Polizia di Stato

CO RE COM PUGLIA
Comitato Regionale per le Comunicazioni

Consiglio Regionale della Puglia

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

*SI RINGRAZIA **AUCHAN** E **IPERCOOP** PER LA GENTILE COLLABORAZIONE.*

Così nasce il progetto ***"Comunicainsicurezza"***

Pc/tablet/smartphone, sono oggetti che ormai fanno parte della nostra vita e della nostra famiglia, esattamente come la tv.
Il mondo entra nelle nostre case e le nostre case possono facilmente entrare nel mondo.
Una vera e propria rivoluzione nelle comunicazioni che ha cambiato, certamente migliorandolo, il mondo del lavoro e dell'intrattenimento degli adulti e che ha profondamente modificato, la crescita, la formazione e la socialità dei ragazzi/ragazze, a cominciare dai più piccoli.
Un mondo pieno di opportunità, ma anche di pericoli.
Un mondo in cui è affascinante ed avvincente avventurarsi, ma nel quale occorre entrare ben sapendo come evitare i pericoli, proprio per poter sfruttare al meglio tutte le opportunità.

Co.Re.Com.* Puglia** (Comitato Regionale per le Comunicazioni) e ***Polizia di Stato - Reparto Specialistico della Polizia Postale e delle Comunicazioni Puglia - nell'ambito di una già rodata collaborazione, hanno fuso le proprie competenze, le proprie esperienze e le proprie professionalità in questo strumento che vuole essere una sorta di vademecum, una raccolta di informazioni semplici ed immediate per tutti coloro che comunicano tramite i cosiddetti 'new media' e, in particolare, per i genitori e per i ragazzi/e.
Se sei un ragazzo/a, ***"Comunicainsicurezza"*** ti spiegherà come equipaggiarti per viaggiare nelle tante opportunità di questo nuovo, affascinante ed immediato modo di comunicare, senza incorrere nei pericoli e proteggendoti dai rischi.
Se sei un genitore, ***"Comunicainsicurezza"*** ti farà conoscere meglio questo mondo in cui i ragazzi/e imparano, crescono, si conoscono, stringono amicizie, insomma vivono e comunicano virtualmente, e ti farà capire come evitare che in questo mondo virtuale i ragazzi/e incontrino pericoli reali.

http://corecom.consiglio.puglia.it/comunicainsicurezza
www.poliziadistato.it
www.commissariatodips.it

La Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni nasce all'interno dello scenario che, grazie all'evoluzione tecnologica e alla crescita culturale del Paese, ha reso la rete Internet un mezzo indispensabile per lo scambio di informazioni, l'accesso alle grandi banche dati, l'esecuzione di transazioni e disposizioni finanziarie , l'ideazione e la creazione di nuove attività professionali: la rapida diffusione dell'uso di questo nuovo strumento di comunicazione ha messo in evidenza i punti di debolezza della Rete, soprattutto riguardo alla sicurezza informatica; in questo campo la Polizia di Stato, attraverso il reparto specialistico della Polizia Postale e delle Comunicazioni – creato con la legge di riforma dell'Amministrazione della Pubblica Sicurezza – è all'avanguardia nell'azione di prevenzione e contrasto della criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione. Il principale sforzo operativo della Polizia Postale e delle Comunicazioni è nel trovare argini di controllo sempre più adeguati alle nuove frontiere tecnologiche utilizzate dalla delinquenza.

I compartimenti e le sezioni

La Polizia Postale e delle Comunicazioni è presente in modo capillare sul territorio nazionale attraverso **20 compartimenti e 80 sezioni** impegnati nella lotta contro le attività illecite. Dislocazione geografica e conoscenza del territorio sono caratteristiche fondamentali per un'azione investigativa efficace.
I compiti istituzionali comprendono:
• la prevenzione e repressione dei crimini postali ed informatici;
• la tutela dei servizi postali, di bancoposta e di telecomunicazione;
• il controllo del corretto utilizzo delle licenze radio-amatoriali degli apparati, degli impianti, delle emittenti radio e televisive;
• il controllo degli esercizi che commercializzano materiali o apparecchiature di telecomunicazione soggette a marcatura e omologazione;
• il raccordo operativo con gli Ispettorati Territoriali del Ministero delle Comunicazioni nelle attività di controllo amministrativo di comune interesse;
• la prevenzione e repressione dei reati legati al commercio elettronico.

I Comitati Regionali per le Comunicazioni (Co.Re.Com.) sono organismi delle Regioni che si occupano di telecomunicazioni e del sistema radiotelevisivo a livello locale.

Il Co.Re.Com. Puglia

Il Co.Re.Com. ha la funzione di gestire, governare e controllare il sistema delle comunicazioni sul territorio della Regione Puglia: è al tempo stesso organo del Consiglio Regionale, organo delegato dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) e referente operativo del Ministero dello Sviluppo Economico.
Quale organo regionale, il Co.Re.Com. svolge funzioni di garanzia, di consulenza, di supporto nei confronti della Regione e di gestione delle funzioni nel campo della comunicazione spettanti alla Regione secondo le leggi statali e regionali.
Quale organo dell'Autorità per le Garanzie nelle Comunicazioni il Co.Re.Com. esercita le funzioni proprie e delegate assegnate con apposite convenzioni.

FUNZIONI PROPRIE:

• per conto del Ministero dello Sviluppo Economico il Co.Re.Com.predispone le graduatorie delle emittenti televisive locali per l'assegnazione dei contributi pubblici (D.M. 292/2004);
• cura la corretta applicazione ed il rispetto delle norme per la parità di accesso ai mezzi di informazione in periodo elettorale e non - Legge 28/2000 (detta "Par condicio").

FUNZIONI DELEGATE:

• tutela dei minori in riferimento al settore radiotelevisivo locale;
• esercizio del diritto di rettifica nell'informazione radiotelevisiva locale;
• vigilanza sulla pubblicazione di sondaggi sui mezzi di comunicazione di massa locali;
• conciliazione e definizione delle controversie tra gestori del servizio di telecomunicazione e utenti in ambito locale;
• monitoraggio TV locali - Vigilanza sul rispetto degli obblighi di programmazione e delle disposizioni in materia di esercizio dell'attività radiotelevisiva locale, inclusa la tutela del pluralismo, mediante il monitoraggio delle trasmissioni dell'emittenza locale secondo le linee-guida dettate dall'Autorità e la successiva verifica di conformità alla vigente disciplina in materia di diffusione radiotelevisiva, ed eventuale avvio delle conseguenti istruttorie procedimentali;
• tenuta del Registro degli Operatori di Comunicazione (R.O.C.);
• vigilanza in materia di sondaggi sui mezzi di comunicazione di massa in ambito locale.

Partiamo equipaggiati

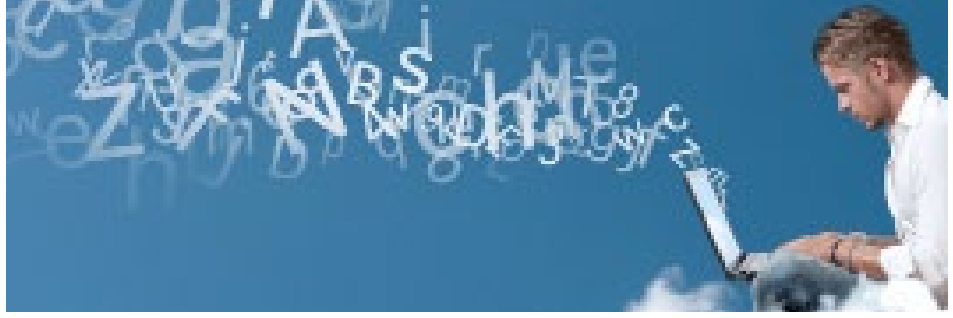
Avete appena acquistato uno strumento che vi aiuterà a migliorare il vostro modo di lavorare, studiare, comunicare, divertirvi. Prima di iniziare ad utilizzarlo, eccovi alcuni consigli per "equipaggiare" il vostro nuovo pc/tablet/smartphone e utilizzarlo in sicurezza!

- Installate e tenete aggiornati un buon antivirus e un firewall che proteggano continuamente il vostro pc/tablet/smartphone e chi lo utilizza;
- fate backup regolari dei dati più importanti;
- custodite le informazioni personali;
- prima di inserire i vostri dati personali su internet controllate che siano presenti i segni che indicano la sicurezza della pagina: la scritta https nell'indirizzo e il segno del lucchetto;
- utilizzate password sicure e tenetele riservate, meglio se lunghe - con almeno otto caratteri - , con maiuscole e minuscole, numeri e simboli;
- non usate la stessa password per siti diversi;
- non tenete il vostro pc/tablet/smartphone allacciato alla rete quando non lo usate: è consigliato piuttosto disconnetterlo.

Ricordate:

- **il Corecom Puglia** è pronto ad aiutarvi nella risoluzione di controversie con gestori di telefonia fissa, mobile, traffico internet, pay tv;

- **la Polizia Postale e delle Comunicazioni** contrasta il crimine informatico e tutela la comunità e i singoli utenti dalle minacce in Rete.



ATTENZIONE

SE SEI UN GENITORE:

Cerca di avere una preparazione informatica quantomeno analoga a quella dei tuoi figli per rispondere alle loro domande e predisporre le opportune misure di protezione del nuovo pc/tablet/smartphone. Se possibile, posizionalo in una stanza centrale della casa, piuttosto che nella camera dei ragazzi/e. Ti consentirà di dare anche solo una fugace occhiata ai siti visitati senza che tuo figlio/a si senta "sotto controllo".
Non lasciare troppe ore i bambini/e e i ragazzi/e soli in rete, stabilisci quanto tempo possono passare navigando su internet: limitare il tempo che possono trascorrere on-line significa limitare di fatto l'esposizione ai rischi della Rete.
Controlla periodicamente il contenuto dell'hard disk e imposta la cronologia di navigazione in modo che mantenga traccia per qualche giorno dei siti visitati da tuo figlio.
Per la navigazione usa software "filtri" che evitino l'esposizione a contenuti inadeguati da parte dei più piccoli, stabilendo un elenco predefinito di siti accessibili e di siti "bloccati". È opportuno verificare periodicamente che i filtri funzionino in modo corretto e tenere segreta la parola chiave. Insegna ai tuoi figli l'importanza di non rivelare in Rete i dati personali come nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici.

ATTENZIONE

SE SEI UN RAGAZZO/A:

Non scaricare programmi se non conosci bene la provenienza: potrebbero contenere virus che danneggiano il tuo pc/tablet/smartphone, spyware che violano la privacy e rendono accessibili informazioni riservate.

La promessa di ricariche facili, di regali gratuiti, di vantaggi fantastici che arrivano via sms o nelle chat da adulti sconosciuti devono metterti in allerta: alcuni truffatori e criminali utilizzano questi mezzi per farti aderire a costosi abbonamenti a pagamento, o per carpire la tua fiducia e suggerirti di fare cose non adatte alla tua età.

Ricorda che se qualcuno vuole offrirti un vantaggio troppo facile, senza neanche conoscerti, probabilmente ti prende in giro!

Iniziamo a navigare

La posta elettronica/e-mail

Con la posta elettronica si trasmettono messaggi in tempo reale da un pc/tablet/smartphone ad un altro, utilizzando un proprio indirizzo e-mail da cui si scrive all'indirizzo e-mail del destinatario. Occorre sempre verificare l'identità reale di chi vi scrive: non basta che ci siano un nome ed un cognome per essere sicuri che un indirizzo corrisponda davvero alla persona che si chiama in quel modo. Non fornite il vostro indirizzo e-mail se non siete certi dell'identità di chi ve lo chiede e dell'uso che intende farne. Non aprite messaggi di posta elettronica di cui non riconoscete la provenienza, potrebbero nascondere pericoli per il vostro pc/tablet/smartphone.
I messaggi di posta elettronica non sono sicuri al cento per cento, quindi non è opportuno inserirvi informazioni personali e/o riservate.
Fate attenzione ai falsi messaggi allarmistici, richieste disperate di aiuto, offerte imperdibili, richieste di dati personali per "aggiornare il tuo account": diffidate di tutti i messaggi di questo tono e attivate un sistema per individuarli, come il filtro Smart Screen® di Windows® Internet Explorer®
Se non conoscete il mittente non aprite l'e-mail né eventuali allegati: possono contenere virus o spyware in grado di alterare il funzionamento del pc/tablet/smartphone. Date le stesse indicazioni ai ragazzi più grandi.

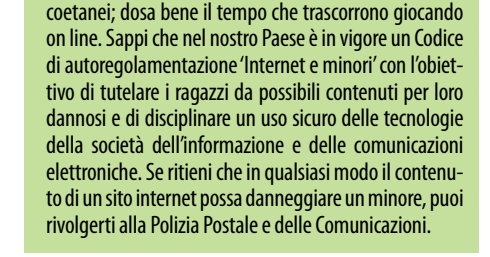
Attenzione! Qualcuno si sostituisce a Polizia Postale!
La Polizia Postale non blocca i computer né richiede pagamenti in denaro per sbloccare i pc. É un virus informatico!!!!

La chat

La chat è un modo di dialogare in tempo reale, ancora più veloce della posta elettronica. Simula una conversazione telefonica, ma avviene tramite la tastiera del vostro pc/tablet/smartphone. Per chattare bisogna registrarsi in una chat e scegliere un 'nickname', ossia un nome di fantasia che da quel momento vi identifica sulla chat e, se lo scegliete diverso dal vostro nome e cognome, nasconde la vostra reale identità. Da quel momento si apre una finestra sul vostro schermo e sarete in contatto con una o con tantissime persone, ovunque esse si trovino. In chat non è consigliabile rivelare i vostri dati sensibili (nome, cognome, indirizzo, numero di telefono) se non siete assolutamente certi dell'identità del vostro interlocutore. Sappiate comunque che in ogni momento l'amministratore del sistema può identificare chi chatta tramite l'indirizzo IP dello strumento da cui chattate e si può denunciare chi viola le regole.

Giochi on line

Se si utilizza un gioco on line si resta connessi alla Rete per tutto il tempo in cui si gioca. Spesso per consentirvi di giocare on line, i siti che caricano i giochi chiedono di registrarvi e di fornire i vostri dati personali. Siate prudenti!
Non è consigliabile giocare on line per troppo tempo.
Fate attenzione ai siti che, mentre giocate, vi propongono di scaricare giochi diversi da quello che avete scelto.



ATTENZIONE
SE SEI UN GENITORE:
Consenti ai ragazzi l'uso della tua posta elettronica solo in tua presenza e del tuo indirizzo e-mail solo dietro tua autorizzazione; spiega ai ragazzi quali sono i rischi di un utilizzo improprio della posta elettronica; verifica che i ragazzi entrino in chat controllate e frequentate solo da coetanei; dosa bene il tempo che trascorrono giocando on line. Sappi che nel nostro Paese è in vigore un Codice di autoregolamentazione 'Internet e minori' con l'obiettivo di tutelare i ragazzi da possibili contenuti per loro dannosi e di disciplinare un uso sicuro delle tecnologie della società dell'informazione e delle comunicazioni elettroniche. Se ritieni che in qualsiasi modo il contenuto di un sito internet possa danneggiare un minore, puoi rivolgerti alla Polizia Postale e delle Comunicazioni.

ATTENZIONE
SE SEI UN RAGAZZO/A:
Non fornire il tuo indirizzo di posta elettronica con leggerezza e non rispondere a messaggi di posta elettronica che ti sembrano provenire da estranei o che ti lasciano perplesso. Se hai dubbi parlane sempre con i tuoi genitori; non chattare con persone che non conosci o della cui identità non sei certo, non fornire tue informazioni personali come numero di telefono, indirizzo, nome della tua scuola e, se vieni contattato da qualcuno che non ti sembra un tuo coetaneo o che ti chiede qualcosa di strano, parlane sempre con i tuoi genitori; non trascorrere troppo tempo giocando on line, perché se non hai un abbonamento internet che te lo consente, potrebbe costare molto e se giochi per troppo tempo potrebbe farti male alla salute.

I social Network

I social Network

Un social network è una 'rete sociale', ossia un gruppo di persone legate tra loro da rapporti di amicizia. Il social network virtuale è una rete di amicizie che ciascuno di noi può crearsi on line utilizzando siti e servizi web in cui è possibile crearsi **un profilo** pubblico o semi-pubblico, una rete di **contatti (amicizie)**.
La grande innovazione introdotta da questo strumento consiste nella possibilità di essere in contatto in tempo reale con amici in tutto il mondo e di seguire attraverso il proprio profilo anche i profili, le amicizie e gli accadimenti della vita di ogni giorno dei vostri amici.
Per entrare a far parte di un social network online occorre costruire il proprio profilo personale, partendo da informazioni come il proprio indirizzo e-mail fino ad arrivare agli interessi e alle passioni. A questo punto è possibile invitare i propri amici a far parte del proprio network, i quali a loro volta possono fare lo stesso, cosicché ci si trova ad allargare la cerchia di contatti con gli amici degli amici e così via.
L'uso dei social network è diffuso soprattutto tra i giovani e i giovanissimi. A fronte degli enormi vantaggi di questo modo di socializzare e restare in contatto, vi sono anche una serie di accortezze che ciascuno di voi deve tenere a mente per evitare di rendere 'pubblico' anche ciò che vuole mantenere 'privato'.
L'uso dei social network **è vietato ai minori di 13 anni e sconsigliato ai minori di 14 anni** perché la loro inesperienza nei rapporti sociali, la curiosità verso gli altri e l'entusiasmo per la facilità con cui vengono condivisi immagini, storie, video, potrebbe indurli a sottovalutare i rischi che da queste eccessive condivisioni potrebbero derivare a se stessi e alle loro famiglie. Tuttavia, a qualsiasi età, è sempre opportuno nella fase di creazione del proprio profilo su un social network, scegliere le impostazioni più alte per garantire la propria privacy e, quindi, consentire l'accesso e la visibilità del proprio profilo solo agli amici e non a tutta la Rete, lasciandosi la possibilità di scegliere, volta per volta, a chi rendere visibile cosa.

ATTENZIONE

SE SEI UN GENITORE:

Piuttosto che vietare a tuo figlio/a di iscriversi ad un social network, cerca di fargli capire l'importanza di non rivelare in Rete dati personali; ricordagli/ le che è **pericoloso, oltre che vietato, pubblicare in Internet foto e video di sé o di altri, specie se si tratta di minori inconsapevoli di apparire on line.** Sappi che per controllare la 'vita in Rete' di tuo figlio/a, specie se piccolo/a, puoi installare programmi e software in grado di filtrare i siti web e che alcuni social network consentono di seguire in tempo reale sul tuo profilo l'attività del profilo di tuo figlio/a .
Spiega serenamente a tuo figlio/a tutti i pericoli che può incontrare nella Rete e fagli capire che può rivolgersi a te in qualsiasi momento e in qualsiasi situazione che gli sembri strana, imbarazzante, nuova. Cerca di dosare il tempo che ogni giorno trascorre con i suoi amici 'virtuali', ricordandogli/le quanto è più bello e divertente giocare e trascorrere del tempo all'aria aperta con i suoi amici 'reali'.

ATTENZIONE

SE SEI UN RAGAZZO/A:

Ricorda che le tue immagini e quelle degli altri sono una cosa privata, da proteggere. Non pubblicare foto o filmati fatti da te o dai tuoi amici in pagine visibili a tutti. Una volta pubblicati, foto e filmati, non sono più controllabili e potrebbero finire ovunque. Non fornire mai informazioni su di te, sulla tua famiglia, sulla tua casa, a persone che non conosci e non accettare mai di fornire il tuo indirizzo, il tuo numero di telefono o, peggio, di incontrare, persone conosciute in Rete senza informare i tuoi genitori. Se vieni contattato da qualcuno che non conosci, prima di rispondere informa sempre i tuoi genitori.
Ricorda di tenere segreta la tua password di accesso al tuo profilo, per evitare che altri, magari anche solo amici e compagni di classe per farti uno scherzo, possano entrare in un social network con il tuo nome e diffondere informazioni che ti riguardano.

Cyber Pericoli

Cyberpedofili

Il pedofilo telematico è prevalentemente un individuo socialmente inserito, di sesso maschile, buon titolo di studio, nessun precedente penale, spesso celibe.
Il Cyberpedofilo cerca innanzitutto di creare un clima di fiducia e di amicizia, fingendosi un coetaneo dei bambini; si assicura più di una volta che il bambino sia solo e che comunque non sia controllato da persone adulte.
Gradatamente introduce argomenti a sfondo sessuale, inviando, a volte, fotografie pedopornografiche, per convincere il minore che tali comportamenti siano normali e che gli altri bambini sono sessualmente attivi.
Accende la curiosità sessuale del bambino , prescrivendogli compiti come compiere atti sessuali.
L'approccio continua tramite telefono o via e-mail, fino a quando tenta di convincere il bambino a un incontro reale, faccia a faccia.

Cyberbullismo

Il cyber bullismo si può manifestare in Internet, in chat , quando si prende di mira qualcuno – ragazzo/a - , lo si aggredisce verbalmente, lo si prende in giro estromettendolo dalla lista di discussione, quando lo si molesta o lo si minaccia.
Registrare e pubblicare confidenze fatte in chat, costituisce una forma di violenza psicologica.

ATTENZIONE
SE SEI UN GENITORE:

I giovani condividono troppi dettagli sui social network esponendosi al grooming cioè all'adescamento in Internet o al cyber bullismo.

Anche gli sconosciuti possono inviare messaggi personali o commenti sui profili pubblici. Parla con i tuoi figli della potenziale pericolosità di richiamare con il telefonino numeri sconosciuti da cui provengono squilli o chiamate mute. In passato si è trattato di una modalità con cui i pedofili adescavano i minori.

Sviluppa il senso critico dei tuoi figli e le loro competenze informatiche.

Spiega ai tuoi figli i pericoli del sesso on – line.

ATTENZIONE
SE SEI UN RAGAZZO/A:

Ignora i cyber-bulli che ti insultano.
Non provocarli con nomi che possano incoraggiare il loro comportamento molesto.
Ricorda che taggare le foto ti espone al rischio di cyber bullismo.
Non fornire mai a nessuno l'indirizzo di casa, il numero di telefono o il nome della scuola o dei luoghi di svago che solitamente frequenti.
Non prendere appuntamenti con persone conosciute in Internet, anche se coetanei, senza comunicarlo ai genitori.
Fai attenzione ai discorsi fatti in chat, a quello che si dice di strano o sul sesso.
Non rispondere mai a domande, mail o a messaggi molesti o allusivi, soprattutto se a sfondo sessuale.
Allarma i genitori se noti o ti inviano fotografie di persone adulte o minori nudi.
Le tue foto, i tuoi messaggi e le tue conversazioni possono essere viste da sconosciuti.
Non postare nulla che consideri personale o riservato e di cui potresti pentirti in futuro.

Cyber Pericoli

Il Cyber -stalking

Il Cyber stalker è un persecutore che, celandosi dietro un pc/tablet/smartphone, entra nella vita delle potenziali vittime , per rimanervi a lungo, generando uno stato permanente di preoccupazione, ansia e terrore, con epiloghi molto spesso tragici. **In Italia lo stalking è un reato, introdotto con la legge 38/2009.**

ATTENZIONE
SE SEI UN GENITORE:

Fai attenzione se tuo figlio/a si comporta in modo diverso dal solito, come ad esempio:

- mostra ansia o rifiuta categoricamente di farti vedere il suo telefonino o lo schermo del pc/tablet/smartphone mentre naviga o è connesso
- consuma molto velocemente il credito telefonico e non ti dà spiegazioni circa i suoi consumi
- mostra ansia e preoccupazione quando squilla il telefonino o mentre è connesso senza spiegarne spontaneamente il perché
- modifica i ritmi sonno-veglia (dorme troppo, dorme poco, ha incubi) o il comportamento alimentare e il rendimento scolastico.

ATTENZIONE
SE SEI UN RAGAZZO/A:

Se concedi la possibilità a sconosciuti di accedere alla tua casella di posta, al tuo blog, al tuo profilo di social network segnala immediatamente agli amministratori dei vari servizi web eventuali comportamenti indesiderati.
Dietro alla schermo di un pc/tablet/smartphone si nascondono intenzioni anche molto diverse: le parole scritte, gli emoticons, le immagini che ricevi da uno sconosciuto possono far nascere in te sentimenti reali verso persone che non esistono.
Se la tua relazione d'amore o di amicizia virtuale ti fa sentire a disagio, parlane con qualcuno di cui ti fidi: ricorda che un amore o un'amicizia autentica non generano, di solito, sensazioni così negative.
Considera un gioco le relazioni sentimentali che nascono su internet: un incontro reale con qualcuno conosciuto nel mondo virtuale ti espone sempre al rischio di trovare una persona molto diversa da quella che pensavi, magari anche pericolosa.
Non rispondere mai a messaggi provocatori, offensivi e minacciosi pubblicati sugli spazi web personali: le tue risposte possono alimentare l'ossessione del potenziale stalker. Annota i tempi e i luoghi virtuali degli atti persecutori, i contenuti dei messaggi minatori e rivolgiti alla Polizia Postale e delle Comunicazioni.
Se le attenzioni virtuali di una persona conosciuta sul web si fanno costanti, minacciose, offensive, o comportano la rivelazione pubblica di immagini e contenuti personali forse sei vittima di cyberstalking: segnala i comportamenti, la tempistica dei contatti, i contenuti diffusi senza il tuo consenso al sito **www.commissariatodips.it** in modo che esperti della materia possono aiutarti a capire cosa fare.

Sexting

La pubblicazione di foto, l'aggiornamento dei messaggi di stato, la condivisione di SMS in rapida successione e la compagnia virtuale degli amici costituisce la normalità per gli adolescenti di oggi. Ma questa cultura di connessione continua crea anche un ambiente in cui gli adolescenti possono prendere decisioni impulsive di cui potrebbero pentirsi. Per "sexting" si intende lo scatto e l' invio di foto discinte e sessualmente esplicite di sè ad amici, fidanzati, tramite SMS, video o e-mail. Il sexting è una realtà ben radicata tra gli adolescenti. Lo fanno per mettersi in mostra, dichiarare interesse nei confronti di qualcuno o per dimostrare il proprio impegno verso qualcuno.
Il vero problema nasce dalla condivisione indiscriminata di tali contenuti. Come fin troppi adolescenti hanno già scoperto a proprie spese, il destinatario di questi messaggi entra in possesso di immagini o materiale altamente compromettente che può essere facilmente pubblicato su un sito di social network o inviato ad altri tramite e-mail o SMS.

ATTENZIONE
SE SEI UN GENITORE:

Non attendere che accada qualcosa a tuo figlio/a o all'amico di tuo figlio/a : parla con i tuoi figli delle conseguenze del sexting. Una foto, una volta inviata e pubblicata, non può più essere recuperata e potrebbe essere vista da insegnanti, genitori o l'intera scuola ecc.

Fai leva sulla sua responsabilità. **Se trasmette foto compromettenti o imbarazzanti ad altri, diventa distributore di pornografia, un crimine perseguito per legge.**

La Televisione

La televisione è stata ed è lo strumento tecnologico più pervasivo, presente in tutte le case e ormai visibile anche su pc/tablet/smartphone!

La televisione è stata ed è lo strumento tecnologico più pervasivo, presente in tutte le case e ormai visibile anche su pc/tablet/smartphone!
Nonostante la diffusione dei Nuovi Media, è ancora molto presente nella vita dei bambini e dei ragazzi. É sempre più difficile individuare il ruolo educativo che questa può assumere. I Nuovi Media stanno influenzando e cambiando il concetto tradizionale di televisione. Certamente la tv è in naturale declino considerata l'evoluzione dei pubblico: i giovani si "dedicano" alla nuova tecnologia e gli anziani rimangono legati all'utilizzo della "vecchia TV".
Per tanti anni la televisione ha svolto la funzione di baby sitter a cui far ricorso nei momenti in cui si era impegnati. Ricordate? Si è parlato per molto tempo di generazione bim bum bam!!! Non si è fatto caso ai contenuti. Molto spesso il televisore è stato sintonizzato, in casa propria o dei nonni, su programmi non proprio consigliati ai minori. Non si è fatto caso all'utilizzo eccessivo o all'isolamento che poteva produrre. Si è scoperto pian piano che la televisione poteva produrre dipendenza e che la visione di particolari programmi avveniva nelle ore notturne fuori dal controllo dei genitori. Purtroppo l'assuefazione a programmi spesso privi di contenuti non sembra essere di rilevante importanza per i nostri giovani. Nella tv generalista vi è una scarsa presenza di programmi per bambini e ragazzi. L'arrivo della tv digitale ha portato sul video tanti canali con programmi dedicati ai bambini. Sui canali satellitari, poi, ci sono programmi per bambini anche 24 ore su 24. Esistono, addirittura, programmi dedicati alla fascia di età che va da 0 a 3 anni. La presenza di questi canali tuttavia, non deve sollevare nessuno dalla responsabilità di vigilare e selezionare i programmi.

ATTENZIONE
SE SEI UN GENITORE:

Sappi che le emittenti televisive hanno sottoscritto un Codice di autoregolamentazione chiamato Media e Minori e che si sono impegnate a:
- migliorare la qualità delle trasmissioni destinate ai minori, ad aiutare le famiglie e il pubblico più giovane ad un uso corretto e consapevole della Tv;
- sensibilizzare sui problemi dell'infanzia tutte le figure professionali coinvolte nella preparazione dei programmi;
- rispettare la persona, senza strumentalizzazioni e intrusioni nella vita familiare;
- non trasmettere immagini di minori che siano autori, testimoni o vittime dei reati, e in ogni caso, garantire l'anonimato;
- non utilizzare minori disabili o con gravi patologie a scopi propagandistici in contrasto con la loro dignità;
- non intervistare minori in situazioni di crisi (fuggiti da casa, che abbiano tentato il suicidio, implicati in giri di prostituzione o che abbiano genitori in carcere);
- impedire la partecipazione a dibattiti sul loro eventuale affidamento ad un genitore oppure all'altro;
- non utilizzare minori in grottesche imitazioni degli adulti;
- non diffondere dalle 7,00 alla 23,00, immagini crude o brutali o scene che possano creare nei minori turbamento o forme imitative e notizie che possano nuocere all'integrità dei minori, se non quando si presentassero esigenze di straordinario valore sociale ed informativo dandone preavviso;
- darsi strumenti propri di valutazione circa l'ammissione in tv di film, telefilm, spettacoli di intrattenimento vari a tutela del benessere morale, psichico e fisico dei minori;
- annunciare con congruo anticipo la programmazione di film e di altri spettacoli destinati agli adulti adottando idonei sistemi di segnalazione;
- evitare trasmissioni che usino i conflitti familiari come spettacolo, il ricorso gratuito al turpiloquio, le espressioni scurrili e le offese alle confessioni religiose.

Le imprese televisive si sono impegnate inoltre a controllare i contenuti delle comunicazione commerciali, dei trailer e dei promo e a non trasmettere pubblicità che possa ledere i minori. Le pubblicità in particolare, non devono presentare minori impegnati in atteggiamenti di violenza, dediti al consumo di alcool, tabacco e stupefacenti né rappresentare in forma negativa chi si astiene dal consumo di tali sostanze; non devono esortare i minori all'acquisto di tali prodotti.
Tra le ore 16,00 e le ore 19,00 è individuata "una fascia protetta" idonea ai minori con un particolare controllo sui programmi, trailer e pubblicità. In particolare, negli spot pubblicitari adiacenti ai cartoni animati non devono essere rappresentati i personaggi degli stessi.
Comunque, come previsto dalla normativa vigente, tutte le tv stanno adottando strumenti (simili al parental control) che ti consentiranno di filtrare i programmi non adatti ai tuoi figli.

ATTENZIONE
SE SEI UN RAGAZZO/A:

Poni attenzione alle informazioni che vengono fornite all'inizio e durante i programmi (in particolare film, telefilm, tv movies, fiction e spettacoli di intrattenimento).
Bollini colorati, scritte in sovrimpressione o altre forme di segnalazione, ti faranno capire se il programma è adatto ai bambini (verde), se la sua visione è consigliata in presenza di un adulto (giallo) o se è del tutto sconsigliata ai minori (rosso).

PUOI RIVOLGERTI ALLA POLIZIA POSTALE PER:

PEDOPORNOGRAFIA

•

CYBER TERRORISMO

•

COPYRIGHT

•

HACKING

•

PROTEZIONE DELLE INFRASTRUTTURE
CRITICHE DEL PAESE

•

E-BANKING

•

ANALISI CRIMINOLOGICA
DEI FENOMENI EMERGENTI

•

GIOCHI E SCOMMESSE ON-LINE

PUOI RIVOLGERTI AL CORECOM PER:

CONTROVERSIE CON I TUOI GESTORI DI:
TELEFONIA FISSA
MOBILE
TRAFFICO INTERNET
PAY TV

http://corecom.consiglio.puglia.it/
conciliazionicorecom@consiglio.puglia.it
PEC: corecompuglia@pec.it
080/5402527 - fax: 080/5951882

SEGNALARE LA MESSA IN ONDA SULLE TV
LOCALI DI SCENE E/O PUBBLICITÀ CONTRARIE
ALLE NORME CHE TUTELANO L'UTENZA
E IN PARTICOLARE I MINORI

http://corecom.consiglio.puglia.it/
PEC: corecompuglia@pec.it
corecom@consiglio.puglia.it
080/5402527 - fax: 080/5951883

GLOSSARIO

ADWARE: Particolare versione di spyware atto a monitorare informazioni personali o sensibili a fini pubblicitari.
ANTISPAM: Programma o tecnologia che impedisce, o quantomeno limita, la ricezione di posta indesiderata nella propria casella di posta in antrata.
ANTISPYWARE: Il software antispyware protegge il computer da popup pubblicitari, lentezza e minacce alla sicurezza dovute a spyware e altro software indesiderato.
ANTIVIRUS: Programma che individua, previene e rimuove programmi dannosi, come virus e worm. Affinchè sia efficace deve essere costantemente aggiornato.
ATTIVAZIONE: Procedura indispensabile, connessa all'installazione di molti software per attestarne la genuinità.
BACKDOOR: Accesso abusivo a un sistema informatico. Di solito una backdoor viene inserita dagli stessi programmatori del sistema per poter effettuari accessi di emergenza, ma a volte gli hacker riescono a individuarle sfruttandole a proprio vantaggio.
BACKUP: Operazione che consiste nel salvare periodicamente i dati memorizzati sul disco fisso del PC. È indispensabile fare backup frequenti perché un virus, un guasto dell'hardware, un incendio o anche un'operazione sbagliata possono causare la perdita dei dati.
BOT: Il termine bot è un'abbreviazione di "robot". I pirati informatici li usano per trasformare il tuo computer in un dispositivo in grado di effettuare automaticamente operazioni su Internet a tua insaputa.
CHAT: Significa "chiacchierare" e indica le conversazioni scritte in tempo reale che si possono fare in rete con altri utenti tramite appositi programmi, per esempio Messenger e Skype. Nelle versioni più evolute le Chat prevedono la possibilità di parlare sfruttando microfono e casse del PC o addirittura di effettuare videoconversazioni.
CLOUD: Il termine inglese cloud computing indica un insieme di tecnologie che permettono di memorizzare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in Rete. SkyDrive e le Office Web Apps sono un esempio di servizio cloud offerto gratuitamente da Microsoft.
CONTROLLO ACTIVEX: I controlli ActiveX sono piccoli programmi che vengono utilizzati su Internet. Nella maggior parte dei casi sono utili, per esempio per l'installazione di aggiornamenti di sicurezza, ma se usati illegalmente possono effettuare attività senza il tuo controllo.
COOKIE: I Cookie sono piccoli file che i siti web salvano sul tuo disco rigido alla tua prima visita. Il loro compito è quello di ricordare i tuoi dati quando ritorni a visitare un sito. Generalmente i cookie non sono dannosi, ma se usati in maniera fraudolenta possono sottrarre informazioni a tua insaputa.
COPYRIGHT: È il diritto d'autore che stabilisce la proprietà intellettuale di un'opera.
CRACCARE: Neologismo gergale da "to crack", "spezzare". Si intende il superamento delle protezioni di un programma o di un sistema informatico.
CRACK: Un sistema, generalmente software, in grado di eliminare le protezioni che vengono normalmente applicate ai programmi per evitare che vengano duplicati e installati illecitamente. L'utilizzo dei crack è illegale.
CRACKER: Declinazione negativa dell'hacker. Quest'ultimo generalmente viola i sistemi informatici solo per metterli alla prova, mentre il Cracker lo fa con l'obiettivo di sottrarre i dati, danneggiare i sistemi o sottrarre denaro, per esempio da un conto corrente online.
CYBERBULLISMO: Termine che identifica attività di bullismo perpetrate tramite internet. Segnala l'episodio di bullismo al sito Web in cui è avvenuto. Molti servizi si avvalgono di moderatori e di luoghi in cui segnalare gli abusi, ad esempio abuse@microsoft.com
CYBERPEDOFILIA: Il pedofilo telematico è un individuo estremamente pericoloso perché spesso è difficile da individuare. Tipicamente cerca di instaurare un clima di fiducia e di amicizia fingendosi coetaneo dei bambini e cercando di agire quando il minore non è controllato da persone adulte.
DIALER: è uno speciale programma auto-eseguibile che altera i parametri della connessione a internet impostati sul computer dell'utente, agendo sul numero telefonico del collegamento e sostituendolo con un numero a pagamento maggiorato su prefissi internazionali satellitari o speciali.
DISCLAIMER: Significa "Esonero di responsabilità". L'insieme dei diritti e doveri dell'utente e limitazioni di responsabilità del produttore, relative a un software, da accettare al momento dell'installazione.
DRM: Acronimo di Digital Right Management, standard ideato da Microsoft sulla gestione dei diritti relativo alle opere digitali protette da copyright.
FAKE: Identifica un falso. Su Internet usato spesso per identificare l'utilizzo di un'identità falsa o altrui, un file fasullo o un allarme relativo a un virus inesistente.
FILE SHARING: Scambio di file solitamente attraverso reti paritarie (p2p), ma anche attraverso apposite piattaforme. Può essere illegale.
FILTRO SMART SCREEN: Il filtro SmartScreen è una funzionalità di Internet Explorer 9 e 8 che ti aiuta a evitare le minacce di ingegneria sociale, sotto forma di malware e phishing, e le truffe online quando navighi sul web.
FIREWALL: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker, virus e worm che cercano di raggiungere il computer attraverso Internet.
FIRMA DIGITALE: Procedura che garantisce l'integrità e l'autenticità di un documento informatico, in analogia con la firma autografata.
FLAME: Il termine significa "fiammata" ed è tipico dei newsgroup. Identifica un attacco o reazione aggressiva verbale nei confronti di un utente.
FURTO DI IDENTITÀ: Il furto di identità è un qualsiasi tipo di frode che porta alla perdita di dati personali, come password, nomi utente, dati bancari o numeri di carte di credito. La forma più diffusa è il phishing, ovvero la frode perpetrata tramite mail.
HACKER: Nella sua forma più pura si può considerare

una sorta di studioso dei sistemi informatici, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. Purtorppo sempre più spesso gli hacker diventano cracker, ovvero persone che lo fanno a scopo di lucro, per sottrarre dati o per mettere fuori uso i sistemi informatici.

HOAX (FINTE MAIL): Un fenomeno legato al Phishing e al furto dì identità. Si tratta di finte mail, per esempio provenienti da istituti bancari o altri organismi, il cui unico scopo è sottrarre informazioni personali.

HTTPS: L'utilizzo del protocollo HTTPS (Hypertext Transfer Protocol Secure) consente di proteggere le informazioni inviate in Internet. In Hotmail viene per esempio utilizzato il protocollo HTTPS per la crittografia delle informazioni di accesso.

ICRA: Internet Contant Rating Association. Un'associazione internazionale senza fini di lucro nata per difendere e aiutare la navigazione dei minori in Rete.

INPRIVATE BROWSING: Tecnologia che consente di evitare che la cronologia delle esplorazioni, i file internet temporanei, i dati dei moduli, i cookie nonché i nomi utente e le password vengano mantenuti nel browser. In questo modo non lascerai traccia della tua navigazione.

LOGIN: Procedura di accesso a un computer, a un programma o a un servizio, generalmente legata all'inserimento di un user name e di una password.
È fondamentale scegliere password sicure per evitare che altri possano accedere senza il nostro consenso.

LURKER: Chi sta in agguato. Nelle attività in rete indica chi osserva senza prendere parte attiva.

MALWARE: Malware è l'abbreviazione di "malicious software", ovvero software dannoso. Con questo termine si identifica un software che viene installato senza il tuo consenso, per esempio mentre scarichi un programma gratutito o un file da una rete peer to peer.

MICROSOFT SECURITY ESSENTIALS: Microsoft Security Essentials è un software antimalware gratuito per il tuo computer. Ti protegge da virus, spyware e altro malware. È scaricabile gratuitamente per Windows 7, Windows Vista e Windows XP SP2 e superiori.

NETIQUETTE: Contrazione di Net Etiquette, ovvero "etichetta di rete". Insieme di regole che disciplinano il comportamento di un utente in internet. Il rispetto della netiquette non è imposto da alcuna legge, ma è prassi comune attenervisi.

NETIZEN: Il termine significa "cittadino della Rete". Neologismo abbastanza usato derivato da network e citizen.

NEWBIE: Neologismo gergale che indica un nuovo utente della rete, un navigatore alle prime armi.

NICKNAME: Quando non si vuole usare il proprio nome in rete, si può scegliersi un soprannome, detto appunto nickname. Non è possibile sapere chi si nasconde dietro a un nickname, per questo occorre fare molta attenzione quando si naviga in rete e ci si raffronta con altri utenti.

PEER-TO-PEER: Architettura di rete nella quale tutti i computer funzionano sia come client sia come server. Tutti i computer sono quindi uguali e di pari livello. Un esempio di rete peer to-peer è Emule. Spesso questo tipo di reti vengono utilizzate per scambiare file illegalmente.

PHARMING: Tecnica che permette di sfruttare a proprio vantaggio le vulnerabilità di server controllando il dominio di un sito e utilizzandolo per redirigere il traffico su un altro sito.

PARENTAL CONTROL: Un filtro che permette di bloccare la visione dei contenuti non adatti ai bambini o a persone particolarmente sensibili.

PHISHING: Il phishing è un furto di identità online. Si basa su email, notifiche e siti web fraudolenti progettati per rubare dati personali o informazioni riservate, come dati account, numeri di carte di credito, password o altro.

POP-UP: Il termine significa "saltar su" e indica le finestre che si aprono nel browser in modo automatico, di solito a scopi pubblicitari.

PROXY SERVER: Un server che si interpone tra i computer di chi naviga e il Web. Il suo scopo è sia quello di incrementare le prestazioni di navigazione, verificando se la pagina richiesta è già disponibile in memoria, sia di filtrare la navigazione, per esempio per impedire ai dipendenti di visitare siti vietati o aree particolari.

RIPPER: Letteralmente "squartatore". È così definito un programma che acquisisce i dati da CD musicale o DVD video e li importa sul disco fisso, per un'eventuale conversione e modifica. Questo genere di azioni è quasi sempre illegale.

SPAM: Lo spam è qualsiasi tipo di comunicazione online indesiderata. Attualmente la forma più comune di spam è la posta elettronica, per questo sono nate tecnologie, come il filtro SmartScreen di Microsoft, che riduce drasticamente la posta indesiderata in grado di raggiungere la nostra casella di posta.

SPYWARE: Spyware è un termine che descrive un software che si installa sul computer senza il tuo consenso. Uno spyware può fare pubblicità, raccogliere informazioni personali e addirittura arrivare a modificare la configurazione del tuo computer.

SSL: Acronimo di "Secure Sockets Layer", un protocollo che rende sicure le transazioni commerciali in rete, per esempio con carte di credito, grazie alla trasmissione dei dati cifrata.

TRACKING PROTECTION LIST: La TPL o Protezione da monitoraggio, permette di scegliere i siti autorizzati a ricevere le informazioni che riguardano la navigazione da parte dell'utente e di controllare la propria privacy durante la navigazione.

TROJAN: è un software che nasconde al suo interno un virus. Installando ed eseguendo il programma che contiene il Trojan, l'utente innesca il virus.

VIRUS: I virus informatici sono software progettati per diffondersi da un computer all'altro e interferire con il funzionamento della macchina. Un virus può cancellare dati, carpire informazioni, usare il programma di posta per diffondersi ad altre macchine e addirittura rendere il PC inutilizzabile.

WAREZ: Neologismo usato per individuare software scaricabili abusivamente e illegalmente dalla rete.

WEP: Acronimo di Wired Equivalent Privacy, un sistema di crittografia che si basa su una chiave pubblica. Serve per rendere più sicure le comunicazioni wireless. Fa parte dei protocolli di sicurezza wireless anche l'algoritmo di crittografia AES, sigla di Advance Encryption Standard.

WORM: Un worm è un particolare virus informatico in grado di propagarsi senza la necessità che l'utente inneschi il suo funzionamento compiendo un'operazione, per esempio installando un software.

www.commissariatodips.it

Compartimento Polizia Postale e delle Comunicazioni "Puglia" - Bari
Via Amendola 116 - cap 70100 Bari
Centralino: 080 59220611 • Fax: 080 5507058
E-mail: poltel.ba@poliziadistato.it

Sezione Polizia Postale e delle Comunicazioni - Foggia
Via Isonzo 10 - cap 71100 Foggia
Centralino: 0881 722100 • Fax: 0881 708243
E-mail: poltel.fg@poliziadistato.it

Sezione Polizia Postale e delle Comunicazioni - Taranto
Lungomare Vittorio Emanuele III - cap 74100 Taranto
Centralino: 099 4554265 • Fax: 099 455435
E-mail: poltel.ta@poliziadistato.it

Sezione Polizia Postale e delle Comunicazioni - Lecce
p.le Stazione FF.S - cap 73100 Lecce
Centralino: 0832 244150 • Fax: 0832 249877
E-mail: poltel.le@poliziadistato.it

Sezione Polizia Postale e delle Comunicazioni - Brindisi
Piazza Vittorio Emanuele - cap 72100 Brindisi
Centralino: 0831 523185 • Fax: 0831 523185
E-mail: poltel.br@poliziadistato.it

CO RE COM PUGLIA
Comitato Regionale per le Comunicazioni

www.corecom.consiglio.puglia.it

VIA LEMBO, 40 - 40/F • 70124 • BARI
TEL. 080 5402530 • 080 5402527
FAX 080 5402529 • 080 5951883
corecom.consiglio.puglia.it

*UN PARTICOLARE RTINGRAZIAMENTO A **MINGO** PER LA PREZIOSA COLLABORAZIONE.*

Polizia di Stato

CO RE COM PUGLIA
Comitato Regionale per le Comunicazioni

Consiglio Regionale della Puglia

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

COMUNICAINSICUREZZA

TOUCH PROTECTION

spazioeventi.org

Polizia di Stato

CO RE COM PUGLIA
Comitato Regionale per le Comunicazioni

Consiglio Regionale della Puglia

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

COMUNICAINSICUREZZA

TOUCH PROTECTION

www. poliziadistato.it
www.commissariatodips.it