RACCOMANDAZIONI PER LA SICUREZZA DEI MINORI IN RETE AD USO DEI GENITORI

Le presenti Raccomandazioni sono destinate ai genitori, allo scopo di informarli sugli eventuali rischi nei quali i figli in età minore possono
incorrere umizzando Internet, e di suggerire qualche soluzione.
INTERNET costituisce la più vasta rete di reti di computer esistente. Creata come strumento per lo scambio elettronico di informazioni tra un limitaio numero di organizzazioni essa si è velocemente estesa a livello mondiale, aprendosi anche a privati cittadini e modificando, così, profondamente la sue funzioni originarie, lnternet, oggi, offre non solo la possibilità di scambio di informazioni, ma anche una gamma di servizi sempre più ampia e diversificata: dalla posta alle conferenze elettroniche, dei servizi gratuiti per i cittadini ai servizi commerciali, fino alle operazioni finanziarie. Considerando l'evoluzione tecnologica e Ia diffusione sempre crescente di internet è difficile prevederne i possibili ulteriori sviluppi. Internet ,dunque, é nata come strumento per gli adulti; benché attualmente siano disponili in rete servizi informativi, educativi e
ricreativi specificameme destinati ai bambini e ragazzi, tuttavia il libero accesso ai siti e l'assenza di un efficace sistema di controllo dell'uso da parte di questi, rendono possibile che i ragazzi si tirovino ad imbattersi in situazioni poco appropriate o addirittura rischiose.

Quali i rischi?

Gli eventuati rischi per il minore possono riguardare

1) la sua tutela intellettuale ed educativa:

- l'attendibilità non sempre garantita delle informazioni presenti in rete; il facile accesso a siti con contenuti scabrosi, violenti, razzisti;
- il libero accesso a newsgroup o chat (conferenze elettroniche) che affrontano i temi più vari e senza alcun controllo sulla qualità degli interventi:

2) la sua sicurezza personale:

- la comunicazione di dati strettamente personali (nome. eta, indirizzo. telefono, ecc), anche quando indirizzata a persone ritenute di fiducia, per la possibilità che i dati stessi siano catturati da altri utenti e utilizzati per scopi illeciti;
- l'anonimato o la possibilità che gli interlocutori del minore si presentino sotto falsa identità (nome, età, interessi, ecc.) per carpirne con l'inganno l'attenzione e la fiducia a fini illeciti o lesivi del suo equilibrio psicologico o della sua incolumità;

3) le sicurezza finanziaria personale o dei genitori:

- possibilità di fare acquisti - anche di grossa entità - e di eseguire operazioni finanziarie dietro semplice comunicazione del numero di carta di credito; possibili usi impropri, da parte di terzi che li catturino, delle coordinate e dei dati bancari (conti correnti, numeri di carte di credito, ecc.) inviati in linea;

4) la sicurezza legale, in quanto è possibile incorrere, anche non intenzionalmente, in infrazioni a leggi vigenti (comportanti anche conseguenze civili o penali), quali:

- la violazione del copyright (scarico e riutilizzazione - senza autorizzazione dell‘autore - di testi, fotografie, immagini, partiture, ecc.);
- la copia e distribuzione di software non definito di “pubblico dominio“ - shareware;

- la violazione della privacy (in caso di comunicazione a terzi di dati personali non riguardanti se stessi

L'accesso non permesso a sistemi informativi privati (hacking).

Soluzioni possibili

Esistoni varie soluzioni che i genitori possono adottare per limitare in qualche modo l'accesso indiscriminato dei minori ai siti ed evitare che siano contattati da altri per scopi illeciti:

L'educazione all'uso:

Apparentemente è la soluzione più impegnativa ma senz'altro anche la più efficace. Essa richiede all'adulto la conoscenza di internet e una buona esperienza di "navigazione", oltreché un rapporto di confidenza e fiducia con il minore. In altre parole, l'adulto dovrà essere in grado di spiegare al ragazzo in maniera esauriente (assumendo il ruolo di persona dotata di esperienza e di guida, piuttosto che di censore) quali sono le risorse presenti sulla rete, mettendo al contempo in guardia contro eventuali rischi della navigazione e suggerendo un codice di comportamento attento e responsabile (allo scopo so invita a prendere visione delle Raccomandazioni per una navigazione sicura ad uso dei miinori).

In sintesi, le regole da seguire possono essere le seguenti:

- fare esperienze di navigazione comune;
- stabilire insieme' in un clima di "complicità reciproca", i siti che meritano di essere visitai oppure no;
- spiegare come funziona la pubblcità in linea e quali possono esseme gli scopi;
- convincere il ragazzo della necessità della riservatezza dei dati personali e della famiglia;
- spiegare che un atteggiamento di scarsa responsabilità in rete può far incorrere, anche inconsapevolmente, in illeciti.

I filtri

I filtri sono sistemi in grado di bloccare in modo automatico l'accesso ad alcuni siti o l'uso di determinati servizi che si possano ritenere non appropriati ai minori.

Il sistema di filtraggio attuato nella Biblioteca di Taglio di Po è basato sulla **piattaforma OpenDNS** che ha introdotto da poco un sistema di "content filtering and security". Questa funzione si basa sulla reputazione e sulla classificazione dei vari siti web. Infatti il sistema prevede diversi livelli di "content filtering" in base appunto al contenuto di questi siti.

Nello specifico si è scelto di configurare un sistema "ad-hoc" andando a scegliere manualmente quali categorie di sito web bloccare (es. Pornografia, Militare, Armi, Alcool etc.), aggiungendo anche delle eccezioni verso alcuni siti web consentiti (es. Youtube) che altrimenti sarebbero stati oscurati in quanto facenti parte di categorie segnate come blocco.

Quando l'utente cerca di andare a visitare o richiamare un contenuto non consentito il sistema mostra in automatico un avviso, segnalando che il contenuto richiesto non è permesso.

Essendo questi filtri progettati anche per la sicurezza nel web offrono protezione bloccando quei siti ritenuti avente codice malevolo o responsabili di phishing/malware/virus.