispondente alle aspettative. In questi casi sarà infatti necessario rispedire il prodotto al venditore e seguire burocratiche procedure per il cambio di quanto acquistato o per la restituzione del denaro.
Quando poi gli acquisti sono fatti all'estero è necessario considerare che al momento della consegna potrebbero esserci addebitati gli ulteriori costi di sdoganamento, dazio ed imposta.

CONSIGLI PER I RAGAZZI

- Diffida dei piccoli siti e di quelli "sconosciuti"
- Conserva i messaggi di conferma dell'acquisto
- Valuta accuratamente i costi di spedizione ed eventuali ulteriori oneri di acquisto
- Non sempre dietro un prezzo basso c'è un affare

CONSIGLI PER I GENITORI

- Preferisci sistemi di pagamento certificati e che garantiscano il rimborso in caso di mancata ricezione della merce
- Richiedi al venditore più informazioni e dati possibile
- Diffida dai prezzi eccessivamente vantaggiosi

COMPRARE

Mercatini online

I veri protagonisti del commercio elettronico sviluppatosi negli ultimi tempi sono i mercatini online e sopratutto i siti attraverso i quali è possibile acquistare beni all'asta.
Gli attori di queste comunità sono costituiti sia da privati che da negozianti. Ci sono i curiosi, i collezionisti, i cacciatori d'affari e piccoli commercianti che vogliono promuovere i loro prodotti.
Anche in questo caso le barriere geografiche vengono frantumate dalla forza del web e alcuni siti costituiscono delle comunity virtuali che vanno al di là dei confini territoriali dei singoli Stati. Queste comunità possono essere costituite da milioni di persone. Pensate che se E-bay fosse una Nazione sarebbe la quinta più popolosa la mondo dopo Cina, India, Stati Uniti ed Indonesia...!!!

PRESTATE ATTENZIONE A

La maggior parte dei venditori sono corretti ed onesti.
Tuttavia, l'anonimato, la distanza e la mancanza di contatto tra acquirente e venditore, i meccanismi ed i tempi di pagamento e spedizione possono favorire individui malintenzionati, pronti a giocare brutti scherzi.
Quello dei mercatini e delle aste online è un terreno estremamente fertile per i moderni truffatori che vendono attratti dalla possibilità di trarre illeciti abusando della fiducia o dell'inesperienza di alcuni utenti.

CONSIGLI PER I RAGAZZI

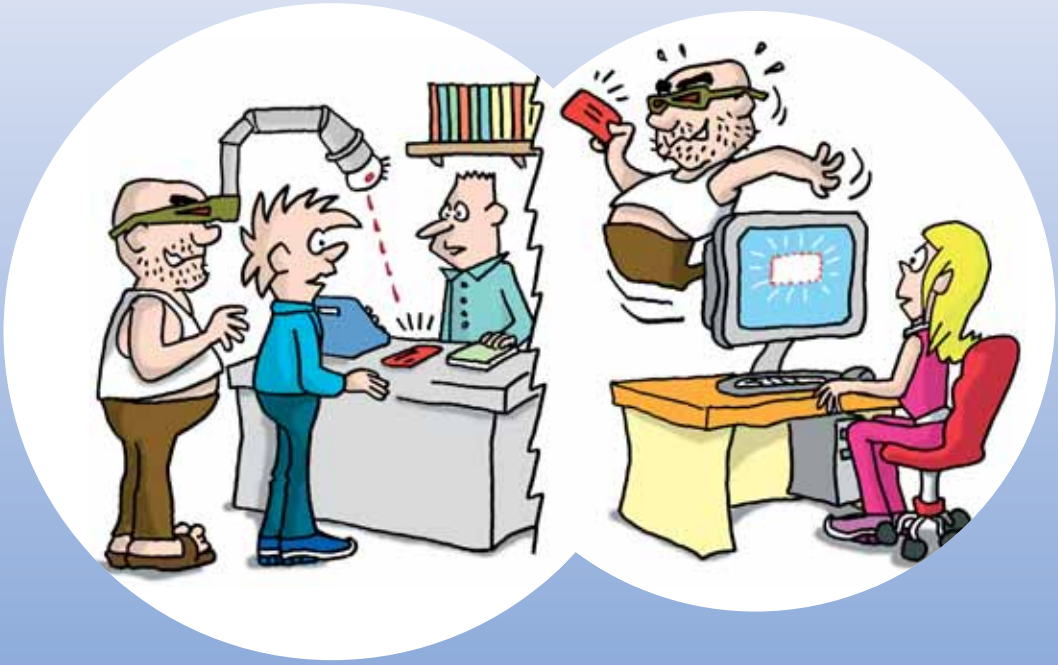
- Verifica se il venditore è un privato o un negoziante
- Diffida dalle offerte troppo basse, il materiale potrebbe essere rubato o non esistere affatto
- Non inviare denaro prima di esserti accertato dell'esistenza del venditore
- Usa maggior cautela se i soldi sono diretti all'estero
- Presta attenzione ai rilanci ed ai feedback: potrebbero essere fasulli
- Non partecipare ad offerte "esterne"

CONSIGLI PER I GENITORI

- Se consegni a tuo figlio una carta di credito prepagata considera che la potranno utilizzare anche via
- Assistiti tuo figlio nei primi acquisti
- Verifica che cosa ha acquistato tuo figlio
- Usa sistemi di pagamento certificati

COMPRARE

Le carte di pagamento



Sono sempre più le persone che utilizzano la carta di credito o il bancomat per pagare qualunque tipo di spesa: da quella del supermercato al conto al ristorante, dai rifornimenti di carburante ai pedaggi autostradali.
Persino bollettini postali, prestazioni sanitarie o le spese relative al rilascio di un passaporto possono essere corrisposte tramite bancomat o carta di credito. Inoltre tali tessere vengono utilizzate per il prelievo o per l'anticipazione di denaro contante presso sportelli bancari automatici e non, ovvero per effettuare transazioni e acquisti su Internet.
Le carte magnetiche di pagamento sono uno strumento veloce, sicuro e che ci permette di girare con pochi spicci in tasta, senza dover rinuncia, all'occorrenza, ad una spesa più consistente.

PRESTATE ATTENZIONE A

Proporzionalmente al rapido diffondersi di questo comodo e generalmente sicuro mezzo di pagamento, abbiamo assistito alla forte espansione di truffe sempre più complesse perpetrate in danno degli utilizzatori di questi strumenti.
Per tale ragione, la carta di credito deve essere custodita ed utilizzata in modo riservato e prudente. Per potersi attivare in tempi estremamente rapidi in caso di abuso è consigliato abilitare il servizio sms di avviso delle spese effettuate. È inoltre importante verificare con oculatezza gli estratti conto periodici segnalando tempestivamente alla società emittente eventuali transazioni non effettuate.

CONSIGLI PER L'UTILIZZO TRADIZIONALE

- Non perdere mai di vista la carta di credito al momento del pagamento, soprattutto nei luoghi che non frequenti abitualmente o all'Estero
- Controlla che al momento del recapito della carta di credito e del pin le buste siano integre e ben sigillate
- Quanto ti rechi presso un bancomat, verifica con attenzione l'integrità della tastiera e della parte dove inserisci la tessera

CONSIGLI PER L'UTILIZZO TELEMATICO

- Negli acquisti privilegia siti conosciuti ed affidabili, sia per quanto riguarda i prodotti venduti che per i marchi proposti
- Verifica che i siti presso i quali fai acquisti utilizzino protocolli di sicurezza delle transazioni
- Evita di fornire informazioni personali non necessarie all'esecuzione del contratto di acquisto

3

E SE CAPITASSE ANCHE ME

Le grandi potenzialità della Rete e l'aumento dell'uso del mezzo telematico ci fanno sentire un po' indifesi. Sentiamo il bisogno di essere protetti anche quando usiamo Internet per lo svolgimento quotidiano delle nostre attività, per divertimento o per semplici contatti interpersonali, e percepiamo la necessità che aumenti la sicurezza della navigazione.

Sensibili a questi fattori, amministrazioni pubbliche ed associazioni hanno creato una stabile rete di contatti da interessare se si rinvengono su Internet situazioni illecite o pericolose, e si sono validamente impegnate in progetti di sensibilizzazione dell'opinione pubblica e di studio di nuovi modelli di attenzione socio-pedagogici.

Anche la Polizia di Stato ha adeguato le proprie strutture investigative alle mutate esigenze, strutturando nel corso degli anni unità sempre più specializzate (la Polizia Postale e delle Comunicazioni con le sue articolazioni territoriali dei Compartimenti e delle Sezioni), e istituendo un Ufficio di Polizia a cui il cittadino stesso può rivolgersi direttamente dalla propria casa o dal proprio luogo di lavoro (il portale del "commissariato di ps online").

Inoltre diverse associazioni hanno promosso iniziative per potenziare l'area della sicurezza in Internet, agendo in sinergia con le istituzioni e le Forze di Polizia.

Ricordiamoci che noi stessi possiamo fornire un contributo notevole attraverso tempestive segnalazioni, con la formalizzazione di denunce/querele per la commissione di reati e con un corretto ed attento uso del computer e di Internet.

E se è impossibile garantire una protezione assoluta, proprio come nel mondo "reale", c'è una strategia utilissima per minimizzare i rischi: conoscere a fondo lo strumento Internet e difendersi dai malintenzionati con il buon senso e con le poche regole pratiche inserite nei "contratti di collaborazione figli-genitori per l'uso sicuro di Internet", che speriamo vengano sottoscritti da tutti.

COME SEGNALARE O DENUNCIARE

Gli spazi presenti sulla Rete sono ormai molto numerosi. La Polizia Postale e delle Comunicazioni effettua costanti monitoraggi di Internet, ma le sue "pattuglie virtuali" non riescono a verificare tutti i contenuti disponibili. Per questo è fondamentale il tuo aiuto!

Se trovi materiale illecito o pericoloso sulla rete, provvedi a segnalarlo tempestivamente.
Puoi effettuare **la segnalazione**, anche in forma anonima:
• mediante il portale del Commissariato di PS online (www.commissariatodips.it) o il sito della Polizia di Stato (www.poliziadistato.it);
• via email ai Compartimenti ed alle Sezioni della Polizia Postale e delle Comunicazioni competenti per territorio (indirizzo dei Compartimenti: poltel.sigla del capoluogo di regione@poliziadistato.it - ad esempio poltel.mi@poliziadistato.it; email delle Sezioni: sez.poliziapostale.sigla della provincia@poliziadistato.it, ad esempio sez.poliziapostale.co@poliziadistato.it);
• attraverso i siti www.hot114.it o www.stop-it.org;
• chiamando le numerazioni 114 e 19696 (le comunicazioni sono inviate alla Polizia Postale e delle Comunicazioni per le indagini di competenza).

Se sei stato spettatore di un reato commesso ai danni di altre persone o hai subito un danno, presenta una denuncia o una querela affinché possano essere avviati gli accertamenti per risalire al responsabile.

La denuncia è relativa esclusivamente ad un reato perseguibile d'ufficio, ossia ad un illecito che non necessita della manifestazione di volontà da parte della vittima e che può essere segnalato da ogni persona che ne abbia notizia.

Puoi decidere in piena libertà quando e se sporgere la denuncia (a meno che non si tratti di casi per i quali deve essere necessariamente resa entro i tempi stabiliti dalla legge).

Puoi presentarla personalmente o a mezzo di procuratore speciale,
• al pubblico ministero (quindi depositandola in Tribunale);
• a un Ufficiale di polizia giudiziaria presente negli uffici delle Forze di Polizia:
- in forma orale, ed in tal caso l'Ufficiale redigerà verbale con la descrizione dei fatti avvenuti;
- con un atto scritto, firmato da te o dal procuratore speciale, nel quale sono riportati gli eventi illeciti. Puoi redigere autonomamente la nota o puoi usare per i reati informatici il modulo per la denuncia via web presente sul portale del Commissariato di PS online (www.commissariatodips.it). L'atto già predisposto verrà ratificato con un verbale dall'Ufficiale di PG.

È stato violato un tuo diritto o hai subito un danno (per esempio una truffa?) In questo caso devi presentare **una querela**.

Il diritto di proporre querela spetta esclusivamente alla persona offesa da un reato e non può essere esercitato trascorsi tre mesi dalla notizia del fatto che costituisce reato.
Puoi presentare la querela personalmente o attraverso il procuratore speciale, alle stesse figure incaricate di ricevere la denuncia, con le medesime modalità.
In qualsiasi momento puoi rimettere la querela.

GLI ELEMENTI UTILI PER LE INDAGINI

Vuoi aiutare la Polizia Postale e delle Comunicazioni ad avviare le indagini in modo proficuo?
Ecco gli elementi che devi indicare nelle segnalazioni o nelle denunce/querele.

SITI WEB: nome del sito; stampa del contenuto, se il sito non è pedo-pornografico (se contiene immagini di minori è sufficiente il nome della pagina web).

ATTENZIONE! **Non scaricare mai sul computer materiale pedopornografico: la sua detenzione è illegale!**

MESSAGGI PRESENTI IN NEWSGROUP: indicazione del nome del newsgroup e del modo di poterlo reperire; stampa del messaggio, se questo non è pedo-pornografico (se contiene immagini di minori è sufficiente spiegare come poterlo reperire).

EMAIL: copia dell'email comprensiva dell'header (intestazione) del messaggio e degli allegati (anche se sono relativi a immagini pedo-pornografiche).

CHAT-LINE: giorno e ora della chat; nome della chat adoperata; nick name dell'utente con cui si è conversato; dati della stanza in cui è avvenuta la conversazione (ad esempio il nome del server e del canale in IRC; la stanza in C6; l'UIN (Universal ICQ Number) in ICQ); testo della conversazione; log relativi alla conversazione in chat; files inviati durante la chat.

FILE SHARING: giorno e ora del collegamento; nome del file sharing adoperato; nick name dell'utente; file che è stato scaricato; log relativi alla divulgazione illecita.

QUERELA PER TRUFFA TRAMITE ANNUNCIO DI VENDITA: nome del servizio di vendita usato; dati del venditore; email comprensive di header relative ai contatti intrattenuti con il truffatore; indicazioni del sistema di pagamento adoperato.

DENUNCIA PER SOSTITUZIONE DI PERSONA: nome del servizio attivato a nome del denunciante; documentazione relativa all'attività illecita compiuta.

DENUNCIA PER USO INDEBITO DI CARTA DI CREDITO/DEBITO: copia di estratto conto della carta di credito o lista dei movimenti disconosciuti effettuati con bancomat.

QUERELA PER INGIURIA/DIFFAMAZIONE: copia del contenuto illecito (copia del sito, del messaggio o dell'email comprensiva di header).

QUERELA PER ACCESSO ABUSIVO A UN SISTEMA INFORMATICO: files di log relativi agli accessi; tipo e versione del sistema in uso, descrizione del tipo di operazioni illecite e dei danni accertati; nominativi delle persone informate sui fatti; backup dei file interessati dalle modifiche contenenti informazioni relative all'attacco.

QUERELA PER FRODE INFORMATICA AVVENUTA CON IL DIROTTAMENTO DI CHIAMATE VERSO CODICI 899, SATELLITARI E INTERNAZIONALI: lista delle chiamate disconosciute; copia della bolletta telefonica; indicazioni su come è stato scaricato il dialer e su come si adopera e si protegge il computer.

A CHI RIVOLGERSI

La Polizia Postale e delle Comunicazioni
www.poliziadistato.it

La Polizia Postale e delle Comunicazioni offre al cittadino una presenza capillare in tutto il territorio nazionale attraverso i 19 Compartimenti, presenti nei capoluoghi di regione, e le 76 Sezioni, presenti nelle province più grandi, che si occupano "in prima linea" di contrastare le attività illecite presenti su Internet attraverso un costante monitoraggio e la verifica delle segnalazioni e delle denunce di privati cittadini o di associazioni.

Il Commissariato online
www.commissariatodips.it

Dal 15 febbraio 2006 è attivo il portale del "commissariato di ps online" all'indirizzo www.commissariatodips.it dove è possibile ricevere informazioni (su internet, passaporti, immigrazione, minori, concorsi e licenze), scaricare modulistica nonché presentare denunce quando il cittadino è rimasto vittima di un reato informatico (dialer, truffa, hacking, carte di credito, phishing) o di un furto o smarrimento (la denuncia va comunque ratificata davanti ad un Ufficiale di polizia giudiziaria di un Ufficio di Polizia).

Comitato di Garanzia Internet e Minori
www.comunicazioni.it

Nominato dal Ministro delle Comunicazioni di concerto con il Ministro per l'Innovazione e le Tecnologie con decreto del 18.02.04, il Comitato si occupa di garantire l'osservanza del Codice di autoregolamentazione Internet e Minori e di fornire assistenza agli operatori del settore ed ai cittadini in merito alle problematiche della salvaguardia dei minori su Internet.

Hot114
www.hot114.it

Hot114 è un progetto gestito da Telefono Azzurro Onlus (gestore anche del Servizio 114-Emergenza Infanzia) e promosso dalla Commissione Europea, con l'obiettivo di costituire e rendere operativa in Italia una hotline in servizio 24 ore su 24, che permetta a chi naviga in Internet di segnalare contenuti pedo-pornografici o potenzialmente pericolosi per i minori, così da contrastare la diffusione e limitarne l'accessibilità in rete.

Save the Children Italia
www.savethechildren.it

È un'organizzazione internazionale impegnata nella difesa e nella promozione dei diritti dei bambini. Save the Children Italia coordina STOP-IT (progetto finanziato dalla Commissione europea), che è l'altra hotline presente in Italia. Si tratta di un sito Internet (www.stop-it.org), attraverso il quale è possibile segnalare l'esistenza di materiale pedo-pornografico o pericoloso.

Associazione Italiana Internet Provider - Assoprovider
www.aiip.it

Si tratta di associazioni di provider che hanno supportato e condiviso, collaborando con le Forze di Polizia, le istituzioni e le aziende di settore, l'obiettivo di creare un ambiente normativo e tecnologico che fornisca protezioni ai minori che navigano in rete, attraverso la predisposizione di misure adeguate e compatibili con la rete e il coinvolgimento di famiglie ed educatori.

CONTRATTO

Il contratto di collaborazione figli-genitori per l'uso sicuro di Internet (dal "Codice di Autoregolamentazione "Internet e Minori")

A firma del minore
*(nome del minore)*_____

Sono consapevole che la possibilità di utilizzare il computer di famiglia e il permesso di accesso alla posta elettronica ed a Internet sono dei privilegi che mi verranno accordati esclusivamente se mi comporterò in modo corretto. Pertanto:

1) Prometto di rispettare le regole sull'uso di Internet stabilite dai miei genitori.

2) Prometto di rivolgermi immediatamente ai miei genitori se qualcosa o qualcuno mi fa sentire minacciato o spaventato.

3) Prometto di far supervisionare ai miei genitori ogni tentativo di incontrare un "corrispondente virtuale".

4) Prometto di non usare materiali o linguaggi inappropriati e di rivolgermi immediatamente ai miei genitori se trovo materiale sessualmente esplicito.

5) Prometto di usare il computer e la Rete soltanto per il tempo concordato con i miei genitori.

6) Prometto di non violare per nessun motivo le leggi sul diritto d'autore.

7) Prometto di non invadere gli spazi sul computer dei miei familiari e di accettare i controlli dei miei genitori sui miei ambiti.

8) Prometto di non rivelare mai a nessuno informazioni personali.

Ho letto attentamente e ho compreso le regole sopraccitate. Se per qualsiasi ragione dovessi violare le regole, resta inteso che tutti i miei privilegi per utilizzare il computer saranno revocati per un tempo che verrà stabilito esclusivamente dai miei genitori.

Firma del minore _____

Firma del genitore _____ Data_____

Il contratto di collaborazione figli-genitori per l'uso sicuro di Internet (dal "Codice di Autoregolamentazione "InternetInternet e Minori")

CONTRATTO

A firma del genitore
(nome del genitore) _____

Sono pienamente consapevole che uno dei miei doveri principali è quello di aiutare la mia famiglia a ottenere tutto il meglio che Internet può offrire, proteggendola dai pericoli che può nascondere. Partendo da questa premessa:

1) Prometto di migliorare le mie conoscenze sul mondo di Internet e sul linguaggio di mio figlio.

2) Prometto di non adottare misure drastiche sull'uso di Internet.

3) Prometto di non comportarmi come un poliziotto invadente.

4) Prometto di essere ragionevole nello stabilire regole di utilizzo del computer e di Internet.

5) Prometto di rispettare la dignità di mio figlio.

6) Prometto di ascoltare con calma e comprensione mio figlio.

7) Prometto di rappresentare un buon esempio per mio figlio.

8) Prometto di risolvere immediatamente insieme a mio figlio un problema legato all'uso di Internet.

9) Prometto di farmi coinvolgere da mio figlio.

Ho letto attentamente e ho compreso le regole sopraccitate. Sono cosciente che la mia cooperazione e il mio aiuto sono fondamentali affinché mio figlio sia in grado di usare in maniera sicura il mondo informatico e telematico.

Firma del minore _____

Firma del genitore _____ Data_____

PROVINCIA DI COMO
ASSESSORATO ALLA SICUREZZA E POLIZIA LOCALE

Dott. Roberto Zanetti
Vicepresidente

Dott. Marco Virdis
Dirigente Settore Polizia Locale

POLIZIA POSTALE E DELLE COMUNICAZIONI
COMPARTIMENTO PER LA LOMBARDIA

Dott. Salvatore Rossi
Dirigente del compartimento

ASSOCIAZIONE NAZIONALE POLIZIA DI STATO
SEZIONE DI COMO

Marcello Chirulli
Consigliere Nazionale

CENTRO STUDI SICUREZZA PUBBLICA

Dott. Maurizio Marinelli
Direttore del C.S.P. - Brescia

Ideazione e testi a cura di:

Dott.ssa Fabiola Treffiletti
Vice Questore Aggiunto
Compartimento Polizia Postale e delle Comunicazioni per la Lombardia

Dott. Giorgio Ferrara
Specialista Direttivo Amministrativo
Provincia di Como, Assessorato alla Sicurezza

Definizioni di Internet - glossario

ADSL	Acronimo di Asymmetric Digital Subscriber Line, è una tecnologia che permette l'accesso ad Internet ad alta velocità.
Allegato	È un file che può essere aggiunto ad una email. Potrebbe essere una fotografia come la tua canzone preferita. Potrebbe però anche essere qualcosa di dannoso per il tuo PC, come un virus. Ricorda che i bambini non devono mai aprire una email o un allegato che arriva da qualcuno che non conoscono.
Blog (abbreviazione di web log)	È solitamente definito blog un sito InternetInternet personale e non commerciale che utilizza un dato sistema di accesso.
Browser	È un programma che consente di navigare su Internet e visualizzare le pagine web. I browser più popolari sono Netscape Navigator e Microsoft Internet Explorer.
CD-ROM / DVD	Acronimo di "compact-disk, read-only memory" oppure di "digital video disk". Sono tipi di dischi di notevole memoria. I giochi, i film, software e molto altro vengono venduti su questi supporti. Nelle versioni –R (recordable) e –RW (re-writable) consentono di salvare informazioni e dati che possono essere trasferiti da un PC ad un altro.
Chat	Comunicazione in tempo reale su Internet. Si scrivono e si inviano messaggi che appaiono pressoché istantaneamente sullo schermo del computer della persona che sta partecipando alla chat.
Chatroom	Stanza virtuale dove si più chiacchierare in tempo reale. La chatroom è il luogo on-line ove si svolge la chat. Molte chat sono realizzate allo scopo di chiacchierare a proposito di argomenti specifici, musica, film, politica, etc.
Cookie	Un piccolo file che viene scaricato da alcuni siti Internet per memorizzare alcune informazioni sul proprio browser. Questi pacchetti includono informazioni come quelle di login o identificative di una registrazione, le preferenze del navigante, informazioni sul carrello della spesa (shopping cart). Il browser salva le informazioni e le ritrasmette quando si visita nuovamente il sito Internet. I cookies possono essere utilizzati per personalizzare ciò che si desidera vedere nella homepage di un sito o per tenere traccia delle differenti pagine che si sono visitate. Il browser può essere configurato in modo che avvisi quando i cookies vengono inviati. È sempre possibile rifiutare i cookies e cancellare quelli presenti nel browser.
Cronologia	Lista dei siti web visitati dall'utente del computer. Verificare la cronologia può essere importante per monitorare i siti visitati dai bambini.
Cyberbullying	Inviare o postare messaggi o immagini offensivi o cruenti su Internet o su di un sistema di comunicazione.
Cyberspazio	Si riferisce alla rete di tutti i computer su Internet. Il termine distingue il mondo reale/fisico dal mondo virtuale o basato sui computer.
Dialer	È un programma che installandosi all'insaputa dell'utente effettua chiamate a numeri remoti attraverso la normale linea telefonica, senza il consenso del proprietario del PC. Il fenomeno dei dialer ha colpito in migliaia di utenti che ignari effettuavano chiamate dai costi esorbitanti.
Download	Scaricare informazioni su proprio computer. Si può scaricare da Internet, da un disco, o da un altro computer.
email (posta elettronica)	È un servizio che permette alle persone di trasmettere messaggi di testo, immagini o suoni dal proprio computer ad un altro in qualsiasi luogo del mondo. Per trasmettere messaggi è necessario un account di posta elettronica e conoscere l'indirizzo email dell'altra persona.
Emoticons	Facce animate che esprimono differenti stati d'animo o emozioni che possono essere trasmessi con email, chat e Instant messaging. Gli emoticons sono il modo di rappresentare a qualcuno online come ci sentiamo in quel momento.
File sharing (programmi)	Programmi che consentono a differenti utenti di accedere simultaneamente allo stesso file. Solitamente questi programmi vengono utilizzati per scaricare illegalmente musica, film e software.
Gruppo di discussione	Un gruppo di persone che si scambia informazioni su di un topic.
Haker	Termine popolare per definire qualcuno che accede illegalmente a computer o a sistemi informatici altrui.

Definizioni di Internet - glossario

Hardware	Componente per il funzionamento del computer, come la tastiera, il mouse, il monitor e le parti elettriche.
Homepage	Pagina web che nel proprio browser è configurata come pagina iniziale, oppure pagina principale di qualsiasi sito Internet.
HTLM	Acronimo di Hypertext Markup Language. È il formato di codifica utilizzato per creare documenti sul word wide web e controllare come le pagine web appaiono.
HTTP	Acronimo di Hypertext Transfer Protocol. Metodo standard utilizzato dai computer per comunicare via word wide web.
Indirizzo	Una serie di lettere e numeri che identificano una posizione. Su Internet, digitare un indirizzo consente di trasmettere o ricevere informazioni da una specifica fonte. Si può digitare un indirizzo di posta elettronica, di un sito web o di una rete. Per esempio l'indirizzo email della Provincia è azionisicure@provincia.como.it e il sito web è www.azionisicure.it
Instant messaging	Un servizio che permette alle persone di trasmettere e ricevere messaggi pressoché istantaneamente. Per inviare messaggi utilizzando l'IM è necessario effettuare il download di un software e conoscere l'indirizzo IM della persona che utilizza il medesimo programma di Instant Messaging.
Internet	Una rete di milioni di computer collegati da tutto il mondo. La rete Internet permette ai computer di scambiarsi informazioni utilizzando le linee telefoniche, i cavi in fibra ottica o collegamenti satellitari e wi-fi. Anche definito "la Rete".
Internet Service Provider (ISP)	Compagnia che offre il collegamento ad Internet per i consumatori
Intranet	Rete privata interna ad un ente o un'azienda
Link	Immagine o porzione di testo che, quando cliccata, permette connessioni elettroniche. Queste connessioni accedono ad altro materiale Internet come immagini, suoni, animazioni, video oppure altre pagine web.
Motore di ricerca	Sistema di ricerca di informazioni presenti sul world wide web ottenute sulla base di specifiche parole chiave. Informazioni che poi vengono offerte attraverso una lista di argomenti collegati alla parola chiave inserita.
MP3	File di musica digitale. Gli MP3 permettono di ascoltare la musica sul proprio computer.
Multimediale	Combinazione di differenti tecnologie che permettono di vedere disegni grafici, animazioni, effetti sonori e testo.
Navigare	Azione consistente nel movimento da una pagina ad un'altra e da un sito web ad un altro. Sono spesso utilizzati i sinonimi surfare o browsing.
Netiquette	Comportamento educato, corretto, civile e compito tenuto su Internet
Newsgroup	Bacheca virtuale di messaggi o gruppo di discussione con specifico soggetto che si svolge online. I partecipanti ad un newgroup conducono discussioni postando messaggi e rispondendo a messaggi postati da altri.
Offline	Si riferisce al non essere connesso ovvero al non essere su Internet.
Online	Espressione per descrivere l'essere connesso ad Internet oppure utilizzare attivamente Internet.
Parole chiave (keyword)	Parole utilizzate quando si cercano informazioni attraverso i motori si ricerca.
Password	Parola segreta utilizzata per accedere ad Internet o ad un servizio online che consente di confermare la propria identità.
Pharming	Tipo di truffa online perpetrata attraverso l'aggressione degli indirizzi Internet. L'utente crede di digitare un indirizzo valido ed incoscientemente viene dirottato ad un sito illegale che ruba i propri dati personali.
Phisching	Tipo di truffa online che utilizza le email allo scopo di "pescare" (fish) dall'utente informazioni private imitando le modalità di comunicazione utilizzate da banche o altre compagnie. La phisching email solitamente contiene un collegamento ad un sito illegale. I truffatori copiano l'impostazione grafica del sito della banca o della compagnia in modo che appaia pressoché identico ed induca in errore l'utente malcapitato.
Pirateria	Duplicazione illegale di brani musicali, film o software coperti da copyright.

Definizioni di Internet - glossario

Politiche sulla privacy	Consiste nella politica adottata da un ente o da una organizzazione operante sul web (e non solo) circa la gestione dei dati personali raccolti.
Postare	Lasciare/inviare un messaggio ad un newsgroup o ad un blog
Preferiti	Un elenco di indirizzi Internet ai quali si desidera accedere rapidamente attraverso il salvataggio nel proprio browser. Ad esempio www.poliziadistato.it può essere aggiunto ai preferiti per trovare rapidamente suggerimenti anche sulla sicurezza in Internet.
Query	Una richiesta di informazioni circa uno specifico argomento. È una query anche ciò che si digita nell'apposito spazio di un motore di ricerca.
Sistemi di controllo dei contenuti	Sono dei programmi che consentono di filtrare e bloccare la navigazione sui siti ritenuti dannosi. È possibile aggiungere o rimuovere un sito dalla lista "non-andare".
Sito web	Collezione di "pagine" o file collegati tra loro e disponibili sul world wide web
Spam	email non desiderata proveniente da qualcuno che non si conosce. È solitamente utilizzata per vendere qualcosa, ma può nascondere insidiose truffe.
Spyware	Programma in grado di identificare le abitudini di navigazione nel web o di apportare modifiche alle impostazioni del computer senza il consenso o il controllo dell'utente.
Streaming	Visualizzazione o scambio attraverso Internet di filmati, brani musicali o altri tipo di file multimediali. Concetto assimilabile alla televisione o alla radio.
Tempo reale (real time)	Si riferisce all'essere presente in quel momento su Internet. Esprime un concetto simile a quello di essere in diretta nelle trasmissioni televisive.
Temporary Internet file (file temporanei)	È una cartella presente all'interno della memoria del computer che può far conoscere tutti i siti visitati da chi lo utilizza, ad esempio un bambino. Ogni volta che si apre una pagina web, il computer automaticamente salva una copia del file e della grafica del sito visitato nella cartella "temporary Internet files".
Topic	Argomento o soggetto di una discussione.
Trojan	È un particolare programma che installandosi all'insaputa dell'utente è in grado (come un vero e proprio Cavallo di Troia) di rendere accessibile il computer o l'intera rete da parte di individui non autorizzati.
Virus	Un programma per computer che distrugge i file o, come si dice, manda il crash il PC. I virus possono essere mandati via email o attraverso i programmi di file-sharing. Un buon anti-virus e l'evitare il download da persone che non si conoscono riduce incredibilmente il rischio di danneggiamento al computer.
Webmaster	Persona responsabile dell'amministrazione di un sito web.
Wi-Fi	Abbreviazione di Wireless Fidelity. Tecnologia che permette la connessione ad Internet o l'interconnessione di più computer senza la necessità di fili.
WWW world wide web	Un infinito numero di giochi, siti web, immagini, suoni, informazioni, racconti e molto altro ancora, tutti connessi attraverso Internet. Si può surfare il web attraverso il proprio browser e trovare informazioni inerenti pressoché qualunque cosa. Il web costituisce solo uno dei servizi di Internet. Gli altri servizi su Internet includono le chat, i newsgroup e le email. I siti web sul world wide web hanno un indirizzo che prepone "www".

PER MAGGIORI APPROFONDIMENTI E INFORMAZIONI SUGLI ARGOMENTI TRATTATI VISITATE IL SITO

www.guidaallasicurezza.it

www.guidaallasicurezza.it

"Internet offre un mare
di opportunità
tutte da cogliere,
ma è importante
imparare a navigare
senza rischi".

Il Vicepresidente
della Provincia di Como

Dott. Roberto Zanetti

PER AVERE CONSIGLI UTILI O INVIARE SUGGERIMENTI E RICHIESTE
CONTATTATECI ALL'INDIRIZZO DI POSTA ELETTRONICA

info@guidaallasicurezza.it