Per qualsiasi dubbio, informazione o consiglio in rete contatta la:

Sezione Polizia Postale Cuneo
Via Cavour nr. 3
Tel.: 0171460351
Mail: sez.polposta.cn@pecps.poliziadistato.it

…qualche consiglio…

……..PER I RAGAZZI:

- **NELLE CHAT E NEI FORUM**

  Nelle chat, nei forum, nei blog e nei giochi di ruolo non dare mai il tuo nome, cognome, indirizzo e numero di cellulare o di casa. Lo schermo del PC nasconde le vere intenzioni di chi chatta con te.

- **NON SCARICARE PROGRAMMI**

  Non scaricare programmi se non conosci bene la provenienza: potrebbero contenere virus che danneggiano il PC, spyware che violano la privacy e rendono accessibili informazioni private.

- **NON INCONTRARE MAI CHI NON CONOSCI REALMENTE**

  Non incontrare mai persone conosciute in internet. Se proprio vuoi incontrare chi hai conosciuto su internet prendi appuntamento in luoghi affollati e porta con te almeno due amici.

- **OCCHIO A COSA PUBBLICHI**

  Ricorda che le tue immagini e quelle degli altri sono private, da proteggere. Una volta immessi in rete, foto e filmati possono continuare a girare in rete anche se tu non sei d'accordo.

- **NON TI FIDARE**

  La promessa di ricariche telefoniche facili, di regali che ti arrivano via sms, nelle chat da persone sconosciute devono metterti in allerta.

- **PRIMA DI ATTIVARE LA WEB CAM PENSACI!**

  Attiva la web cam solo con chi conosci e non farti riprendere in atteggiamenti tali di cui potresti pentirti in quanto potresti essere registrata da ignoti truffatori con successive richieste di denaro per non far visualizzare il filmato in rete.

- **NON OFFENDERE**

  Non offendere nessuno in rete. I tuoi commenti oltre a essere visibili da tutti possono ravvisare un reato previsto dal codice penale (diffamazione). Anche se li cancelli poco dopo averli postati in rete ormai l'offesa è stata visualizzata da più utenti.

- **CREARE PER SCHERZO UN PROFILO FALSO**

  Creare per scherzo un profilo falso, su Facebook o su altro social network a nome di un tuo amico o di un tuo conoscente, può ravvisare un reato previsto dal codice penale (sostituzione di persona).

.....CONSIGLI PER I GENITORI:

- **SIATE VIGILI**

  Scegliete per i vostri figli un PC portatile e, se possibile, utilizzatelo per la sola navigazione in internet: posizionatelo in una stanza centrale della casa, piuttosto che nella camera da letto dei ragazzi. Vi consentirà di dare anche solo una fugace occhiata ai siti visitati senza che vostro figlio si senta "sotto controllo" e vi permetterà inoltre che vostro figlio non navighi in orari notturni.

- **STABILITE DEGLI ORARI PER LA NAVIGAZIONE**

  Non lasciate troppe ore i bambini e i ragazzi da soli in Rete. Stabilite quanto tempo possono passare in Rete: limitare il tempo che possono trascorrere on line significa limitare di fatto l'esposizione ai rischi della Rete.

- **PER LA NAVIGAZIONE DI PIÙ PICCOLI**

  Utilizzate software "filtro" con un elenco di siti possibili, scegliete la lista di questi siti insieme ai vostri figli bloccando la navigazione in determinati orari: spiegate loro che è una misura di sicurezza indispensabile.

- **INSEGNATE AI VOSTRI FIGLI A TUTELARE LA LORO PRIVACY ANCHE IN RETE**

  Insegnate ai vostri figli l'importanza di in rivelare in Rete dati personali come nome, cognome, età, indirizzo, numero di telefono e orari della scuola. Ricordate loro inoltre che non è consigliabile pubblicare foto di sé o degli altri.

…….ALTRE REGOLE DA TENERE IN MENTE

- **TIENI IL TUO PC BEN PROTETTO**

  Utilizza gli aggiornamenti automatici per avere sempre l'ultima versione dei software, soprattutto quello per Internet. Usa firewall, antivirus, antispyware e antispam.

- **UTILIZZA PASSWORD SICURE E TIENILE RISERVATE**

  Le password devono essere lunghe (almeno otto caratteri) complesse (alternando maiuscole, minuscole, numeri e simboli). Non usate la stessa password per le diverse piattaforme che utilizzate.

- **ATTENZIONE AI FALSI**

  Messaggi allarmistici, richieste disperate di aiuto, segnalazioni di virus, offerte imperdibili, richieste di denaro per sbloccare il vostro computer, 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 Smart Screen di "Windows Internet Explorer"
  Sui social network con allegria e prudenza
  Su Facebook, Twitter e altri profili, controlla bene le impostazioni. Chi può vedere il tuo profilo? Chi può fare richieste su di te? Chi può "taggare" le tue foto?"

- **LE CATENE DI SANT'ANTONIO**

  Non diamo seguito alle catene di Sant'Antonio sui vari Social come quella che circolava qualche giorno fa su FAcebook con il seguente testo:" *sfida delle mamme. Sono stata nominata da….per postare tre foto che mi rendano felice di essere mamma. Scelgo alcune donne che ritengo siano grandi madri. Se sei una madre che ho scelto copia questo testo inserisci le tue foto e scegli le grandi madri*". Postando le immagini proprie e dei propri figli può essere molto rischioso in quanto sia le immagini che i dati personali postati potrebbero essere utilizzati da soggetti per azioni illecite e fraudolente.

- **NAVIGA CON ATTENZIONE**

  Non scaricare programmi se non conosci bene la provenienza: potrebbero contenere virus che danneggiano il PC, spyware che violano la privacy e rendono accessibili informazioni private. Controlla la sicurezza dei siti che visiti e leggi le recensioni postate dai vari utenti (la critta https nell'indirizzo e il simbolo del lucchetto chiuso)