IL PROGETTO

Nel mondo, milioni di famiglie si servono quotidianamente di Internet come strumento didattico e di ricerca, per fare spese, acquisti importanti e operazioni bancarie, per investire, condividere foto, divertirsi con i videogiochi, scaricare film e musica, comunicare con amici, fare nuovi incontri e per tutta una serie di altre attività. Tuttavia, se è vero che il ciberspazio offre molti vantaggi, opportunità e comodità, è anche vero che presenta rischi crescenti, con nuove minacce che emergono numerose ogni giorno.
Ecco perché la prudenza è d'obbligo ad ogni connessione on-line.
Non appena un familiare diventa un utente attivo di Internet - indipendentemente dalla sua età - devi sensibilizzarlo al tema della sicurezza.
Devi tenere presente che anche se non hai installato un computer a casa, i PC sono disponibili praticamente ovunque : a scuola, in biblioteca, dagli amici e perfino negli oratori delle chiese. È essenziale che ognuno conosca i principi fondamentali dell'autoprotezione nel cyberspazio.

Città di
Reggio Calabria

ASSESSORATO
POLITICHE SOCIALI E DELLA FAMIGLIA

Recasi

Società appartente al gruppo Comune di Reggio Calabria

Internet oggi: la prudenza non è mai troppa

Il 50% degli adolescenti on-line ha fornito informazioni personali

- Gli hacker attaccano i PC dotati di accesso Internet ogni 39 secondi
- Secondo i produttori di Antivirus esistono oggi 222.000 virus informatici conosciuti in circolazione e il numero di minacce cresce di giorno in giorno
- Il 30% degli adolescenti ha subito atti di "cyberbullismo" una o più volte durante il periodo scolastico
- Nel 2008 i crimini in Internet sono cresciuti del 33% rispetto all'anno precedente
- Il 31% dei bambini è stato esposto a contenuti pericolosi
- Ogni anno 3,2 milioni di persone in tutto il mondo sono vittime di frodi di identità

SECUR SCUOLA

SICUREZZA ON LINE

Il posto giusto per il PC

Scegliere dove installare il computer domestico è una delle decisioni più importanti da prendere. Ti consigliamo di installarlo in una zona molto frequentata della casa e di limitare a poche ore il tempo che i tuoi figli passano davanti allo schermo.

Decidere insieme i limiti da rispettare

Stabilire esattamente cosa è ammissibile e cosa è inaccettabile riguardo a:

- Il tipo di siti web che si possono visitare
- Le chat e i forum ai quali è consentito partecipare:
  - Scegliere soltanto chat controllate
  - Accertarsi di rendere inaccessibili le chat/forum ".alt", dedicate a tematiche che possono non essere adatte ai più giovani
- Il genere di argomenti di cui è lecito discutere on-line e il linguaggio considerato sconveniente

Stabilire insieme le regole d'uso del PC

Ti consigliamo di rispettare i seguenti criteri:

- Non collegarsi mai con nomi utente che rivelano la vera identità personale o che possono risultare provocanti
- Non rivelare mai le proprie password
- Non rivelare mai numeri di telefono o indirizzi
- Non divulgare mai informazioni che rivelano l'identità personale
- Non divulgare mai fotografie sconvenienti o che possono rivelare l'identità personale (ad esempio: con nomi di città o scuole sulle magliette)
- Non condividere mai informazioni con estranei conosciuti on-line
- Non incontrare mai di persona estranei conosciuti on-line
- Non aprire mai allegati inviati da estranei

Accertati che il tuo PC sia protetto da un software di protezione efficace, capace di neutralizzare *virus, hacker e spyware e di filtrare i contenuti, le immagini e i siti web offensivi*. Il software deve essere aggiornato regolarmente, per far fronte alle nuove minacce che emergono quotidianamente.

Tutti coloro che si collegano on-line devono rendersi conto che gli "amici" virtuali sono e rimangono degli estranei.
Quando si chiacchiera on-line è molto facile mentire e fingere di essere qualcun altro. I bambini, in particolare, devono sapere che dietro un nuovo "amichetto" può in realtà nascondersi un uomo di 40 anni anziché un loro coetaneo.
I social network quali ad esempio Bebo, Orkut, MySpace e Facebook sono nati per favorire nuovi incontri on-line. Pertanto, i genitori devono visitare questi siti e verificare il profilo dei propri figli per accertarsi che non frequentino luoghi di conversazioni sconvenienti e di diffusione di fotografie disdicevoli.
I genitori devono inoltre controllare i messaggi immediati scambiati dai loro figli per accertarsi che non siano preda di molestatori on-line.
Insisti bene sul fatto che i tuoi ragazzi devono dirti se ricevono messaggi strani o sgradevoli durante una chat e che non ti arrabbierai con loro per questo né li punirai privandoli dell'accesso a Internet. Chiarisci che sei consapevole del fatto che non possono controllare quello che gli altri dicono e che non sono responsabili di questi episodi.

È bene inoltre controllare che i preadolescenti non subiscano o compiano atti di bullismo on-line. Non sempre all'uscita di scuola, i ragazzi e i loro compagni si lasciano i conflitti di classe alle spalle; e-mail, SMS e telefoni cellulari consentono agli studenti di rimanere sempre in contatto e non è da escludere che abusino della tecnologia per assillare, tiranneggiare e fare del male.

GLOSSARIO

Adware
Il termine adware indica una modalità di licenza d'uso dei programmi che prevede la presentazione all'utente di messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Talvolta i programmi adware presentano rischi per la stabilità e la sicurezza del computer.

Malware
Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito.

Phishing
In ambito informatico il phishing "spillaggio"è una attività illegale che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici. Grazie a messaggi che imitano grafico e logo dei siti istituzionali, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc..

Pop-up
I banner pop-up sono una forma di pubblicità presente sul World Wide Web e costituiscono una tipologia di web marketing definita promotion marketing online.
Si ha un popup quando alcuni siti aprono una nuova finestra del browser contenente il messaggio pubblicitario.

Spam
Lo spamming (detto anche fare spam o spammare) è l'invio di grandi quantità di messaggi indesiderati (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

Spyware
Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.

Trojan Horse
Un trojan o trojan horse, è un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.

Virus
Nell'ambito dell'informatica un virus è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.