Polizia di Stato

POLIZIA POSTALE E DELLE COMUNICAZIONI 2016

I consigli della Specialità
Poche semplici regole da seguire

L'uso dei social network è vietato ai minori di 13 anni ed è sconsigliato ai minori di 14: la loro inesperienza, la loro tendenza a sottostimare i rischi della diffusione di immagini e informazioni riservate, la loro curiosità verso gli altri e verso le nuove tecnologie potrebbero esporre i ragazzi e le loro famiglie a vari rischi reali (es. adescamento, violazione della privacy propria e altrui, commissione inconsapevole di reati, etc.).
Ricorda che un'immagine condivisa in un social network entra definitivamente nel web e che non sarà possibile controllarne mai più la diffusione, anche qualora fosse utilizzata in siti che non conosci, che non ti piacciono e/o che non condividi.
Ricorda che molte delle informazioni che posti nella bacheca del tuo profilo consentono di ricostruire la tua identità, le tue abitudini, i tuoi gusti e molto più di quel che immagini: sei sicuro di volere che molte persone, magari anche i tuoi genitori e/o i tuoi insegnanti e/o i tuoi futuri datori di lavoro sappiano quello che racconti?
Creare profili con nomi equivoci e/o postare messaggi allusivi di una disponibilità sentimentale e/o erotica ti espone al rischio di richiamare l'attenzione di malintenzionati della rete.
Evita di proporti in un ruolo non adatto alla tua età o ai tuoi reali desideri se non sei pienamente consapevole, per età ed esperienza, delle conseguenze che tali dichiarazioni di disponibilità possono comportare (es. contatti da sconosciuti, argomenti imbarazzanti, offerte e richieste oscene).
Ricorda che a disciplinare il comportamento in Rete c'è non solo una netiquette da rispettare ma anche leggi che definiscono chiaramente cosa costituisce reato e cosa no: comportati sempre correttamente nei confronti degli altri utenti dei social network, evita di creare gruppi che inneggiano a comportamenti indesiderabili e che ledono l'immagine e/o la credibilità di persone note e meno note. Ricorda di tenere segreta la password di accesso al tuo profilo sul social network: compagni di classe e conoscenti potrebbero utilizzarla per sostituirti e commettere azioni scorrette a tuo nome, per diffondere informazioni riservate che ti riguardano, anche al solo scopo di fare uno scherzo. Non cercare di ottenere la password di accesso al profilo o alla casella di email di altri utenti poiché questo, seppur animato dalle più innocenti intenzioni, costituisce reato ed espone te al rischio di accuse molto serie. Imposta il tuo profilo in modo da consentirne la visibilità solo agli amici che avrai autorizzato tu previa richiesta: in questo modo selezionerai direttamente chi accede alla tua pagina e ti garantirai di essere contattato solo da persone conosciute e affidabili.

Come equipaggiare il computer e usarlo in sicurezza

- **GARANTISCITI UNA PREPARAZIONE** informatica quantomeno analoga a quella dei vostri figli per rispondere alle loro domande e predisporre le opportune misure di protezione del computer.
- **FAI REGOLARI BACKUP** dei dati più importanti.
- **TIENI AGGIORNATO UN BUON ANTIVIRUS** e un firewall che proteggano continuamente il vostro pc e chi lo utilizza. Vi metterete al sicuro dal rischio di malware e virus indesiderati e dai rischi per la vostra sicurezza personale che essi comportano. Aggiornate e scaricate le nuove versioni dei programmi per rendere permanente la protezione del computer.
- **USA UN FIREWALL** come "gatekeeper" tra il vostro computer e Internet; i firewall sono essenziali per chi ha una connessione ADSL o via cavo ma sono preziosi anche per chi utilizza la connessione telefonica.
- **IMPOSTA LA "CRONOLOGIA"** di navigazione in modo che mantenga traccia per qualche giorno dei siti visitati da vostro figlio.

I consigli della Specialità
Poche semplici regole da seguire

- **CONTROLLA PERIODICAMENTE IL CONTENUTO DELL'HARD DISK** del computer.
- **USA SOFTWARE "FILTRI"** con un elenco predefinito di siti da evitare. Verificate periodicamente che funzionino in modo corretto e tenete segreta la parola chiave.
- **LEGGI LE E-MAIL CON I BAMBINI PIÙ PICCOLI** controllando ogni allegato al messaggio. 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 computer. Date le stesse indicazioni ai ragazzi più grandi.
- **NON TENETE IL COMPUTER ALLACCIATO** alla Rete quando non lo usate: è consigliato piuttosto disconnettere il computer.
- **NON APRIRE GLI ALLEGATI** delle e-mail provenienti da sconosciuti e verificate prima il nome dei mittenti e l'oggetto.
- **SIATE SOSPETTOSI** anche di allegati inaspettati ricevuti da chi conoscete perché possono essere spediti da una macchina infettata senza che l'utilizzatore ne sia a conoscenza.
- **SCARICA REGOLARMENTE LE "SECURITY PATCHES"** (modifiche per incrementare la sicurezza dei software) dal vostro fornitore di software.

Nove regole da tenere a mente

- **TIENI IL TUO PC BEN PROTETTO**
  Usa gli aggiornamenti automatici per avere sempre l'ultima versione del software, soprattutto quello per Internet. Usa firewall, antivirus e antispam.
- **CUSTODISCI LE INFORMAZIONI PERSONALI**
  Prima di inserire i tuoi dati personali su Internet controlla che siano presenti i segni che indicano la sicurezza della pagina: la scritta https nell'indirizzo e il segno del lucchetto.
- **UTILIZZA PASSWORD SICURE E TIENILE RISERVATE**
  Devono essere lunghe (almeno otto caratteri), contenere maiuscole e minuscole, numeri e simboli. Non usare la stessa password per siti diversi.
- **PRIMA DI FARE CLIC, USA LA TESTA**
  Quando ricevi un allegato sospetto, controlla bene prima di selezionarlo: potrebbe essere un trucco. Se conosci la persona che lo invia chiedi conferma che te lo abbia mandato veramente; se non la conosci, ignoralo.
- **NON DARE INFORMAZIONI VIA E-MAIL**
  Non dare mai informazioni personali in risposta a un messaggio e-mail o di Messenger (cognome, indirizzo, numero di telefono, foto, età e così via).
- **ATTENZIONE AI FALSI**
  Messaggi allarmistici, richieste disperate d'aiuto, segnalazioni di virus, offerte imperdibili, richieste di dati personali "per aggiornare il tuo account": diffida di tutti i messaggi di questo tono e attiva un sistema per individuarli, come il filtro SmartScreen® di Windows® Internet Explorer®.
- **SUI SOCIAL NETWORK CON ALLEGRIA E PRUDENZA**
  Su Facebook, Twitter, Windows Live™ e su tutti gli altri social network controlla bene le impostazioni. Chi può vedere il tuo profilo? Chi può fare ricerche su di te? Chi può fare commenti? Chi può esporti in situazioni che non controlli?
- **PENSA A QUELLO CHE PUBBLICHI SU INTERNET**
  Le tue foto, i tuoi messaggi e le tue conversazioni possono essere viste anche da sconosciuti. Non postare nulla che consideri personale o riservato e di cui potresti pentirti in futuro.

I consigli della Specialità
Poche semplici regole da seguire

- **RISPETTA LA NETIQUETTE**
  La netiquette è un insieme di regole di buon comportamento da seguire sui social network, nei forum, nelle community: prima di seguire il tuo istinto, leggi il regolamento del sito in cui ti trovi; non insultare o mettere in cattiva luce nessuno; non pubblicare messaggi privati di altre persone.

Alcuni utili consigli per i genitori

- **SCEGLI PER I TUOI FIGLI** un computer portatile e, se possibile, utilizzatelo per la sola navigazione in internet: posizionatelo in una stanza centrale della casa, piuttosto che nella camera dei ragazzi. Vi consentirà di dare anche solo una fugace occhiata ai siti visitati senza che vostro figlio si senta "sotto controllo".
- **NON LASCIARE** troppe ore i bambini e i ragazzi da 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.
- **PER LA NAVIGAZIONE** dei più piccoli usate software "filtro" con un elenco predefinito di siti possibili, scegliete la lista di questi siti insieme ai vostri figli spiegandogli che è una misura di sicurezza indispensabile. 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 dati personali come nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici. Ricordategli inoltre che non è consigliabile pubblicare in internet foto di sé o degli altri, soprattutto se questi sono minorenni e inconsapevoli di apparire on-line.

Per i bambini e i ragazzi

- **NELLE CHAT, NEI FORUM,** nei blog e nei giochi di ruolo non dare mai il tuo nome, cognome, indirizzo, numero di cellulare o di casa. Lo schermo del computer nasconde le vere intenzioni di chi chatta con te.
- **NON SCARICARE PROGRAMMI** se non ne conosci bene la provenienza: potrebbero contenere virus che danneggiano il computer, spyware che violano la privacy e rendono accessibili informazioni riservate.
- **NON INCONTRARE MAI** persone conosciute su Internet senza avvertire i tuoi genitori. Se proprio vuoi incontrare qualcuno conosciuto su Internet, prendi appuntamento in luoghi affollati e porta con te almeno due amici.
- **RICORDA** che le tue immagini e quelle degli altri sono una cosa privata, da proteggere: non mettere foto o filmati fatti con il telefonino in community, chat o socialnetwork che siano aperti a tutti, grandi e piccini. Una volta immessi in rete, foto e filmati, possono continuare a girare anche se tu non vuoi.
- **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!

I consigli della Specialità
Poche semplici regole da seguire

L'uso sicuro del telefonino per i genitori

- Spiega a tuo figlio che il telefonino è un mezzo di comunicazione che impone una cautela analoga a quella che si ha nei confronti del computer. Scegli per i più piccoli modelli semplici, quelli con telecamere e fotocamere riservali a quando sapranno utilizzarli in modo sicuro e consapevole.
- Spiega a tuo figlio che foto e riprese effettuate con il telefonino sottostanno alla normativa italiana in materia di protezione dell'immagine e della privacy delle persone.
- Per i telefonini che consentono la navigazione in Internet o l'accesso a community e chat, spiega a tuo figlio che i rischi in termini di adescamento da parte di pedofili on line sono i medesimi della Rete "tradizionale".
- Scegli per i tuoi figli SIM Card ricaricabili e ricarica sempre tu il credito in modo da poter monitorare la quantità di traffico telefonico effettuato.
- Al momento dell'attivazione della SIM Card fornisci ai tuoi figli il PIN ma non il PUK. Con il PUK infatti potrai accedere al telefono anche se il PIN è stato modificato.
- Spiega ai tuoi figli che sms o mms che promettono ricariche facili o altri vantaggi immotivati sono spesso il primo contatto effettuato da chi non ha buone intenzioni.
- Parla ai tuoi figli della potenziale pericolosità di richiamare col 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.
- Scoraggia tuo figlio dal diffondere foto o filmati fatti con il telefonino in community o chat telefoniche. Una volta immesse in Rete foto e filmati possono continuare a essere diffuse senza controllo per lungo tempo.

Polizia Postale e delle Comunicazioni

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 entrata.

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. Affinché 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 effettuare 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 video conversazioni.

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 on line.

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.

Glossario

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 on line quando navighi sul web.

FIREWALL: Un firewall è un programma software o un componente hardware che permette di respingere gli attacchi di hacker, virus o 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 phising, 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. Purtroppo sempre più spesso gli hacker diventano cracher, 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 di 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 (Hyper text 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 username 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 "maliciuous software", ovvero software dannoso. Con questo termine si identifica un software che viene installato senza il tuo consenso, per esempio mentre scarichi un programma gratuito 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, Window Vista e Windox 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.

Glossario

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 scegliere 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 ridirigere il traffico su 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 on line. Si basa su e-mail, 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 a 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 on line 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'algorismo 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.