Per non cadere nella rete

.... navigate a vista

IIIª Edizione 2007/08

Come difendersi in Internet

Serie di incontri-dibattiti tra operatori scolastici, educatori, genitori studenti ed autorevoli professionisti del settore, organizzati dal Comune di Ascoli Piceno, Assessorato alle Politiche Educative e Servizi Informatici.

Gli incontri sono incentrati sulle problematiche che scaturiscono dall'utilizzo senza protezioni della connessione alla rete Internet da parte dei minori in ambito familiare e scolastico e le tecniche di difesa da adottare.

SOMMARIO

OPUSCOLO INFORMATIVO PER GENITORI ED EDUCATORI

Premessa

Il nostro intento è quello di *mettere in guardia*, non di *terrorizzare* i genitori e insegnanti. Non c'è giorno, infatti, che non veniamo informati su un nuovo tipo di utilizzo distorto di Internet: gli arresti continui di pedofili sulla Rete, le torture e le uccisioni in Kenia, storie di droga, la violenza negli stadi di calcio, ecc……. si può leggere di tutto in Internet.

Gli aspetti positivi spesso passano in silenzio: "Internet facilita la circolazione di informazioni per la cura delle malattie tumorali".

Nessuno può negare che nella Rete ci siano anche delle cose negative, assolutamente da evitare ai nostri figli, solo che la loro quantità ci sembra esagerata, forse perché, come si dice, *"fa più rumore un albero che cade di mille che crescono"*.

In realtà, in Internet le cose buone sono di gran lunga più numerose di quelle cattive. **Bisogna rendersi conto che Internet è una comunità mondiale che rispecchia, nel bene e nel male, quella reale; ciò significa che il nostro atteggiamento non potrà essere quello di *"bruciare il paese per arrostire il maiale".***

***I pericoli in Internet ci sono*.**

Bisogna evitarli, non ignorarli.

Difendersi non collegandosi a Internet, significa escludere i propri figli da tutte le opportunità che la rete comunque offre. La linea di difesa più sicura resta sempre l'educazione ai valori e il rifiuto dei disvalori cui certi siti sono portatori.

Per fortuna che oggi ci sono anche molti altri modi per difendersi dai pericoli di Internet.

Il vero problema è che molto spesso i genitori non conoscono "il navigare in Internet"; una volta conosciuto, si possono dare le regole e i comportamenti necessari per evitare rischi.

Nella prima parte dell'opuscolo, illustriamo i possibili pericoli che i minori possono incontrare e si scoprirà che sono magari altri o diversi da quel che comunemente si pensa.

Nella **seconda parte**, chiarito che si passa sempre in un contesto educativo tra il minore, la famiglia e la scuola come valido supporto, verranno forniti alcuni consigli e indicazioni su come organizzare *in modo proficuo* la navigazione in Internet dei propri figli.

Nella **terza parte** si forniranno indicazioni sugli strumenti di controllo parentale attualmente disponibili. Con l'avvertenza che sarebbe comunque illusorio per gli educatori demandare a mezzi artificiali un compito che spetta loro e che va risolto nell'ambito dei rapporti personali a livello sia familiare che scolastico.

1. PERICOLI IN INTERNET

Bisogna tener sempre presente che quello che è considerato un crimine nel mondo reale, resta un crimine anche nel cyberspazio. Purtroppo è difficile per le forze dell'ordine controllare i molti siti che sono contrari alle leggi, ma non si deve mai dimenticare che genitori e insegnanti rappresentano la prima linea nella loro difesa on-line.

Oltre alla pornografia e alla pedofilia, su cui generalmente si accentra l'attenzione, ci sono altri pericoli nel cyberspazio: **l'esaltazione della violenza e della crudeltà**, la disinformazione e l'istigazione all'odio, **la pubblicità di tabacco e alcool**, **siti che raccolgono e vendono informazioni private sui nostri figli e sulla nostra famiglia**, che usano le **strategie di marketing interattivo rivolte ai bambini più piccoli.**

Inoltre, ci sono quei pericoli che i nostri figli e i loro amici on-line possono rappresentare per gli altri, noi compresi: possono **rendere note le informazioni sulla nostra carta di credito**; condividere informazioni private su di noi e la famiglia; non rispettare il copyright; commettere crimini col computer; **perdere o distruggere documenti** esistenti nel computer. E tutto questo magari inavvertitamente. Ci sono, infine, i rischi che i virus rappresentano per i *file* dei nostri computer.

1.1. La pornografia

È il più temuto e diffuso dei pericoli in Internet, anche se, forse, non è il più preoccupante. Com'è noto, il mondo del cyberspazio offre moltissimi siti che propongono materiale pornografico di tutti i generi e livelli di erotismo, molti ben oltre il limite della decenza e del buon gusto.

Resta il fatto che **la difesa dei minori dal materiale pornografico in Internet, diventa un problema familiare o** comunque che riguarda **le persone che nelle scuole o nelle biblioteche gestiscono l'utilizzo della Rete** con criteri e intenti educativi. A parte certe esagerazioni erotiche su cui, col solo buon senso non possono sussistere dubbi, il criterio dell'oscenità in Internet riguarda principalmente i singoli genitori che devono considerare il materiale osceno in relazione all'età e alla maturazione dei propri figli, oltre che alle proprie convinzioni personali.

Dopotutto è lo stesso problema che ogni insegnante e ogni genitore ha il cinema, con la televisione, persino con l'edicola di sotto casa.

1.2. La pedofilia

Inutile dire che la pedofilia è il pericolo più grave in cui un minore può incorrere navigando nella Rete. Da una parte, **ci sembra giusto dire che i pedofili non li crea Internet**, ma chi usa la Rete per questo genere di intenti, **è già pedofilo prima di mettersi on-line**; **ciò non toglie che**, purtroppo, come anche i recenti casi di cronaca dimostrano, **in Internet ci sia un rischio pedofilia da cui difendere i propri figli on-line.**

E il problema non è solo l'accesso, per altro non facile, ai disgustosi siti di pornografia infantile o del turpe commercio di materiale pornografico relativo a bambini; il vero grande problema è che un minore sia agganciato on-line da un pedofilo.

Incoraggiate i vostri figli a farsi amici on-line, ma è importante tenere il computer in un posto centrale della casa **e cercare di conoscere i loro amici on-line**, **per evitare queste particolari relazioni segrete.**

1.3. Disinformazione e pubblicità on-line

Internet è un modo economico e facile per diffondere informazioni. Nella Rete tutti possono pubblicare, tutti sono esperti. **Una delle cose più difficili da fare nel cyberspazio è separare la realtà dalla finzione.**

Il pericolo diventa chiaramente maggiore con la pubblicità che risulta molto attraente per i ragazzi. Come si può educare i figli alla difesa dalle esagerazioni pubblicitarie?

Questo tipo di disinformazione è un grosso problema, ancora senza una valida risposta tecnologica. **Tocca quindi a genitori e insegnanti fornire strumenti di conoscenza verso le**

"persuasioni occulte" e le fonti credibili, e soprattutto spiegare che, sia nella vita e sia in Internet, **non sempre le cose sono quel che sembrano**.

1.4. Odio, violenza e fanatismo

Internet abbonda di siti in cui dei propagandisti senza scrupoli diffondono l'odio ed esaltano la brutalità e la violenza; ecco perché il controllo dei siti a cui i figli possono accedere è fondamentale. **Bisogna che i bambini diventino scettici sulle sollecitazioni che ricevono, che siano informati e non disponibili a certi messaggi**. Purtroppo i messaggi ispirati dall'odio o scaturiti dal fanatismo sono per loro natura messaggi forti e particolarmente attraenti per minori non preparati a riceverli; non per niente la cultura, intesa come insieme di esperienze e conoscenze, è il maggior nemico che odio e fanatismo possono incontrare.

E' importante che genitori e insegnanti forniscano ai nostri bambini le conoscenze critiche tali da porli in condizione di fare debite distinzioni tra i valori, **saper distinguere i pericoli che derivano dal pregiudizio e dell'intolleranza verso i nostri simili**.

1.5. I Predatori del cyberspazio

Predatori (dall'inglese *predator*) è il termine con cui si possono designare quanti usano la Rete per scopi illeciti. Il vero problema è quello di scovarli. I messaggi che viaggiano via Internet, infatti, provengono da persone apparentemente *neutre*, cioè delle quali poco o nulla si può sapere con sicurezza per quanto riguarda genere, età, razza e religione.

Bisogna che noi e i nostri figli abbiamo sempre coscienza del fatto che, chi si incontra in Internet non è sicuro che sia quello che dice di essere; se dice la verità o mente; non si può mai sapere con sicurezza che età abbia, se sia maschio o femmina, la città da cui comunica. La regola base, su cui bisogna far convinti i nostri figli, è: **in Internet non sempre uno è quel che dice di essere**.

1.6. Flaming (il turpiloquio in Rete)

***Flaming* è il termine inglese per indicare quando qualcuno insulta o si comporta in modo scortese in una discussione on-line**. Spesso, purtroppo, il fatto di sentirsi anonimi fa dire alle persone quello che non direbbero mai direttamente, arrivando a vere e proprie forme di turpiloquio.

La cosa diventa ancora più fastidiosa quando i messaggi volgari arrivano anche ai bambini nelle loro chat room.

Di fronte ad un flame, cioè al turpiloquio on-line, **bisogna insegnare ai bambini anzitutto a riferirlo ai genitori,** oppure, se non è particolarmente disturbante, a ignorarla del tutto; **importante è comunque non rispondere mai**, **in nessun caso e, naturalmente, non inviare mai *flame* a nessuno.**

1.7. Cookie

Ci sono sostanzialmente due modi per perdere l'anonimato on-line: **uno, involontario, sono i *cookie* e l'altro, volontario, cioè fornendo noi stessi le informazioni che ci riguardano.**

I *cookie* sono dei mini-programmi con cui il *provider* può entrare nel disco fisso del nostro computer e raccogliere certe informazioni sul computer e sulla nostra navigazione.

Non tutti i *cookie* possono essere considerati come una ingerenza indebita; alcuni svolgono funzioni tecnicamente utili, come facilitare la connessione, altrimenti ci si dovrebbe registrare ogni volta che ci si connettete ad Internet.

Nell' *e-market* (mercato elettronico), ad esempio, i *cookie* servono anche a permetterci di acquistare on-line più di un articolo per volta. Anche nel *browser* ci possono essere *cookie* a scopo pubblicitario. I *cookie* possono in teoria essere rimossi dal nostro computer, in modo da poter navigare anonimamente; prima di farlo però bisogna essere sicuri che la rimozione non influisca sull'accesso al vostro *provider.* Quindi bisogna saper scegliere.

1.8. La privacy

Mettere on-line i propri dati privati è uno dei più seri pericoli in cui si può incorrere in Internet. Eppure il 90% dei siti per bambini chiedono loro i dati personali (nome, cognome, indirizzo, età) anche senza il consenso dei genitori; spesso, proprio riempiendo un questionario con i loro dati personali e familiari, i bambini ricevono in premio un accattivante omaggio.

I dati così raccolti possono poi essere usati per scopi commerciali, o addirittura essere venduti a terzi in un fiorente commercio di indirizzi oggi esistente.

Così come cerchiamo di difendere i nostri figli dai pericoli di Internet, così dovremmo cercare di difenderci dai pericoli che, magari inavvertitamente e non intenzionalmente, **loro possono causare a noi e ai nostri amici**; **anche perché spesso, essendo a casa loro, i nostri figli credono di essere anonimi e non si rendono conto della gravità di questi fatti**.

1.9. La propaganda della violenza

Abbiamo già detto che nell'immenso mondo di Internet ci sono anche siti che diffondono messaggi di odio e fanatismo, con forme di vera e propria violenza sui minori; **altri siti, invece, si propongono di insegnare la violenza, di diffondere tecniche sull'uso della stessa.**

Un buon metodo di protezione è anche un programma filtro che blocchi questi siti. Fondamentale resta comunque acquisire la fiducia dei figli e far crescere in loro il senso di responsabilità.

1.10. Alcool, tabacco e droga

La propaganda all'uso di queste sostanze, come ben si sa, non è solo un problema di Internet, ma un problema più generale, ormai da anni entrato nel dibattito dell'opinione pubblica attraverso i mass-media.

Diventa allora imperativo morale, anzitutto, educare i minori a prendere coscienza dei pericoli della droga, dell'alcool e del tabacco. **Ma i genitori possono difendersi anche con programmi filtro che bloccano i siti in base a parole chiave o che sono compresi nelle liste dei siti proibiti** (si veda Strumenti di controllo parentale).

1.11. Il cyber-gioco d'azzardo

Anche il cyberspazio non è sfuggito al gioco d'azzardo. Di solito i siti che gestiscono i *cyber-casino* chiedono di versare anticipatamente con carte di credito la cifra che si vuol giocare. Bisogna inoltre considerare che i siti illegali sono migliaia e che, per i gestori questi casino virtuali, il denaro dei minori è buono quanto quello di altri.

È quindi necessario tenere sotto stretto controllo la carta di credito e le disponibilità finanziarie dei figli, bloccando la possibilità non solo di usare fondi, ma anche di fornire dati personali. Inoltre, occorre far capire che al gioco d'azzardo on-line è una grande beffa perché non si vince, e gli unici a guadagnare sono gli organizzatori dei siti.

1.12. Cracking

Un *cracker*, nome inglese per “pirata informatico”, **è una persona che entra nei siti altrui, talvolta per gioco, per sfida, per curiosità o talvolta con scopi criminosi, come distruggere file, diffondere virus, modificare dati, ecc.**

Il vero problema è che non c'è una diffusa coscienza del crimine informatico, per cui un *cracker* è a volte considerato una specie di eroe della *Internet generation*. Per far capire che il cracking è un crimine da combattere, bisognerebbe chiedere ai minori di porsi mentalmente dalla parte dei danneggiati, delle vittime, il cui computer di casa venga visitato e danneggiato da estranei nei file a cui tengono di più.

1.13. I diritti d'autore.

Troppo spesso ci si dimentica che le leggi applicate nella realtà valgono anche nel cyberspazio. Tra queste leggi ci sono anche quelle che regolano **il diritto d'autore (copyright) e la proprietà intellettuale delle opere in genere.**

La facilità con cui con il computer si può copiare, tagliare e incollare materiale altrui per utilizzarlo, fa spesso dimenticare che si tratta di una infrazione contro le leggi del copyright. On-line valgono le stesse regole della riproduzione di immagini, citazioni e bibliografie altrui che vigono in altri ambiti. **L'insegnamento al rispetto delle opere altrui, aiuta anche all'apprezzamento e alla valorizzazione delle creazioni in genere.**

1.14. Segreto d'ufficio

È dimostrato che metà delle persone si connettono a Internet per lavoro. Per un datore di lavoro si pone quindi il problema di un uso improprio di Internet da parte dei dipendenti, **con tutti i possibili rischi di crimini come la diffamazione, il non rispetto dei diritti d'autore, diffusione di segreti commerciali e mancanza di riservatezza, molestie e criminalità amministrativa.**

Inoltre, per quanto sia facile farlo, non è certo educativo usare l'*account* commerciale della nostra ditta a casa propria per metterci on-line con i nostri figli.

1.15. Proteggersi dai virus

Un virus è uno speciale codice informatico contenuto dentro un programma predisposto per infettare un file quando viene eseguito. Con un virus si può rovinare un file, ma si può anche cancellare il disco fisso. Se improvvisamente il vostro computer fa qualcosa di strano, prima di tutto controllate che non sia un virus. Gran parte dei virus provengono comunque dai floppy disk che fanno funzionare programmi infetti.

In Internet è molto difficile prendersi un virus, ma quelli che ci sono, sono molto pericolosi e possono provocare gravi danni al sistema.

Per evitare i virus ci sono oggi in commercio efficaci programmi di protezione che esaminano il disco fisso e rimuovono eventuali virus. Ci sono anche molti messaggi e-mail con cui si segnala la presenza di virus inesistenti; sono scherzi di pessimo gusto, quindi da evitare.

2. *DIFENDERSI BENE*

È difficile per i genitori mantenersi al passo con le conoscenze e le competenze informatiche dei loro figli; ma la funzione di controllo, che spetta principalmente a loro, può essere efficacemente svolta anche senza essere maghi del computer.

Da una parte bisogna avere una informazione di base sul funzionamento del computer, sulla navigazione in Internet e sul cyberspazio in generale, dall'altra, con queste conoscenze di base, si può esercitare quel "controllo discreto" che ci permette di assicurarci di evitare ai nostri figli i pericoli maggiori della navigazione in Internet.

Di seguito, forniamo alcuni consigli di cui i Genitori dovrebbero tener conto quando hanno dei figli che navigano nella Rete.

2.1. Quando nostro figlio ha l'età giusta per cominciare con il computer ?

Non c'è un'età prestabilita, soprattutto non c'è nessuna gara da vincere con i genitori di altri bambini. **Più importante è invece dosare opportunamente i tempi di utilizzo del computer**, per bilanciarlo con le altre attività che sono tipiche della vita di un bambino.

La navigazione in Internet dei figli andrebbe opportunamente bilanciata non solo all'interno dell'organizzazione della giornata, ma anche rispetto al tempo dedicato a guardare la tv.

Da raccomandare ancora una supervisione da parte dei genitori delle attività informatiche dei figli, con un controllo più o meno discreto sulla navigazione in Internet.

2.2. Quando si capisce che è abbastanza?

I genitori devono preoccuparsi che i loro figli non eccedano nelle attività con il computer e nella navigazione on-line. Bisogna aiutarli a non esagerare.

Assicuriamoci quindi che nostro figlio non passi troppo il suo tempo al computer, sacrificando altri aspetti della sua vita che sono fondamentali per l'equilibrio della sua crescita.

2.3. La password

La password (o parola d'ordine) è la parola o il numero che funziona da chiave, ed è indispensabile per entrare in un dato computer o programma informativo. Proprio per questo **la password non va condivisa con i propri figli** e va conservata dove non la possono trovare.

Una password deve essere facile da ricordare, ma non ovvia da indovinare. **Quando la digitate non permettete che nessuno la veda e cambiatela di frequente. Non mettetela mai nel disco fisso.**

2.4. Quando i figli navigano fuori casa

Proteggiamo i nostri figli anche quando non navigano in Internet a casa. Assicuriamoci di avere le stesse idee e di adottare gli stessi criteri sulla sicurezza on-line, dei genitori degli amici di nostro figlio, e che anche loro siano in grado di assicurare quella stessa sicurezza in Internet che noi cerchiamo di garantire ai loro (e ai nostri) figli a casa nostra.

2.5. File importanti

Non lasciamo nel nostro computer file importanti senza aver fatto un back-up o una copia su floppy. Assicuriamoci con una password dal pericolo di cancellazione involontaria e accidentale dei nostri file.

2.6. Carte di credito

Non mettiamo le informazioni della nostra carta di credito nel computer. È comunque una tentazione. Per il resto non preoccupiamoci di usare la carta di credito on-line purché seguiate queste regole:

- Fornite le informazioni sulla vostra carta di credito solo su linee sicure.
- Anche se la linea è sicura, assicurarsi di star trattando con una ditta seria e, soprattutto, che siano quelli che dicono di essere.

2.7. Il computer di casa

Anche il computer di casa va gestito in base ad alcuni criteri di cui si dovrebbe tener conto quando si hanno figli che navigano in Rete:

- Tenere il computer un una zona centrale della casa e non nella stanza dei ragazzi.
- Anche gli amici hanno eventualmente più difficoltà a provocare nostro figlio se ci siamo noi attorno.
- Diciamo a nostro figlio che in Internet molte persone non sono quello che dicono di essere.
- Assicurarsi di poter vedere sempre cosa c'è sul monitor e fate capire a nostro figlio che di tanto in tanto diamo un'occhiata a quello che fanno in on-line.
- Ogni tanto controllare il nostro disco fisso per verificare cosa è stato scaricato. Far capire a nostro figlio che controlliamo ciò che viene scaricato.
- Coprire le proprie tracce. Se avete visitato siti che non volete far vedere a vostro figlio, cercare di eliminare le tracce dall' hard disk e dal bookmark.
- Non far navigare da soli i nostri figli finché non siete sicuri che siano pronti a farlo con sicurezza, rispettando le regole, delle quali le 2 più importanti sono:
- Assicurarsi che nostro figlio sappia quali informazioni possono e quali non possono essere condivise con altri on-line.
- Assicurarsi che nostro figlio sappia che è pericoloso incontrare di persona qualcuno che ha conosciuto on-line.
- Essere parte attiva e interessata nella vita on-line di nostro figlio, cercare di conoscere i suoi amici e corrispondenti on-line.
- Non critichiamo aspramente nostro figlio se c'è qualcosa che non va bene, in modo che si possa fidare e si rivolga a voi quando si sente a disagio o riceve messaggi che violano le regole stabilite con noi.
- Non fare grande affidamento nel software per prevenire i pericoli in Internet; quello resta un nostro compito.
- Bisogna sapere se possiamo fidarci di nostro figlio. Bisogna educarlo sui rischi dell'hacking, su un comportamento adatto on-line, e a rispettare le regole della Rete.
- Se si capisce di non poterci fidare di nostro figlio, blocchiamo il computer e portiamo la chiave con noi. Si tratta di salvarlo dai guai.

2.8. Non accettare niente da estranei

Nel cyberspazio gli estranei entrano via Internet a casa nostra, dove i nostri figli si sentono più sicuri. I cyber-predatori contano su questo senso di intimità familiare per convincere i nostri figli che non sono per niente estranei. Invece lo sono.

2.9. Non dire cose offensive sugli altri

Parlare male degli altri nel cyberspazio si chiama *flaming*; questo va contro la netiquette (oltre che contro il buon gusto e l'educazione) e provocherà la reazione degli altri interlocutori on-line. Nel caso si venga coinvolti, bisogna dirlo subito al sysop (*system operator*, gestore del sistema) o ai genitori.

2.10. L'educazione non guasta mai

L'educazione e il rispetto per gli altri sono le regole base per ogni area on-line. Ogni chat-room poi ha le proprie regole:

- Non entrare nella discussione prima di aver capito bene di che cosa parlano.
- Leggere l'argomento delle ultime 2 settimane invece di chiedere di che cosa hanno parlato finora.
- Rispettare gli altri e le loro opinioni.
- Non mettere messaggi dappertutto.
- Se qualcuno ci aiuta dire "grazie"; anche nel cyberspazio con la cortesia si va lontano.

2.11. Non dare alla gente proprie informazioni personali

Non dare informazioni personali sulla propria famiglia, **non si sa mai con chi si sta parlando,** e anche se si crede di saperlo, ci possono essere altre persone che possono essere in ascolto senza che noi lo sappiamo. Sarebbe come scrivere il nostro diario su una cartolina. Cercare di assicurarsi che i figli sappiano esattamente cosa intendete per informazioni personali.

2.12. Punti da considerare nel regolamento d'uso di Internet

Con i propri figli cercare di stipulare una vero e proprio regolamento con le norme sull'uso di Internet. Le regole dovrebbero mirare ad aiutarli a rispettare la *netiquette*, a sapere che cosa aspettarsi dagli altri on-line, a come comportarsi quando succede qualcosa di strano e a come proteggersi dai pericoli del cyberspazio.

Ecco alcune regole base che suggeriamo di includere nella polizza e che naturalmente si è liberi di cambiare per adattare a noi e ai nostri figli:

- La gente in Internet può fingere di essere chiunque; non farsi prendere in giro.
- Non usare un linguaggio improprio.
- Non entrare in dispute e non rispondere a chi usa un linguaggio improprio.
- Non rispondere se qualcuno dice qualcosa che vi mette a disagio e che avvertite come inopportuno.
- Se qualcuno sta facendo qualcosa che vi turba, dovreste dirlo subito ai genitori. Ma non spegnete il computer o non disconnettetevi dall'area dove questo succede (L'adulto potrebbe scoprire chi è e riferire queste attività come violazione alle norme del servizio).
- Usate un nome finto quando siete on-line, non il vostro vero cognome e nemmeno il vostro nome.
- Non trascorrete tutto il vostro tempo on-line; stabilite limiti all'uso del computer.
- Non date mai a nessuno il vostro nome, indirizzo, scuola, nomi dei genitori, dove lavorano, l'indirizzo e-mail di qualche altro o il numero di telefono.
- Se qualcuno vi chiede queste informazioni, non rispondete, e ditelo ai vostri genitori o agli adulti che gestiscono la chat-room.
- Non parlate mai al telefono con qualcuno che avete incontrato on-line, non mandate loro nulla e non accettate nulla da loro e non accordatevi di incontrali, a meno che i vostri genitori siano d'accordo e vi accompagnino.
- Non mostrate mai a nessuno la vostra fotografia on-line senza il consenso dei genitori.
- Non mettete alcuna informazione on-line senza il consenso dei genitori
- Ci sono posti in Internet dove la gente parla di cose e mostra immagini su cui i vostri genitori non sono d'accordo. Se vedete qualcosa del genere, cliccate sul bottone *back* e ditelo ai vostri genitori.
- Non fate niente on-line che costi denaro, a meno che i vostri genitori non siano d'accordo.
- Non date mai a nessuno la vostra password.
- Non date mai informazioni sulla vostra carta di credito.
- Non copiate materiale altrui fingendo che sia vostro.

Se questa polizza va bene si può usarla, altrimenti può rappresentare una traccia per una di nostra.

2.13. *Netiquette*

Per quanto sia una cultura del tutto nuova, anche in Internet ci sono delle **regole di comportamento, alla cui base c'è il rispetto per gli altri.** In queste regole, all'inizio di Internet credevano fermamente i cosiddetti *techies* (patiti del computer) che sognavano un mondo virtuale basato sulla libera espressione, sulle regole della generosità e dell'altruismo, contro ogni forma di censura e di sfruttamento commerciale. Poi invece, purtroppo, il romanticismo è finito e anche nella Web è invalso il principio del *business is business* (gli affari sono affari).

Dobbiamo convincere i nostri figli a non dire e a non fare mai on-line cose che sanno non devono essere dette o fatte nel mondo reale.

Ecco alcune regole della netiquette:

Da non fare

- ☑ Scrivere una parola a lettere maiuscole è considerato gridarla
- ☑ Incitare o provocare una lite (*flaming*).
- ☑ Mettere on-line un annuncio in molti siti nello stesso tempo (tecnicamente si chiama *spamming*), ciò che costituisce una forma di indebita invadenza; mentre abbiamo i mezzi per difenderci dalla pubblicità indesiderata (televisiva o cartacea) in quella on-line dobbiamo addirittura pagare il tempo di connessione quando scarichiamo le e-mail nel nostro computer.

2.14. *Emoticon*

Ridere nel cyberspazio: dal momento che on-line non si possono comunicare le varie emozioni, come ad esempio il sarcasmo, la presa in giro, l'umorismo, **ci sono degli «indicatori di emozioni» chiamati "*smiley*" o "*emoticon*".**

2.14. Acronimi

Come nei fax anche nei messaggi e-mail si fa largo **uso di abbreviazioni.**

3. ALCUNE TECNICHE DI DIFESA

3.1. Software di controllo parentale

I prodotti per la sicurezza informatica dei minori sono di diversi tipi.

- Alcuni possono bloccare l'accesso ai siti *"cattivi"* o permettere l'accesso solo ai siti *"buoni"*.
- Altri "filtrano" le parole per cercare quelle proibite e impedire l'accesso al sito in cui si trovano; qualcuno, per prevenire il blocco di frasi innocue, le filtra non come termini isolati ma nel loro contesto.
- Alcuni avvertono quando si entra in certi siti, mentre altri vi bloccano l'accesso senza che ce ne possiamo accorgere.
- Ci sono software che controllano persino l'uso del computer off-line, come per quante e quali ore viene usato dal minore.
- Ci sono provider come Aol (America on-line) che usano difese funzionanti solo per i loro programmi, alcuni sono utilizzabili solo on-line, mentre altri solo in Internet.
- Si può infine usare software di controllo parentale per bloccare o filtrare le informazioni in entrata o impedirne l'uscita. Anche i motori di ricerca possono essere bloccati.
- Alcuni programmi sono adattabili, altri sono predeterminati dal produttore, altri ancora offrono diversi livelli di protezione per bambini diversi di età e maturazione.
- Molti dei migliori programmi combinano opzioni diverse per offrire la migliore protezione e il massimo di flessibilità.

Gli atteggiamenti estremi dei genitori verso la navigazione in Internet da parte dei figli, sono da evitare. La giusta misura di controllo è forse il modo migliore di acquisire fiducia da parte loro; soluzioni intermedie che i genitori responsabili devono adattare alle specifiche caratteristiche e alla evoluzione della crescita dei loro figli.

3.2. Metodi di controllo parentale

Ci sono sostanzialmente 3 metodi oggi in uso per permettere ai genitori di controllare l'accesso dei figli a certe informazioni e a certi siti in Internet.

- **Il più popolare è di bloccare o di filtrare il software installato nel vostro computer**. I più conosciuti sono **CyberPatrol**, **Cybersitter**, **NetNunny** e **Surf Watch**. La maggior parte di questi programmi ha una lista predeterminata di siti *"cattivi"*, che vengono bloccati quando il programma viene attivato. Il database dei siti cattivi deve essere continuamente aggiornato, e per questo alcune ditte richiedono un abbonamento. Alcuni di questi programmi controllano il computer sia on-line che off-line. Alcuni forniscono anche una protezione in uscita per impedire ai vostri figli di diffondere dati personali.
- **Il secondo metodo è il blocco dei programmi presso il server con cui si ha l'accesso a Internet.** Il software non viene quindi installato nel vostro computer; diventa così più difficile per vostro figlio by-passarlo, ma il programma non può essere da voi configurato. Il più diffuso si chiama **Bess.**
- **Il terzo metodo**, quello su cui oggi la maggior parte dei professionisti esperti contano, **è PICS (*Platform of Internet Content Selection*, piattaforma di selezione dei contenuti di Internet), consente di controllare i siti in base a determinati standard di valutazione dei contenuti, permettendo l'accesso solo a siti che offrono livelli di sicurezza scelti dai genitori.**

3.3. Elenchi di siti da evitare

Sono programmi che bloccano l'accesso a siti considerati indesiderabili o da evitare ai minori, **in base ad una lista formulata sia dal produttore che dai genitori**; alcuni di questi programmi permettono infatti ai genitori di aggiungere o togliere dei siti dall'elenco, adattandolo al proprio figlio.

Spesso con l'acquisto del programma si fa anche l'abbonamento agli aggiornamenti periodici; per altri l'abbonamento viene fatto pagare extra.

3.4. Accesso solo a siti approvati

Alcuni produttori, riconoscendosi incapaci di star dietro all'evoluzione dei siti da evitare, **hanno optato per una lista di "siti buoni", cioè adatti ai minori**. In questi casi l'acceso è possibile solo ai siti compresi nell'elenco, escludendo tutti gli altri; **il problema è che questi programmi bloccano l'accesso anche ai nuovi siti, magari solo perché non sono ancora in elenco.** Anche questi programmi possono avere degli elenchi di siti aggiornabili per abbonamento. Resta anche in questo caso opinabile il criterio con cui questi siti vengono considerati *"buoni"*.

L' Assessore alle Politiche Educative e Servizi Informatici
(*Dr. Giovanni Silvestri)*

INFO:

Comune di Ascoli Piceno
Assessorato alle Politiche Educative –Servizi Informatici
Via Giusti, 1
Tel. 0736-298558
Fax: 0736-298560
sito: www.comune.ascolipiceno.it
e_mail*: pubblica.istruzione@comune.ascolipiceno.it*

Un ringraziamento particolare per la disponibilità:

***Nello Giordani** sociologo del Comune*
***Maurizio Pierlorenzi** responsabile regionale del nucleo di Polizia postale e delle comunicazioni*
***Patrizia Carosi** responsabile del nucleo ufficio minori della Polizia di Ascoli Piceno*
***Massimiliano D'Angelo** ideatore progetto, consulente organizzativo ICT*