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.
- ✓ 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.

Cosa fare in caso di problemi

Se i tuoi fi gli si sentono turbati o spaventati da qualcosa o qualcuno incontrato su Internet, invitali a **parlartene immediatamente**, senza paura di essere sgridati o di perdere la possibilità di utilizzare il computer. Per aiutarli a gestire la situazione, devi sapere che cosa sta succedendo.

Se il bambino è in pericolo immediato, chiama il pronto intervento **ai numeri 113 o 114**.
Se qualcuno molesta, minaccia o infastidisce in modo continuativo i tuoi figli, oppure tenta di indurli a incontrarsi di persona per scopi illegali, segnalalo ai numeri 113 o 114, oppure all'indirizzo **www.commissariatodips.it**, che è gestito dalla Polizia Postale e delle Comunicazioni e offre informazioni di contatto per tutti i reparti appropriati delle forze dell'ordine.

Se il problema riguarda l'utilizzo inappropriato di un servizio Microsoft, scrivi all'indirizzo **abuse@microsoft.com**

Link utili:

www.poliziadistato.it
www.commissariatodips.it
www.unicef.it
www.microsoft.com/italy/athome/security
https://fss.live.com/

L'UNICEF è la principale organizzazione mondiale **per la difesa dei diritti dell'infanzia e dell'adolescenza** e si ispira in tutta la sua azione ai principi della **Convenzione sui diritti dell'infanzia** ratificata dall'Assemblea Generale delle Nazioni Unite.

In questo quadro si motiva la partecipazione dell'UNICEF al progetto didattico "La scuola ricomincia navigando", attraverso il quale si è voluto approfondire un diritto ormai cruciale per i nostri ragazzi: quello di ricevere una informazione corretta e comprensibile e, di conseguenza, **il diritto di muoversi nel mondo di Internet in modo sicuro, liberi da pericoli e da rischi di abusi e manipolazioni**.

La scuola ricomincia navigando

In collaborazione con:

polizia delle comunicazioni · unicef · SICURAMENTE WEB L'impegno di Microsoft per un mondo digitale migliore · Microsoft · Radio 1 · Next Generation

Con il patrocinio di:

Ministero delle Comunicazioni

Internet è un terreno di gioco per i bambini,

perfetto per esplorare, apprendere e divertirsi. Quando diventano più grandi, offre anche la risorsa ideale per creare reti di contatti, inviando e-mail e messaggi immediati, pubblicando blog, creando pagine Web personali, cercando musica e svago.

Molte attività svolte dai ragazzi su Internet contribuiscono a sviluppare forme sane di comunicazione ed espressione personale, ma possono anche essere pericolose per la sicurezza dei tuoi figli.

Proteggere la propria famiglia su Internet significa comprendere i rischi della rete, fornire ai ragazzi chiare indicazioni per un comportamento sicuro on-line, parlare apertamente con loro e utilizzare le tecnologie quando possono essere d'aiuto.

- ✓ La miglior garanzia di tutela per i tuoi figli è quella di non lasciarli soli in un ambiente popolato da adulti: cerca di accompagnarli il più possibile quando navigano in Rete.
- ✓ In generale, insegna ai tuoi figli quali possono essere i rischi di Internet senza terrorizzarli e senza dimenticare che la Rete è come il mondo reale, ci sono cose belle ma anche cose brutte.
- ✓ Colloca i computer, le console di gioco e gli altri dispositivi di gioco connessi a Internet in soggiorno o in un'altra posizione centrale, invece che nella camera dei ragazzi. Assisti i tuoi figli ogni volta che ritieni sia necessario esercitare una funzione di guida e di controllo.
- ✓ Cerca di imparare ad usare Internet (non è difficile) per riuscire a capire i giochi utilizzati dai tuoi figli, i contenuti che scrivono nei loro blog e le chat che visitano. Crea un rapporto di dialogo con loro, cerca di conoscere i loro interessi in Rete (siti visitati, chat, ricerche e scoperte effettuate) e i loro amici on-line.
- ✓ Parla con i tuoi figli dei rischi legati a Internet, inclusi quelli della pedo-pornografia e del bullismo on-line, della possibilità di imbattersi in contenuti inadatti alla loro età e di veder compromessa la loro privacy. Insegna ai tuoi figli a fidarsi del loro istinto e incoraggiali a dirti se qualcosa li ha turbati o spaventati.
- ✓ Stabilisci regole chiare per l'accesso a Internet, definendo i tempi di utilizzo del computer e del collegamento in Rete secondo l'età dei tuoi figli.
- ✓ Leggi le e-mail che i tuoi figli ricevono da sconosciuti. Molti pedofili allegano foto di pornografia infantile alle e-mail, per convincere il bambino che altri bambini compiono atti sessuali; assicurati di controllare tutti gli attachments alle e-mail (file di testo o di immagini allegate).
- ✓ Controlla l'eventuale iscrizione dei tuoi figli alle chat, per capire con chi sono in contatto.
  Aiuta i tuoi figli ad usare il computer in maniera equilibrata. Molti bambini e ragazzi si appassionano troppo al computer, dimenticando di giocare con gli amici reali.
- ✓ Assicurati che i ragazzi non incontrino le persone conosciute on-line senza il tuo consenso, perché non sono sempre così sincere come dicono di essere.
- ✓ Insegna ai tuoi figli a non rivelare nel Web o nelle chat informazioni personali (come il loro nome, l'età, il sesso, il numero di telefono, l'indirizzo di casa, la scuola che frequentano e i luoghi dove preferiscono giocare e incontrarsi con gli amici).
- ✓ Tieni i bambini lontani dalle chatrooms, a meno che non siano controllati.
- ✓ Incoraggia discussioni tra te e i tuoi figli su ciò che trovano divertente on-line.
- ✓ Insegna ai tuoi figli a non rispondere quando ricevono e-mail offensive o provocatorie, messaggi da chat o altre comunicazioni, specie su argomenti sessuali.
- ✓ Cerca di sorvegliare i tuoi figli mentre sono connessi on-line, installando sul computer un software di protezione che - attraverso l'utilizzo di parole chiave - memorizzi gli indirizzi Internet più frequentati dai ragazzi.
- ✓ Per impedire la navigazione incontrollata sulla Rete utilizza per le parole chiave di accesso (password) nomi di fantasia non presenti in dizionari italiani e stranieri; scegli una combinazione di lettere e numeri che creino una parola facilmente memorizzabile; memorizza le password evitando di scriverle; non rivelare le password e comunque cambiale spesso.
- ✓ I servizi di posta elettronica offrono in genere opzioni che permettono di configurarli in modo da evitare la ricezione di messaggi indesiderati e dannosi anche per i minori; gli allegati ai messaggi di posta elettronica possono contenere dei programmi eseguibili pericolosi per il sistema informatico, è quindi necessario avere cautela se provengono da persone non conosciute.

Sul sito del Commissariato di P.S. on-line è disponibile il test di navigazione sicura riservato ai genitori.
http://www.commissariatodips.it/

Il computer di tuo figlio è protetto?

Cosa sono virus e malware

1. **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.

2. **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:

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