- ✓ Non aprire gli allegati delle e-mail provenienti da mittenti sconosciuti.
- ✓ Non comunicare mai dati personali di accesso a siti web o alla posta elettronica.
- ✓ Scaricare file solo da siti sicuri e affidabili.
- ✓ Stare alla larga da siti che trattano di pirateria informatica e pornografia.

Qualche informazione in più

Cos' è il cyberbullismo?

Il termine italiano "bullismo" è la traduzione dell'inglese "bullying", che definisce il fenomeno delle prepotenze fatte all'interno di un gruppo contro qualcuno che non sa o non può difendersi.

La parola "cyberbullismo" indica invece in modo specifico un comportamento offensivo, minaccioso, insultante, da parte di qualcuno che aggredisce senza motivo altri utenti della Rete attraverso chat, forum, e-mail ecc...

Il cyberbullo spesso si sente sicuro perché protetto dell'anonimato, consentito dalla Rete.

Come difendersi dal cyberbullismo.

- ✓ Mantieni un comportamento riservato (evita di far vedere inutilmente tue foto, o di fornire dati personali).
- ✓ Imposta nickname generici, in cui non ci sia riferimento alla tua età, al sesso, al luogo dove abiti.
- ✓ Non confidare in chat o forum dettagli della tua vita privata.
- ✓ Non assumere a tua volta atteggiamenti aggressivi, irritanti, o che possano provocare risentimento.
- ✓ Evita di rispondere a messaggi offensivi nei confronti tuoi o dei tuoi amici.

- ✓ Registra i messaggi che ti offendono o ti turbano, potrebbero servirti per eventuali denunce.
- ✓ Parla di questi messaggi ai tuoi genitori o a un tuo insegnante.
- ✓ Isola il bullo, ma non rimanere solo di fronte al cyberbullo!

Se hai bisogno di aiuto, o anche solo se credi di aver bisogno di aiuto

chiama **i numeri 114 o 113** o vai all'indirizzo www.commissariatodips.it, che è gestita dalla Polizia Postale e delle Comunicazioni.

Oppure contatta Microsoft all'indirizzo **abuse@microsoft.com** se il problema riguarda l'utilizzo inappropriato di un servizio Microsoft.

Link utili:

www.poliziadistato.it

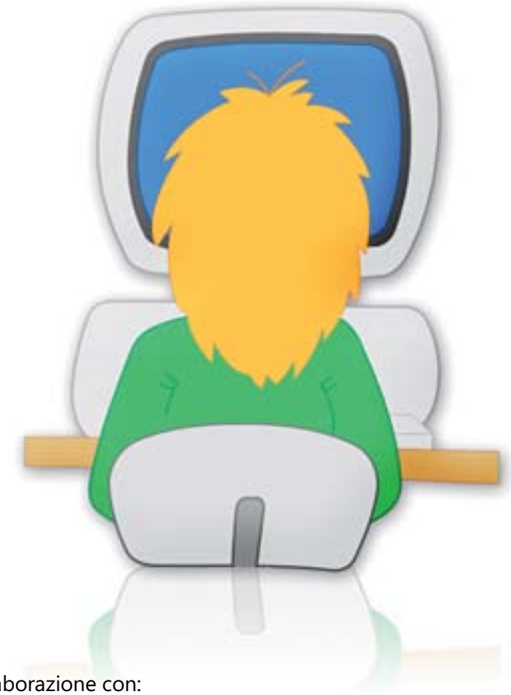
www.commissariatodips.it

www.unicef.it

www.microsoft.com/italy/athome/security

Comune di Roma
Presidenza
Consiglio Comunale

La scuola ricomincia navigando



In collaborazione con:

Con il patrocinio di:

Ministero delle Comunicazioni

Consigli per una navigazione sicura su Internet

Su Internet si gioca, ma non solo.
La Rete è anche un posto da esplorare per **imparare**, **divertirsi** e **comunicare**.
Puoi creare reti di contatti, inviando e-mail e messaggi immediati, pubblicando blog, creando pagine Web personali, cercando musica. Ricorda però che Internet è come il mondo reale, ci sono le cose belle e le cose brutte. Basta seguire queste **regole** e fare un po' di attenzione per divertirsi e per imparare tante cose interessanti senza rischiare brutte sorprese.

Non incontrare MAI persone conosciute su Internet senza **avvertire i tuoi genitori** o comunque prendi appuntamento in luoghi affollati e porta con te almeno due amici.

Se in chat room o via e-mail qualcuno ti dice qualcosa di strano o preoccupante (per esempio discorsi sul sesso) oppure ti invia immagini imbarazzanti, **parlane** appena possibile **con i tuoi genitori** o, se sono impegnati, con i **tuoi insegnanti**.

Non rispondere alle provocazioni, non inviare tue foto, non condividere le password e non raccontare **mai informazioni personali** (dove abiti, dove vai a scuola) a persone appena conosciute nel Web.

Non scaricare loghi, suonerie, immagini da Internet perché possono comportare costi o **addebiti indesiderati**.

Non aprire file allegati a messaggi di posta elettronica di cui non conosci bene il mittente, perché potrebbero contenere virus in grado di danneggiare il tuo computer e in alcuni casi rubarti informazioni personali. In questo caso è meglio **eliminare** le e-mail immediatamente.

Leggi sempre con attenzione tutte le **indicazioni di navigazione** del sito che desideri esplorare.

Ricorda che se qualcuno ti fa un'offerta che sembra troppo bella per essere vera, probabilmente non lo è.

Alcuni comportamenti in Rete possono essere illegali, come per esempio scaricare musica o film d'autore, o installare software privi di licenza, per i quali esistono i diritti di **copyright**.

La netiquette

La parola "netiquette" viene dall'unione tra l'inglese "net" (Rete) e il francese "étiquette" (buona educazione), ed è una raccolta di regole che disciplinano il comportamento di chi usa Internet per comunicare con gli altri attraverso risorse quali newsgroup, mailing list, forum o e-mail in genere.
Ecco le regole più importanti:

1. Sii chiaro, non dare niente per scontato.
2. Esprimiti in modo corretto, usando il linguaggio più adeguato in base alla situazione in cui ti trovi.
3. Cerca di essere educato, rispettando gli altri utenti della Rete e soprattutto rispettando le leggi.
4. Rifletti bene su quello che vuoi o non vuoi comunicare.
5. Ricorda che quando sei su Internet la tua presenza non passa inosservata.
6. Se usi frasi o pensieri di altre persone, che siano protetti dal copyright, non farlo come se fossero opera tua ma cita il loro autore.
7. Usa in modo appropriato le mailing list e chiedi l'autorizzazione prima di inoltrare ad altri destinatari una e-mail che hai ricevuto.
8. Non spedire SPAM.
9. Non dare seguito alle catene di S. Antonio.
10. Non rispondere agli attacchi in modo maleducato o violento, ma ignorali.

Il tuo computer è protetto?

Cosa sono virus e malware

Un virus è una parte di codice del computer che può essere contenuto in un programma oppure in un file. Può danneggiare l'hardware, il software e le informazioni presenti sul computer. Lo scopo di un virus è quello di riprodursi e diffondersi attraverso la condivisione di file o l'invio di messaggi di posta elettronica.
Malware è un termine che viene dalle parole "malicious" e "software" (letteralmente "software malizioso") e indica software creati da malintenzionati che vogliono impadronirsi dei nostri dati personali, dal semplice indirizzo e-mail, alle password di accesso ai servizi on-line della nostra banca. Di solito il malware non blocca il PC, ma ne ruba appunto dati preziosi.
I motivi per cui vengono creati virus e malware possono essere:

1. danneggiare gli utenti di computer;
2. deteriorare il funzionamento di un programma;
3. bloccare l'attività di una banca o di un'azienda;
4. intasare caselle di posta elettronica con una mole enorme di messaggi per impedire il regolare funzionamento del server.

Quali i sintomi

- ✓ Il tuo PC rallenta?
- ✓ Alcuni programmi smettono di funzionare?
- ✓ Si moltiplicano messaggi d'errore?
- ✓ Si aprono automaticamente siti non richiesti?
- ✓ Ricevi posta indesiderata, o qualcuno ti avverte di aver ricevuto e-mail da te, ma tu non le hai inviate?
- ✓ Si creano flussi di dati in uscita dal computer, anche riservati?

Come proteggersi

- ✓ Aggiornare periodicamente il sistema operativo
- ✓ Attivare un firewall: letteralmente "muro di fuoco", è una difesa che consente solo ai programmi legittimi di accedere al Web e di lavorare sul PC.
- ✓ Aggiornare con regolarità l'antivirus scelto attraverso Internet o apposito CD-rom e far sempre partire l'antivirus all'accensione del sistema operativo.