ISTITUTO COMPRENSIVO DI MESENZANA
Via Diaz,35 – 21030 Mesenzana – Tel. 0332/575201
Fax. 0332/575546
e-mail: **ics.mesenzana@libero.it** -
SITO WEB: **www.icsmesenzana.com**

"Sicurezza dei minori in internet: come proteggere i nostri figli dai rischi della rete"

Intervento dell'Insegnante Bellavita Mavie Annalisa

Introduzione

Il computer è entrato nelle case di gran parte delle famiglie; esso stimola le facoltà intellettive e la partecipazione responsabile dell'utente; esso ci pone di fronte alla realtà e ci permette di scegliere da soli il nostro campo di interesse, senza influire interferenze esterne.

È naturale che i giovani si siano appropriati del computer, in quanto sono desiderosi di imparare e giocare con questo oggetto ricco di colori, immagini, suoni e animazioni.
Sappiamo bene che il mezzo che permette al computer di estendere le sue potenzialità, diventando un protagonista di ricerche e un interlocutore senza confini, si chiama Internet. Esso diventa uno specchio della realtà attraverso cui è possibile compiere viaggi interessanti, ma che cela insidie e pericoli; è compito di genitori e docenti insegnare ai giovani come difendersi dai pericoli che incontrano.

Il computer, oltre a fornire possibilità di lavoro e di svago sempre più raffinate, costituisce il più importante strumento di ricerca e comunicazione, che è riuscito ad annullare le distanze: non soltanto tra un individuo e l'altro,ma tra Paesi e culture. Il Pc diventa quasi un amico, intelligente e disponibile ad aiutare i ragazzi nello svolgimento delle attività quotidiane, studio e gioco compresi.
Internet è uno strumento sempre più utilizzato dai giovani perché rappresenta una straordinaria opportunità di informazione, apprendimento, svago e comunicazione che li supporta nello svolgimento delle attività quotidiane, dallo studio all'entertainment.
Come ogni mezzo, oltre ai vantaggi, ha anche dei difetti: violenza, razzismo, pornografia, pedofili in agguato dietro chat, forum apparentemente innocui o linee telefoniche a pagamento celate dietro siti Web.
È necessario che i genitori ne sappiano di più sui meccanismi di Internet e sulla attrattiva che esercita sugli adolescenti: è giusto visitare i siti, valutarne i contenuti e successivamente consentire ai ragazzi l'esplorazione. I genitori, confrontandosi con questa nuova tecnologia, possono dare indicazioni ai propri figli dei pericoli potenziali che si nascondono in Rete. È necessario parlare con franchezza ai ragazzi e lo si può fare solo se coscienti del funzionamento.
Così come ognuno dà ai propri figli delle regole su come dovrebbero comportarsi con gli estranei, su quali spettacoli televisivi, film e video guardare, in quali negozi entrare, quanto lontano da casa andare, allo stesso modo è importante stabilire regole per l'uso di Internet.
Occorrerà anche assicurarsi che esplorare il Web non prenda il posto dei compiti, delle attività sociali o di altri importanti interessi.
Proprio come si dice ai propri figli di essere diffidenti verso gli estranei che incontrano, si deve dir loro di essere prudenti con gli estranei in cui si imbattono in Internet.

- È importante insegnargli alcune regole base per un uso sicuro di Internet.

- Mai dare informazioni personali, quali nome, indirizzo, numero di telefono, età, razza, entrate familiari, nome e località della scuola, o nome degli amici.
- Mai usare una carta di credito on-line senza il vostro permesso.
- Mai condividere le password, neanche con gli amici.
- Mai accettare un incontro di persona con qualcuno conosciuto on-line.
- Mai rispondere a un messaggio che faccia sentire confusi o a disagio. Meglio ignorare il mittente, terminare la comunicazione e riferire quanto accaduto immediatamente a voi o a un altro adulto di cui si fidano.
- Mai usare un linguaggio offensivo o mandare messaggi volgari on-line.

Se il bambino o il ragazzo si imbatte in una brutta esperienza e viene a riferirvelo, lodatelo e ditegli che ha fatto la cosa giusta.
Ricordatevi che i bambini hanno spesso la convinzione che sia colpa loro se qualcuno usa un linguaggio osceno o fa loro delle avances. Dite subito che non siete in collera e che non è assolutamente colpa loro.
Ricordategli che non siamo circondati da persone cattive, ma che su Internet ci sono alcune persone che fanno cose sbagliate e che è fondamentale stare attenti, proprio come starebbero attenti se un estraneo li chiamasse al telefono, suonasse alla porta o li fermasse per strada.
Assicuratevi, inoltre, che i ragazzi sappiano che le persone che incontrano on-line non sono sempre quelle che dicono di essere e che le informazioni on-line non sono necessariamente private.
Inoltre ricordatevi che in Internet i vostri figli potrebbero imbattersi in materiali osceni, pornografici, violenti, pieni di odio, razzisti, o in altro modo offensivi, per cui:

- Assicuratevi che i vostri figli capiscano ciò che voi considerate adatto per loro. Quali tipi di siti siete contenti che visitino. Quali zone sono off limits, cioè proibite. Quanto tempo possono trascorrere al PC. Stabilite regole chiare, ragionevoli, e le conseguenze per il mancato rispetto.
- Fate dell'esplorazione on-line un'attività di famiglia. Mettete il computer in salotto o nel soggiorno. Questa sistemazione coinvolge tutti e aiuta a controllare quello che fanno i figli.
- Fate attenzione ai giochi che i vostri figli scaricano o copiano. Alcuni sono violenti o hanno un contenuto a sfondo sessuale.
- Ricordate che nulla può sostituire la supervisione dei genitori anche nell'esplorare la Rete.

È molto importante mostrare ai figli come usare e valutare le informazioni che trovano su Internet. Non tutte le informazioni on-line sono affidabili. Alcune persone o organizzazioni sono molto attente circa l'accuratezza delle informazioni che spediscono, ma altre no; alcune arrivano perfino ad alterarle di proposito. Ricordate di non copiare informazioni on-line, propagandandole poi come proprie, e di non copiare software, a meno che non sia chiaramente indicato come gratuito (Freeware – Open source).
Non è necessario privare i ragazzi e i genitori di opportunità nuove, di esperienze stimolanti e dell'opportunità di imparare qualcosa assieme eliminando internet.

È molto importante imparare a riconoscere i segnali d'allarme della dipendenza da Internet nei ragazzi, perché la Rete ha la capacità di sedurre e ammaliare.

Segnali d'allarme nei ragazzi

Stanchezza eccessiva. Vostro figlio fa fatica ad alzarsi al mattino, più di quanto facesse prima della comparsa del computer nella sua vita? Avete notato che tende ad assopirsi durante la cena o nei fine settimana? Come per gli adulti, i cambiamenti nelle abitudini del sonno dei ragazzi rappresentano spesso il primo indicatore di un eccessivo numero di ore passato al computer.

Problemi scolastici. Il profitto scolastico sta calando? Solitamente, l'ultimo colpevole di cui si vada a sospettare è il computer. Si è convinti che quando il ragazzo è lì a "smanettare" stia diligentemente facendo i compiti o scrivendo un saggio. Molto probabilmente, invece, si sta perdendo nei meandri della Rete invece di fare i compiti.

Diminuzione dell'interesse per gli hobby. Dopo aver fatto l'abbonamento a Internet, i ragazzi perdono interesse per gli altri hobby? Internet diventa più di un nuovo hobby: è un'ossessione che può rendere tutte le altre attività prive di senso.

Isolamento dagli amici. Si rifiuta di frequentare la compagnia di sempre? Un ragazzo Internet-dipendente sviluppa un attaccamento morboso verso i suoi fratelli e sorelle virtuali, diventando sempre più distante dagli amici e dalla famiglia.

Disobbedienza e ribellione. Il ragazzo ha reagito con aggressività a domande relative all'uso di Internet? Una reazione ostile è segnale di autodifesa.
Gli adolescenti possono diventare psicologicamente dipendenti per le caratteristiche interattive di Internet. Chattando, esplorando e giocando stanno meglio con se stessi ed evitano, al tempo stesso, lo stress della scuola, dell'adolescenza e della vita familiare. Un ragazzo depresso per motivi scolastici o familiari potrebbe trovare nella Rete una via di fuga rassicurante.
Un ragazzo ansioso, invece, può trovare una temporanea calma per la facilità di accettazione e comunicazione tra gli amici della Rete. Con l'aumentare delle ore passate su Internet, questa caratteristica "sedativa" acquista sempre maggiore attrattiva.

Strategie da usare con i ragazzi Internet-dipendenti

Presentare un fronte unito. Entrambi i genitori devono prendere sul serio l'argomento. È importante perché altrimenti il ragazzo farà appello al genitore più scettico e creerà una divisione all'interno della coppia.

Dimostrare affetto e interesse. Fate capire a vostro figlio che gli volete bene, che i suoi comportamenti anomali vi preoccupano e che, se vi interessate a quello che fa, è per la sua felicità.

Assegnare un diario del tempo passato in Internet. Dite a vostro figlio che vorreste vedere un resoconto del tempo passato in Rete ogni giorno. Se rifiuta l'idea o nel diario mente è molto probabile che ci si trovi di fronte alla negazione della dipendenza.

Stabilire regole ragionevoli. Non andate in collera se vostro figlio mostra i primi sintomi della dipendenza da Internet e non sequestrate il PC per punizione. Occorre, invece, collaborare per stabilire limiti chiari nell'utilizzo di Internet. Forse può andare bene un'ora ogni sera, più alcune ore nei fine settimana. Siate coerenti con quanto avete stabilito e ricordate che non state semplicemente tentando di controllare vostro figlio, ma state lavorando per liberarlo da una vera e propria dipendenza psicologica.

Mettere il computer dove si possa vedere. Trasferite il PC dalla sua camera a un posto dove possiate vederlo, come in cucina o in sala da pranzo. Naturalmente, non bisogna spiare il ragazzo, ma passate ogni tanto e inviate il messaggio che Internet non è una risorsa da usare di nascosto, bensì qualcosa da condividere con voi.

Incoraggiare altre attività. Nel momento in cui vostro figlio smette di dedicare troppo tempo a Internet, aiutatelo a cercare attività alternative. Parlate con lui di ciò che trovava divertente fare in Rete e reindirizzatelo nel mondo reale.

Sostenere non legittimare. Non assumete un ruolo di legittimazione con un figlio Internet-dipendente, nascondendo il problema o giustificandolo quando non va a scuola. Se vostro figlio si ribella ai vostri sforzi, lasciate che la tempesta iniziale si plachi: non deve essere facile avere la sensazione che gli state togliendo il suo unico mezzo di comunicazione. Lodatelo per qualunque sforzo stia facendo per collaborare.

La rete

La Rete o Internet è un sistema di connessione che consente di dialogare e scambiare dati con qualsiasi altro computer on-line, ovunque esso si trovi. Una tecnologia chiamata TCP/IP (Transmission Control Protocol - Internet Protocol) permette a tutti i sistemi connessi di interagire tra loro. Ogni "nodo" connesso permette a ognuno di noi di trasmettere informazioni, idee e opinioni e non solo di riceverle. Siamo tutti, contemporaneamente, spettatori e protagonisti: il sistema ci permette di essere davvero e totalmente interattivi.
Per chi vuole connettersi individualmente alla rete occorrono cinque cose:

1. Un computer.
2. Un software di comunicazione.
3. Una linea telefonica (non è necessaria una linea ad hoc).

4. Un modem, che collega il computer alla linea telefonica (o uno strumento equivalente).
5. L'acquisto da un provider del servizio di connessione a Internet.

Il sistema funziona su scala planetaria; non ha sede geografica, né confini.
La Rete offre una serie di servizi, che è opportuno conoscere, perché solo la conoscenza permetterà un uso adeguato di tali risorse. Esse sono:

- Esplorazione di Internet
- Posta elettronica
- Chat
- Blog
- Giochi on-line

Esplorare Internet

Cosa si intende per esplorazione?

Esplorare Internet significa accedere a un numero illimitato di informazioni e di risorse. La Rete è un ottimo modo per risparmiare tempo e fare cose che altrimenti non riusciremmo a inserire nei nostri programmi quotidiani già così intensi.
Grazie al WWW (abbreviazione di World Wide Web) si possono esplorare siti di notizie, musica, personaggi famosi, biblioteche e viaggi affascinanti.
È consigliabile che i genitori stabiliscano delle regole per tutta la famiglia e che discutano con i propri figli circa l'utilizzo di Internet.

1. Utilizzate Internet con i vostri figli e incoraggiateli a parlare con voi delle loro esperienze sul Web.
2. Insegnate ai vostri figli che le regole di buon comportamento sono da rispettare anche in Internet.
3. Spingete i vostri figli a fare domande e ricordate loro che non tutto ciò che trovano su Internet è vero.
4. Spiegate ai vostri figli che copiare il lavoro altrui (musica, film, videogiochi) è un furto.
5. Controllate il lavoro dei vostri figli utilizzando software specifici che lo permettano e che impediscano l'accesso ai siti che ritenete non adatti.

La posta elettronica

Cos'è la posta elettronica?

La posta elettronica è un mezzo per trasmettere dei messaggi in tempo reale da un computer a un altro utilizzando la rete Internet. Si scrive un messaggio sul proprio computer e lo si spedisce all'indirizzo e-mail del destinatario, stando comodamente seduti a casa o in ufficio.

Cosa bisogna sapere per farne un buon uso?

- I messaggi di posta elettronica non sono sicuri, non inserite informazioni riservate.
- La posta elettronica potrebbe essere manomessa, ricordatevi che un messaggio va sempre verificato prima di reputarlo vero.
- Non inviate grandi quantità di messaggi non richiesti: è sinonimo di invadenza e cattiva educazione.
- Non inviate "messaggi infuocati" (cioè quelli che vengono chiamati flames), anche se provocati.
- Non stupitevi se ricevete flames e non rispondete alle provocazioni.
- Quando rispondete, togliete tutto ciò che non serve. È considerata cattiva educazione rispondere includendo per intero il messaggio originale.

Principali Minacce della Posta Elettronica

Per la sua semplicità di utilizzo e diffusione capillare tra gli utenti di Internet, la posta elettronica ha rappresentato uno dei principali vettori per la diffusione di diverse tipologie di minacce ed di attacchi di tipo informatico.
Attraverso la posta elettronica, infatti, è possibile che siano veicolati virus o trojan.
I virus sfruttando soprattutto i file allegati nel messaggio possono:

- contenere programmi che si installano sulla nostra postazione PC per danneggiare il sistema

- controllare porzioni del sistema
- copiare informazioni private
- replicarsi e diffondersi su altre postazioni non protette.

Spesso infatti i virus che si propagano attraverso il servizio di posta elettronica, riescono prima ad infettare una singola casella di posta per poi risalire ad altri indirizzi di posta in essa contenuti e spedire verso di essi nuovi messaggi con il virus in allegato, con lo scopo di diffondere la minaccia informatica.

Propagazione virus attraverso allegati di posta

Per la semplicità con la quale è possibile creare ed inviare i messaggi di posta elettronica, questo servizio viene oggi utilizzato per diffondere messaggi pubblicitari non richiesti, che sono utilizzati per promuovere la vendita di prodotti stravaganti o illegali o per pubblicizzare siti web dai contenuti più disparati. Questi messaggi di posta elettronica indesiderati, finiscono per intasare le caselle di posta elettronica degli utenti creando per questo un disservizio che oggi è ben conosciuto con il nome di Spam.
Un altro esempio di uso malizioso della posta elettronica è rappresentato dal phishing, di cui parleremo in seguito.

La chat

Cos'è la chat?

La chat è una conversazione in tempo reale in Rete. Si tratta di messaggi inseriti via tastiera e visualizzati in successione sullo schermo (l'esempio tipico è l'IRC) e possono partecipare da due a migliaia di persone. In questo modo, si avrà la possibilità di entrare in contatto e discutere con tantissime persone, in qualsiasi posto del mondo esse si trovino.

Come si usa la chat?

La chat è un servizio aperto a tutti, previa registrazione di un nickname. Il nickname nasconde il vero nome agli altri partecipanti della chat. Se non sarà il chatter a comunicare la sua vera identità (nome, numero di telefono, indirizzo, datore di lavoro, ecc.), questa rimarrà anonima.
È consigliabile non rivelarsi in chat perché non si conosce l'interlocutore. Tuttavia nessuno resta del tutto anonimo in una chat. Ogni nickname è associato in modo univoco a un numero IP per tutto il tempo che l'utente resta in chat e questo numero permette all'amministratore di sistema di rintracciare la vera identità dell'utente in caso di necessità.
È possibile denunciare chi infrange le regole all'interno della chat.

Il blog

Cos'è un blog?

Un blog, abbreviazione di Web log, è un sito Web autogestito dove vengono pubblicate in tempo reale notizie, informazioni, opinioni o storie di ogni genere. Il blog è uno strumento di libera espressione, che tiene traccia (log) degli interventi dei partecipanti.
Un blog può essere personale, un diario on-line costantemente aggiornato che tutti possono leggere, oppure un spazio sul Web attorno al quale si aggregano esploratori che condividono degli interessi comuni. Aprire un blog è veramente facile: solitamente bisogna registrarsi al sito che offre questo servizio, e poi scrivere. La pubblicazione on-line è istantanea.

I giochi on-line

Cosa sono i giochi on-line?

I giochi sono on-line quando si trovano all'interno di un sito o che in qualche modo, possono essere a esso "collegati". In Rete esistono un'infinità di siti dedicati al mondo dei giochi dove si possono conoscere le ultime novità e le recensioni, provare le demo, giocare direttamente on-line e scaricare gratuitamente tantissimi giochi tra i più famosi.

Come si usano?

I giochi on-line si utilizzano come i giochi da consolle, solo che essendo attinti dalla Rete è fondamentale che venga letta l'informativa sul trattamento dei dati personali del sito o del servizio di gioco per ulteriori informazioni sull'utilizzo futuro dei dati personali. Se si ritiene che l'informativa sul trattamento dei dati personali non sia soddisfacente, non utilizzare i giochi del sito o del servizio in questione.

Cosa bisogna sapere?

- Limitare il tempo di permanenza on-line
- Stabilire un elenco di compagni di gioco
- Non fare proposte oscene
- Non usare un linguaggio offensivo

I Cyberbulli

Chi sono i cyberbulli?

Così come a scuola ci sono bulli che terrorizzano i compagni, anche in Internet ci sono personaggi molesti. Il cyberbullismo si può manifestare in chat prendendo di mira un utente, aggredendolo verbalmente, prendendolo in giro estromettendolo dalla lista di discussione. Altre forme di violenza psicologica sono la registrazione delle confidenze strappate nelle chat e poi pubblicate integralmente.

Suggerimenti per affrontare i cyberbulli

- Ignorarli.
- Evitare nomi provocatori che possano incoraggiare il comportamento del guastafeste.
- Non fornire informazioni personali.
- Comunicare agli amministratori del sito la scoperta di eventuali nuovi metodi per imbrogliare.

I Cyberpedofili

Chi è il cyberpedofilo?

Il pedofilo telematico è un individuo socialmente inserito, quasi sempre maschio, di età compresa tra i 20 e 30 anni, buon titolo di studio, nessun precedente, la maggior parte delle volte celibe. Spesso la modalità d'approccio on-line è omogenea, nel senso che vengono utilizzate tecniche comuni da pedofili diversi: iniziano subito a creare un clima di fiducia e amicizia fingendosi coetanei dei bambini, si assicurano più e più volte che il bambino sia solo o comunque che non sia controllato da persone adulte.

Poi, gradualmente introducono argomenti sessuali, inviando a volte fotografie pedopornografiche per convincere il minore che tali comportamenti sono normali e che gli altri bambini sono sessualmente attivi. In seguito, accendono la curiosità sessuale del bambino, prescrivendogli compiti come compiere atti sessuali. L'approccio continua poi via telefono o via e-mail. Infine, si tenta di convincere il bambino a un incontro reale, faccia a faccia.

Suggerimenti da dare ai propri figli su come affrontare i cyberpedofili

Quando si è su Internet non dare mai a nessuno l'indirizzo di casa, il numero di telefono il nome della scuola.

Non prendere appuntamenti con persone conosciute su Internet, anche se dicono di essere coetanei, senza prima avere il permesso dei genitori.

Se si frequenta una chat assicurarsi che nessuno dica qualcosa di strano o preoccupante (per esempio discorsi sul sesso).

Non rispondere mai a e-mail o messaggi fastidiosi o allusivi, specie se di argomento sessuale e se capita di notare fotografie di persone adulte o bambini nudi parlarne sempre.

Ricordarsi 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.

La sicurezza di Internet

Per permettere agli utenti di sfruttare le infinite potenzialità di Internet come tecnologia di comunicazione, la Sicurezza informatica si presenta come un requisito fondamentale. Questo è necessario infatti per garantire la disponibilità delle informazioni, l'accesso sicuro alle stesse e la distribuzione dei servizi di Internet.

La Sicurezza in Internet si compone di un insieme di strumenti di protezione quali i Firewall per il controllo delle informazioni che transitano nella rete, gli Antivirus, gli IDS (Intrusion Detection System), di Servizi di Sicurezza, come ad esempio gli aggiornamenti delle applicazioni, e soprattutto di regole comportamentali, non scritte ma dettate soprattutto dal buon senso e dalla conoscenza, che determinano un vero e proprio Codice da seguire per navigare più sicuri. L'insieme di questi elementi contribuiscono a fornire tutte le misure necessarie per contrastare i rischi che si presentano nella rete e che permettono all'utente una navigazione più sicura.

Rischi/Minacce in Internet

Principali Minacce sul WEB

L'accesso a siti con contenuti illegali o pornografici diviene un mezzo per l'immissione nella rete di **Worm** e **Virus**: sfruttando le caratteristiche dei programmi software dei browser, i **Worm** che infettano un computer riescono ad indurre il sistema a replicare il worm ed a diffonderlo nella rete in maniera incontrollabile.

Similmente, i **Virus** che riescono ad inserirsi in un sistema possono esporlo all'accesso da parte di utenti non autorizzati oppure possono utilizzarlo come strumento per l'esecuzione di operazioni illegali o ancora possono danneggiarne il funzionamento.

Per rendere la navigazione di un sito più veloce o semplicemente per personalizzare i contenuti a seconda degli utenti, vengono spesso utilizzati i cosiddetti **Cookie**. I cookie sono piccole serie di informazioni memorizzate dai browser e comunicate su richiesta ai siti web, come ad esempio il nome dell'utente oppure dei contatori del numero di pagine visitate. In alcuni casi, i cookie sono utilizzati in maniera impropria e possono raccogliere informazioni sui comportamenti e sulle preferenze degli utenti, creando dei profili senza che essi abbiano manifestato il loro consenso, commettendo una violazione della privacy. Inoltre, possono avvenire casi di "furto" dei cookie, quando alcune pagine web richiedono informazioni di cookie che non appartengono al loro sito, ma che contengono informazioni riservate a pagine di altri siti.

Un'altra forma di violazione della privacy può avvenire se si è subito l'attacco di uno **Spyware**. Gli spyware sono dei piccoli programmi che restano in esecuzione nel sistema all'insaputa dell'utente e senza manifestare in alcun modo la loro presenza. Il loro scopo, da cui il nome, è quello di spiare il comportamento degli utenti e, se possibile, rubare delle informazioni che possono consentire l'accesso a zone riservate (esempio nome utente, password). Gli spyware generalmente richiedono l'intervento dell'utente per essere installati e pertanto spesso sono camuffati da programmi leciti e spacciati come innocui.

Molto simili agli spyware sono gli **Adware**: dei programmi trasparenti all'utente che hanno lo scopo di mostrare automaticamente oppure prelevare in maniera indesiderata del materiale pubblicitario, magari da mostrare in piccole finestrelle (i cosiddetti popup). Come gli spyware, gli adware si installano nel computer, è l'utente stesso che inconsapevolmente li installa, nascondendosi in programmi che offrono delle funzioni accattivanti. Non sono molto pericolosi, ma possono essere fastidiosi e a volte possono consumare delle risorse del sistema e deteriorarne le prestazioni.

Uno dei fenomeni che tocca in maniera diretta gli utenti della navigazione del Web è rappresentato dal **Phishing**, che consiste nell'imitare nei minimi dettagli delle pagine web che consentono l'accesso a servizi limitati esclusivamente ad utenti autorizzati, allo scopo di rubare delle credenziali di accesso. Il Phishing riesce ad ottenere queste informazioni personali attraverso l'utilizzo di messaggi di posta elettronica fasulli, creati appositamente per sembrare autentici. Ritenendo queste e-mail attendibili, gli utenti troppo spesso

rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali.

Il fenomeno del **Pharming** consiste nel far comparire sul browser di un utente una pagina web diversa da quella richiesta.

Virus e Worm

Virus e Worm rappresentano le due forme più conosciute di malware.

La caratteristica principale di queste due minacce è rappresentata dalla loro capacità di autoreplicarsi analogamente a quanto avviene per i virus biologici, sfruttando le risorse del sistema ospite (il computer dell'utente), con l'obiettivo di infettare altri sistemi.

La differenza tra questi due tipi di malware è rappresentata, principalmente dalla diversa modalità di replicazione e quindi di diffusione. I Virus sono programmi che devono essere prima eseguiti per potersi replicare e quindi infettare il computer che li ospita. Possono essere contenuti all'interno di file, applicazioni o essere nascosti all'interno di codice che viene eseguito automaticamente dal sistema (computer) che li ospita all'apertura di certi tipi di file. Senza questi file o applicazioni i virus non potrebbero replicarsi e attivarsi, provocando un danno nel sistema che lo ha attivato.

Un utente può ricevere un Virus sotto forma di file infetto attraverso gli allegati di posta elettronica, effettuando il download di un file o applicazione da Internet oppure per mezzo di un supporto di memoria esterno (floppy. Cd-rom, DVD, supporti di memoria USB) che funge da vettore per questo malware.

I worm, sono simili ai virus ma agiscono in modo indipendente, ossia non hanno bisogno di utilizzare un file per diffondersi, ma essi stessi rappresentano la minaccia in grado da sola di recare danno al sistema e replicano quindi se stessi da sistema a sistema.

Normalmente, i worm si diffondono sfruttando le vulnerabilità del sistema bersaglio, come ad esempio quelle presenti nel client di posta elettronica, mentre per i virus, tipicamente, la diffusione avviene semplicemente con l'esecuzione di applicazioni.

I virus informatici possono considerarsi, attualmente, in via d'estinzione a causa del sempre minore utilizzo del loro vettore principale d'infezione: i dischi removibili o floppy.

I danni che tali programmi possono arrecare sono i più disparati e riguardano soprattutto la disponibilità e l'integrità delle informazioni memorizzate sul computer infettato o la disponibilità ad utilizzare alcuni programmi installati al suo interno che vengono di conseguenza colpiti dal virus.

I worm, d'altra parte, diffondendosi grazie alla rete Internet, rappresentano oggi una delle principali minacce. Tipicamente un worm non è un malware fine a se stesso e spesso quindi non agisce da solo: mediante il worm infatti sono veicolati altri tipi di malware, come ad esempio gli spyware o le backdoor.

Altro malware: Spyware, Trojan e Backdoor

Spyware

Lo spyware è un software maligno in grado di spiare il comportamento dell'utente e riferirne i risultati anche verso sistemi remoti. I programmi di Spyware a differenza dei virus non si diffondono su altri computer, ma possono essere scaricati più o meno inconsapevolmente dall'utente durante la navigazione di siti Internet. Al momento della loro attivazione gli spyware sono in grado di registrare alcune attività dell'utente e comunicare tali informazioni verso terzi.

Fanno parte di questa categoria:

- **adware** - programmi specializzati nel reperimento di informazione di carattere commerciale finalizzate alla generazione di pubblicità mirata
- **keylogger** - programmi in grado d'intercettare e registrare l'input da tastiera, ossia qualsiasi sequenza di tasti premuti dall'utente e quindi catturare password, numeri di carte di credito, etc.

Trojan

L'etimologia della definizione trojan si rifà al concetto di cavallo di troia: nel contesto informatico un trojan è un programma con funzionalità note di apparente utilità per l'utente, che nasconde al suo interno funzionalità nascoste solitamente dannose. Tale codice nascosto viene attivato inconsapevolmente dall'utente ogni qual volta installa ed esegue tale programma.

Il Trojan presenta funzionalità spesso analoghe a quelle dello spyware o delle backdoor. La diffusione dei Trojan non avviene in modo automatico come quella dei virus o dei worm, ma necessita dell'intervento dell'utente che inconsapevolmente prende dalla rete tale programma e lo esegue sul proprio computer.

Backdoor

Le backdoor rappresentano una forma di malware attraverso il quale è possibile per un utente malintenzionato, prendere il controllo del computer di un altro utente sfruttando una connessione Internet. Le backdoor sono paragonabili a delle "porte di servizio" che consentono, a chi le installa sul computer vittima, di avere una via d'accesso per il controllo remoto del sistema stesso.

Questo tipo di minaccia può nascondersi sotto forma di software apparentemente legittimo al fine di essere eseguito direttamente dall'utente o può essere veicolato attraverso altre forme di malware quali virus, worm o trojan.

Attraverso una Backdoor un utente remoto può controllare il computer infetto, eseguire programmi, accedere e modificare i file personali, o sfruttare tale vulnerabilità per utilizzare tale sistema per diffondere altri attacchi informatici.

Principali Minacce dell'Instant Messaging

L'Instant Messaging permette di contattare e stabilire delle relazioni con persone sconosciute. Analogamente a quanto avviene nella vita reale è importante valutare con estrema attenzione l'interlocutore ed evitare, quando possibile, di parlare apertamente dei propri dati personali, dell'indirizzo della propria abitazione o di altre informazioni delicate.Anche se quanto detto può sembrare banale, spesso la virtualità dei rapporti che si instaurano in rete fa cadere le normali "barriere", dettate dal buon senso, che ognuno di noi applica nei rapporti con le altre persone.

Dal punto di vista tecnologico, molti programmi di IM sono in grado di fornire servizi più evoluti rispetto alla sola chat: ad esempio sono in grado di trasferire file oppure di realizzare delle vere e proprie telefonate (anche con video) fra i partecipanti. Proprio questi servizi aggiuntivi possono essere sfruttati come veicoli per trasmettere virus o cavalli di Troia. Inoltre, un'errata configurazione dei servizi aggiuntivi di condivisione dei file può portare all'esposizione involontaria di documenti e informazioni dal contenuto riservato.

I rischi del servizio di IM

Di seguito vengono elencati alcuni dei **principali rischi dell'IM**:

- le comunicazioni in un sistema di IM non vengono, solitamente, protette con la crittografia e pertanto possono essere lette da terze parti;
- un utente non autorizzato potrebbe essere in grado di reperire le informazioni di accesso al sevizio di IM di un altro utente (*i.e.*: username e password) e connettersi in modo illecito sotto falsa identità. Tale fenomeno è definito come *Account Hijacking*;
- vulnerabilità proprie dell'applicazione di IM potrebbero essere sfruttate da utenti estranei per compromettere il sistema dell'utente;

- possibilità di infettare i computer degli utenti che utilizzano una applicazione di IM diffondendo dei malware (IM worm) sfruttando funzionalità degli IM quali il trasferimento file. In questo senso i pericoli sono paragonabili a quelli relativi ai file allegati che vengono scambiati attraverso il sevizio di posta elettronica;
- i canali IRC possono essere utilizzati da alcuni worm per comunicare con l'attacker oppure anche per lanciare attacchi di tipo DDoS.

Principali Minacce del Peer to Peer

La grande diffusione dei software peer-to-peer per il file-sharing è sfruttata dagli utenti maliziosi per introdurre e diffondere nella rete nuovi virus: introducendo il nuovo virus in un file molto richiesto, è possibile ottenere una diffusione notevole in pochissimo tempo.

Anche la diffusione di spyware e adware sfrutta i canali del peer-to-peer: sono molti gli esempi di programmi per il file-sharing che contengono al loro interno spyware per studiare le preferenze degli utenti o adware per pubblicizzare particolari siti oppure prodotti di mercato.

Un attacco particolare alle reti p2p (peer-to-peer) per il file-sharing è chiamato **poisoning**: tale attacco consiste nel diffondere nella rete un file spacciandolo per un altro, in maniera da ingannare chi ne viene in contatto. Poiché spesso il file-sharing si basa sulla quantità di documenti condivisi nella rete, il poisoning può essere sfruttato per migliorare le prestazioni, a scapito di tutti gli altri utenti della comunità.

Il fenomeno del Pharming

La principale minaccia che sfrutta le vulnerabilità della risoluzione dei nomi di dominio è denominata **Pharming**.
Il Pharming ha le medesime finalità del phishing: il furto d'identità o comunque di informazioni sensibili.

Rispetto al phishing, il pharming è estremamente più insidioso, in quanto più difficile da rilevare: sovvertendo il funzionamento del DNS, in qualche punto della catena di processi volti a portare a termine la risoluzione dei nomi, è possibile per un attaccante far pervenire all'utente un indirizzo IP differente da quello relativo al nome di dominio richiesto.
In particolare, comunicando un indirizzo IP facente capo ad un sistema sotto il controllo dell'attaccante, quest'ultimo può, riproducendo le funzionalità del sistema legittimo, trarre in inganno l'utente e carpire, ad esempio, password o numeri di carta di credito.

Il fenomeno dello SPAM

Lo Spam rappresenta oggi un fenomeno ampiamente diffuso tra gli utilizzatori del servizio di posta elettronica e se pur non presenta spesso la stessa pericolosità di altri Malware, come virus o worm, è sicuramente diventato il principale elemento di "disturbo quotidiano" che un utente si trova ad affrontare utilizzando il servizio di posta elettronica.

Come Spam vengono definiti tutti quei dei messaggi di Posta Elettronica recapitati nella nostra casella di posta che non sono stati direttamente "sollecitati", e che potremmo definire anche come insieme di posta indesiderata.

Lo Spam nasce e si sviluppa come un vero e proprio fenomeno economico, rappresentando un meccanismo di informazione-pubblicità molto conveniente ed in grado di raggiungere con un "clic" un quantità considerevole di possibili clienti. Questa tecnica viene definita come **mass-mailing**, ossia la possibilità di inviare messaggi di posta elettronica "in massa" utilizzando degli appositi software di spam e sfruttando dei veri e propri "elenchi" di indirizzi, al costo della durata della connessione!

Gli artefici di questa minaccia vengono definiti come **Spammer** e possono utilizzare diverse tecniche per riuscire nel loro intento: far arrivare a più destinazioni possibili i loro messaggi di posta elettronica, con lo

scopo che quanto proposto nelle loro “offerte” venga accolto dalla più alta percentuale possibile così da poter accrescere il proprio conto in banca.

Tra le diverse tecniche utilizzate da uno spammer possiamo elencare le seguenti:

- **Acquisto di elenchi**: tecnica utilizzata da uno spammer per reperire indirizzi di posta elettronica acquistando degli elenchi di indirizzi rubati
- **Attacchi dizionario:** fissato un dominio di posta esempio ..@domino.com uno spammer può inserire tutte le varianti di indirizzi più comuni, mario.rossi@dominio.com, m.bianchi@dominio.com, inviando migliaia di messaggi sperando di recapitare più messaggi possibili
- **Ricerca di indirizzi di posta elettronica**: attraverso la semplice navigazione nei siti Web dove sono pubblicati i “contatti” della società che detiene il sito
- **Spoofing**: tecnica utilizzata per nascondere il proprio indirizzo mittente, uno spammer manipolando il protocollo SMTP utilizzato per l'invio della posta è in grado di nascondere la propria identità (da dove proviene il messaggio di spam) modificando il campo Da:
- **Proxy spam**: rappresenta un postazione su Internet sia esso un apposito Server di posta “illecito” o un Pc infettato da un Troiano, che vengono utilizzati per inviare Spam. Queste postazioni una volta individuate da un Provider Internet, vengono inserite in una Black List bloccando la diffusione del loro traffico. A questo punto ad uno Spammer non resta che procurarsene un altro
- **Ingegneria sociale**: alla base di molti fenomeni che riguardano le minacce su Internet si trova il processo di Ingegneria sociale, processo che sfrutta la psicologia delle persone, facendo leva su elementi di bisogno, i desideri e le vulnerabilità intellettuali. Uno spammer può avversi di questo per invogliare un utente ad aprire i propri messaggi
- **Web Bug**: Meccanismo utilizzato dagli spammer per verificare quali utenti hanno aperto i messaggi di spam, e quindi rappresentano un indirizzo attivo. Tale tecnica si basa sull'inserimento nel messaggio di spam di una porzione di codice HTML o GIF che all'apertura del messaggio serve per stabilire una connessione con il server di Posta e comunica così l'indirizzo è attivo

Lo spam continua a diffondersi diventando un vero e proprio fenomeno sociale ed oltre ad essere un meccanismo per la diffusione di messaggi pubblicitari a contenuto pornografico, sponsorizzazioni di medicine a sfondo sessuale, promozioni finanziarie, pozioni magiche per il dimagrimento, rappresenta anche un vettore per truffe e raggiri di diversa natura che si sono evoluti fino a trasformarsi in altre forme di minacce quali ad esempio il **phishing**.

Lo SPAM è un fenomeno che può essere limitato, circoscritto ma per farlo occorre comprendere come questo si sviluppa, imparare a riconoscerlo e cambiare le nostre abitudini nell'utilizzare il nostro indirizzo di posta elettronica.

Il fenomeno del Phishing

Il Phishing può essere considerato una forma di SPAM e rappresenta oggi una delle nuove e più diffuse minacce provenenti da Internet.

I pericoli legati al Phishing sono rappresentati dal furto di identità e reperimento di informazioni riservate (come ad esempio numeri di carte di credito o password di accesso a servizi bancari) che potrebbero essere utilizzate da utenti non legittimi.

Il Phishing utilizza il servizio di posta elettronica come vettore per inviare agli utenti dei messaggi email di tipo ingannevole.

I messaggi di phishing provengono generalmente da indirizzi mittente falsificati creati utilizzando la tecnica dello spoofing. Questi indirizzi fanno riferimento a siti Web ed organizzazioni apparentemente “legittime”, ad esempio la nostra banca ma in realtà contengono dei messaggi contraffatti attraverso i quali viene effettuata all'utente una richiesta diretta di informazioni personali o viene invitato l'utente a visitare dei siti contraffatti.

Il Phishing sfrutta la costruzione di questi messaggi ingannevoli, legati spesso alle attività on-line di maggiore criticità per gli utenti come ad esempio i servizi bancari o servizi relativi alla gestione delle carte di credito. Il contenuto di questi messaggi prospetta generalmente un malfunzionamento del servizio a cui si riferisce, prospettando anche un possibile rischio per i dati dell'utente se questi non agisce secondo quanto indicato. Tale approccio, mirato ad ingannare l'utente sfruttando la sua sensibilità verso temi di interesse è tipico dell'ingegneria sociale utilizzata dal phishing.

Il messaggio di Phishing può agire o formulando una richiesta diretta per l'utente che viene invitato a fornire nuovamente - in risposta alla mail - i propri dati o informazioni riservate, le quali però saranno inconsapevolmente indirizzate all'organizzazione che ha creato il messaggio, oppure sollecitando l'utente a visitare un sito contraffatto dove gli verrà richiesto l'invio dei dati personali, che potrebbero in entrambi i casi essere utilizzati per scopi illeciti violando la privacy.

Esempi di messaggi di Phishing:

Di seguito viene illustrato un esempio di Phishing: un messaggio, avente come mittente un noto gruppo bancario, invita l'utente destinatario ad avviare una procedura di conferma dei propri dati “Cliente”, reindirizzandolo verso un sito web contraffatto.
Il messaggio posto è realizzato in forma pressoché anonima, ed è stato riutilizzato dagli autori dello stesso, definiti come **phisher,** personalizzandolo con il logo e la dicitura mittente e firma dei più famosi gruppi bancari nazionali. Il messaggio in realtà rimanda ad un sito web contraffatto attraverso il quale potrebbe essere avviata la procedura di reperimento dei dati o informazioni riservate, ingannando l'utente che vi accede, cliccando sul link indicato.
Il link stesso presente nel messaggio, se pur contenente il nome del gruppo bancario noto, in realtà nasconde un indirizzo contraffatto.

Sistemi di filtraggio e di classificazione

Nessun software di filtraggio potrà mai sostituire la sorveglianza dei genitori sui loro figli quando questi sono collegati on-line, visto che al momento risulta particolarmente difficile proteggersi dai siti che propagano la violenza. Tuttavia, stando ad una serie di recenti indagini effettuate da "Test Achats" con il contributo finanziario del Piano d'azione comunitario un efficace sistema di filtraggio è probabilmente il modo migliore per bloccare perlomeno la maggior parte dei siti a carattere pornografico.

Molti dei dispositivi per il filtraggio sono prodotti negli Stati Uniti. Ciò significa che i criteri di filtraggio possono essere fortemente influenzati dai valori statunitensi, ad esempio un estremo rigore nei confronti della nudità, ma una maggiore permissività nei riguardi di armi e violenza. Molti di questi prodotti funzionano essenzialmente in inglese. Tra i vari sistemi di filtraggio vi possono essere notevoli differenze di prezzo, ma non è detto che i più cari siano anche i migliori.

Modalità di funzionamento dei sistemi di filtraggio

Liste nere: Viene stilata una lista di siti da evitare (quelli contenenti ad esempio materiale scabroso, violento o razzista), di modo che, se il minore cerca di collegarsi a uno di questi siti, l'accesso viene bloccato. Alcuni programmi utilizzano invece liste di termini "proibiti": ogni volta che all'interno di un link o nell'ambito di un determinato sito appare uno di questi termini, l'accesso viene bloccato. Il problema delle "liste nere" è che necessitano di aggiornamenti continui.

Filtraggio in tempo reale: Il filtro controlla le parole e le immagini mano a mano che vengono caricate e blocca le pagine con i testi o le immagini indesiderate prima che queste appaiano. Il problema è che la pagina può essere vista parzialmente prima che il filtro venga innescato dal testo o dalle immagini in questione. Inoltre un tale sistema può rallentare l'accesso a tutti i siti della rete.

Etichettatura/classificazione dei siti: I proprietari dei siti appongono volontariamente alle proprie pagine web un'etichetta che indica la presenza in esse di determinate categorie di contenuti (ad esempio violenza, nudo, gioco d'azzardo, contenuti pornografici, ecc.). La concezione delle etichette e la definizione delle categorie è di competenza dell'ICRA. Il filtro "legge" l'etichetta e decide se permettere o meno l'accesso ai

minori, a seconda delle scelte effettuate a monte dai genitori. Il problema di un tale sistema è che si basa su una classificazione volontaria da parte dei fornitori di contenuti e che sinora ben pochi siti sono stati classificati.

Aree protette (walled gardens): Vengono preparati elenchi di siti Internet adatti all'infanzia e solo ad essi è consentito l'accesso dei bambini. Si tratta del metodo più sicuro di proteggere i minori.

Browser per bambini

Concettualmente destinati al "parental control" (tutela da parte dei genitori) i browser per bambini sono uno strumento utilizzabile nella relazione formativa, per una serie di ragioni.
La prima, e la più evidente e immediata, è la ***tutela dei minori***: questi ambienti possono infatti sostituire almeno in parte soluzioni più sofisticate e impegnative, che prevedono l'impiego di dispositivi hardware e software complessi, mantenendo l'obiettivo di consentire ai bambini una *navigazione sicura.*
Il meccanismo su cui si basano è infatti la ***supervisione adulta***, che applicano con modalità leggermente diverse da ambiente ad ambiente. Vediamo qualche esempio.

Il programma più noto è **Chibrow™**. The Children's Browser è un software a pagamento, che dà la possibilità di navigare esclusivamente nel bacino di siti definito dal genitore o dall'insegnante. Insieme al programma è fornito un insieme di siti americani i cui contenuti sono giudicati utilizzabili dai bambini da parte dei produttori. Tale lista è protetta da una password, mediante la quale si può accedere all'insieme predefinito e apportarvi modifiche e integrazioni.
Kiddonet™ è invece gratuito: si scarica da http://www.kiddonet.com/knSource/knBrowser.htm
All'inizio esso consente l'accesso solo al progetto omonimo. Starà all'adulto inserire i siti da far navigare al bambino. Iscrivendosi al suo sito (www.kiddonet.com) si possono inoltre usare un sistema di posta elettronica a sua volta protetto e una simpatica agenda e anche costruire una piccola e divertente pagina personale. Anche in questo ultimo caso la tutela è esercitata con grande attenzione: viene esplicitamente sconsigliato, per esempio, di utilizzare foto di bambini.
Kid's Internet World Explorer (Kiwe™) funziona invece in modo analogo a Chibrow e propone anche una versione italiana, così come italiane sono le risorse di rete selezionate e proposte. Anche in questo caso il supervisore può intervenire a ampliare o ridurre i siti raggiungibili. Il programma si scarica in versione di prova (http://www.kiwe.it/maini.htm) e può poi essere registrato.

In tutti i casi i browser per bambini interdicono un eventuale collegamento esterno da uno dei siti consentiti, i quali sono invece esplorabili in tutti la loro profondità. Chi intendesse utilizzarli deve quindi far precedere la costruzione delle liste dei siti utilizzabili dai bambini da una attenta esplorazione delle varie sezioni e pagine.

Aspetti cognitivi e potenzialità didattiche della navigazione

La tutela non esaurisce le motivazioni all'uso dei browser per bambini. Un altro aspetto importante è infatti la ***semplificazione dell'interfaccia***, poiché essi offrono la medesima logica operativa di fondo e le stesse funzioni di base di un browser "per adulti", impiegando "soltanto" una grafica accattivante e soprattutto icone più grandi e in numero ridotto. Ciò è essenziale per evitare atteggiamenti antipedagogici, che forzino l'anticipazione di situazioni e prestazioni troppo complesse.

Questa riflessione ne porta dietro un'altra: *a scuola, e in ogni relazione formativa che in essa ha luogo, ivi compresa quella con persone affette da disabilità cognitive. vanno sviluppate in modo precoce non già le pratiche tecnologiche, ma le competenze di elaborazione comunicativa*, dal funzionamento logico di un sito e delle pagine web in genere, alla vera e propria "*iperlettura*". Ogni "Lettore-Navigatore" abile deve infatti via via perfezionare in modo consapevole una vera e propria strategia di comprensione, di definizione e di verifica della propria navigazione, intesa appunto come *percorso di lettura ipertestuale*, strategia basata costantemente sulle sue capacità associative e deduttive. Egli ha infatti costantemente in carico la ricostruzione dell'insieme, ossia dei sensi, dei significati e della pregnanza dei collegamenti. Questo processo, che non si realizza solo attraverso informazioni di tipo testuale, ma anche con le immagini e con le relazioni tra di esse, può aver inizio in modo del tutto efficace nella scuola materna e elementare: per

affrontare in modo propedeutico le prime tappe di un cammino cognitivo così complesso va quindi colto il vantaggio fornito da ambienti con un'architettura pensata per i bambini.

Ultima considerazione. Usare un browser "protetto" *non significa necessariamente solo inibire o, peggio, proibire*. Nel definire un insieme di siti utilizzabili, l'adulto si renderà infatti *garante* non solo dell'assenza di contenuti che possano turbare il bambino, ma anche del fatto che i contenuti medesimi lo possano davvero interessare, *acquisiscano senso e significato rispetto all'insieme delle sue attività*, *magari valorizzandole per quantità e qualità*. E pertanto, se i genitori di una famiglia che ama gli animali potranno far navigare i loro figli su siti dedicati a questo tema, un insegnante che abbia deciso di trattare a scuola l'argomento fiabe e filastrocche potrà fare altrettanto sulle relative pagine WEB da lui trovate, selezionate e proposte agli allievi, con l'obiettivo di aggiungere valore a un progetto didattico, integrando le risorse culturali disponibili in classe e nella biblioteca della scuola con quelle a distanza, sulla rete.

Riflettiamo sul fatto che definire un bacino di siti "consentiti" può in realtà essere per gli adulti occasione non già di censura. ma piuttosto di ricerca "mirata" e di costruzione di un progetto di consultazione di informazioni secondo un senso e uno scopo utili sul piano formativo ai bambini per qualcosa di più della navigazione in sé e per sé.
Per fare ciò possono essere utili anche i *motori di ricerca e i portali per bambini*, dei quali elenco qualche semplice esempio, avvertendo il lettore che essi sono in realtà assai più numerosi di quel che si possa credere ed inoltre in crescita ed evoluzione continue.

Motori e portali per bambini

Baol, il mago del web, è in lingua italiana e propone ricerche sia per parole-chiave sia per categorie. È stato concepito "come progetto di studio universitario e realizzato nell'ambito delle attività speciali per la didattica sviluppate nel laboratorio multimediale Scians di Matera, nella cui sede il motore è stato prodotto".
Yahooligans è invece in lingua inglese e propone una struttura e un'interfaccia più vicine di quelle dell'esempio precedente a un portale informativo "adulto". Si presenta come "The Web Guide for Kids" ed è uno dei primi esempi di strumenti di ricerca dedicato ai bambini.
Bambini.it si propone come un portale vero e proprio e può essere utilizzato come punto di partenza da chi intendesse andare oltre questo breve elenco: una delle voci della sua pagina iniziale è dedicata proprio a "Indici e motori di ricerca" per bambini.

In rete senza browser

Un cenno particolare merita ancora il progetto *International Children's Digital Library*, che sta realizzando una biblioteca internazionale rivolta ai bambini e fatta di libri in formato digitale leggibili attraverso Internet. Sono interessanti i contenuti, ma anche l'interfaccia, che consente di usare le risorse a distanza senza dover passare attraverso un browser, cosa che tutela in modo molto sicuro l'utente. Al primo accesso dovremo infatti scaricare e installare un'applicazione apposita, che costituirà poi stabilmente un ambiente dedicato in modo esclusivo alla ricerca in biblioteca (per categorie e per localizzazione geografica) e alla lettura dei libri. L'attività è realizzabile a scuola o a casa in presenza di connessioni a banda larga e di abbonamenti a forfait, perché presuppone la costante connessione con la rete.

A SCUOLA, MA NON SOLO...

I possibili mezzi per affrontare i rischi collegati all'uso delle tecnologie on-line devono coinvolgere una gran varietà d'attori a livelli differenti, quali la pubblica amministrazione, le organizzazioni per la tutela dei minori, l'industria (fornitori di servizi e di contenuti, produttori di software), le istituzioni educative, le scuole, i genitori e la Commissione Europea.

Non ha senso porre attenzione al problema solo a scuola. L'uso di Internet nelle famiglie è molto alto. Alcune norme di base, come non collocare il collegamento ad Internet in un luogo nascosto della casa o non lasciare completamente soli i ragazzini quando navigano, sono norme di buon senso anche molto efficaci. Esistono vari sistemi di controllo dei contenuti su Internet per la protezione dei bambini e in generale dei minori: *parental control* (controllo dei genitori), filtro famiglia, sistemi di etichettatura, *walled garden (*il "giardino recintato dove si naviga su un Internet limitatamente ad alcuni siti) entreranno sempre di più nell'uso comune delle famiglie.

E' utile, sia per la scuola che per la famiglia, conoscere anche istituzioni che svolgono attività correlate a questi temi.

TELEFONOAZZURRO E HOT114

E' attiva in Italia una hotline (linea di segnalazione) in servizio 24 ore su 24, a cui segnalare, anche in forma anonima, materiale pedopornografico, contenuti razzisti e discriminatori, siti violenti o che istigano alla violenza e tutto ciò che può essere potenzialmente pericoloso per bambini e adolescenti. Si chiama Hot114 ed è operativa sia attraverso la compilazione di una scheda di segnalazione disponibile sul sito http://www.hot114.it, sia chiamando il numero gratuito 114 da telefonia fissa, oppure il numero di Telefono Azzurro 19696. Ad accogliere le richieste d'intervento degli utenti ci sono operatori esperti, i quali provvedono immediatamente ad inoltrare la segnalazione alle Istituzioni competenti, tra cui la Polizia Postale, sempre nel rispetto dell'anonimato, per chi lo desidera. Vi si trovano molto interessanti sono i consigli per genitori, docenti e ragazzi.

http://www.telefonoazzurro.it

http://www.hot114.it

http://www.inhope.it

http://www.saferinternet.org/ww/en/pub/insafe/index.htm

MINISTERO DELLE COMUNICAZIONI

Il Ministero delle Comunicazioni ha inaugurato un rapporto di collaborazione con Save the Children Italia, che attraverso una convenzione è stata identificata quale partner privilegiato per promuovere attività e elaborare proposte volte alla tutela dei diritti dell'infanzia, sotto il particolare profilo del rapporto del minore e le tecnologie della comunicazione, sia tradizionali che innovative.

http://www.ti6connesso.it
http://www.savethechildren.org/
http://www.savethechildren.it/2003/index.asp

POLIZIA DI STATO

http://www.poliziadistato.it

AZIENDE

Con il progetto "Sicurezza on-line" Microsoft, con il contributo dell'associazione nazionale dei dirigenti e delle professionalità della scuola, intende mettere a disposizione dei docenti un percorso di formazione su quattro temi:

- Sicurezza del computer
- Protezione dei dati personali
- Sicurezza dei ragazzi
- Comportamenti on-line

I dettagli sul progetto: ***http://www.apprendereinrete.it***

RIFERIMENTI NORMATIVI - LA PROTEZIONE DEI MINORI DA CONTENUTI PERICOLOSI

http://www.giustizia.it/casazione/leggi/l38_06.html#TESTO
http://www.comunicazioni.it/it/index.php?IdPag=1177

Internet possiede un formidabile potenziale informativo di cui è difficile fare a meno, la possibilità di reperire qualsiasi tipo di informazione, indipendentemente dal contesto socio-culturale a cui si appartiene costituisce una straordinaria opportunità sociale e didattica. Per evitare però che i minori accedano, anche involontariamente, a materiali non idonei a soggetti in eta' evolutiva, che commettano reati o che si isolino a causa di un eccessivo utilizzo di internet è necessario diffondere la cultura dell'uso legale e consapevole della rete.

Tratto da: http://www.osservatoriotecnologico.it