con la collaborazione di

Google™

SICURAMENTE ONLINE

PROTEGGI LA TUA **FAMIGLIA** ONLINE

PENSI CHE IL **PHISHING**

SIA SOLO UN TIPO DI PESCA?

PENSI CHE I **COOKIE**

SIANO SOLO BISCOTTI?

PENSI CHE UN **VIRUS**

SIA SOLO UN RAFFREDDORE?

PROTEGGI LA TUA **FAMIGLIA** ONLINE

Internet è ormai parte integrante della vita dei ragazzi. La rete offre loro tante opportunità, permette di accrescere le loro conoscenze, di condividere e coltivare passioni e interessi, mantenere i contatti con gli amici vicini e lontani, conoscerne di nuovi, fare nuove esperienze, sperimentare nuove realtà.
Accanto alle opportunità si celano, però, anche dei rischi, come la possibilità che i ragazzi siano esposti a contenuti non appropriati, o che diventino vittime di cyberbullismo, frodi o adescamento, o che si isolino dal mondo reale, rinchiudendosi in quello virtuale.
Tali rischi, che possono essere più o meno concreti, possono essere arginati grazie alla supervisione di un adulto di riferimento.
Di seguito sono elencati i diversi rischi ai quali i ragazzi possono essere esposti e le relative precauzioni che gli adulti possono prendere.

1 Contenuti inappropriati: quali rischi?

Durante la navigazione in rete i ragazzi possono essere esposti a contenuti non adeguati alla loro fascia d'età, come siti che incitano all'**anoressia (pro-ana)** o alla **bulimia (pro-mia)** o al **consumo di droghe**, o siti con **contenuti violenti e/o a sfondo sessuale**. Per quanto riguarda questi ultimi, può accadere che i ragazzi effettuino una ricerca dettata da una curiosità che può definirsi fisiologica in questa fase dello sviluppo. Il rischio è, però, che i ragazzi si imbattano in materiale pornografico o pedopornografico, che fornisce una rappresentazione distorta della realtà.
Partendo dal presupposto che i ragazzi hanno il **diritto** di ricevere informazioni che sono in grado di arricchirli, è altrettanto loro diritto non imbattersi in contenuti che possano metterli in crisi per gradevolezza o eccesso di ansia, poiché il ragazzo non ha ancora la maturità giusta per comprenderli e gestirli nella maniera corretta.

Questo rischio può essere arginato grazie alla supervisione di un adulto di riferimento.

2 Possibili soluzioni

Per evitare che i ragazzi siano esposti a contenuti non adatti a loro è possibile:

- installare un **filtro** sul pc;
- **supervisionare** la loro attività online e **dialogare** con loro, responsabilizzandoli a un utilizzo sicuro della rete.

Il filtro

È possibile installare un filtro, che controlla i contenuti del pc o di una rete specifica, mostrando solo quelli consentiti in base alle impostazioni.

Esistono diverse tipologie di filtri famiglia:

- ***il filtro del browser o browser specializzati***

Alcuni browser hanno delle impostazioni di controllo parentale, con la possibilità di scegliere il livello di filtraggio, che consentono di evitare i contenuti che non si vogliono far visualizzare. Alcuni browser consentono anche di bloccare il cambio delle impostazioni di controllo parentale per evitare che il minore possa cambiarli. Questo sistema di controllo può essere impostato anche sui dispositivi Android. Per abilitarlo bisogna cercare nelle impostazioni del browser.

Ci sono, inoltre, dei browser creati per i minori, che consentono di accedere solo ad alcune risorse predefinite, funzionando quindi come il modello "biblioteca di casa", con la sola differenza che la gestione è affidata a un fornitore esterno. Alcuni sono facilmente aggirabili e consentono all'utente di navigare con altri browser, altri sono più robusti e non consentono questa possibilità;

- ***modello walled garden: la biblioteca di casa***

È il sistema più sicuro di filtraggio. Consiste nel compilare una lista di siti Internet conosciuti e quindi sicuri, e far navigare i propri figli solo su quelli. È così chiamato poiché equivale a

inserire nella biblioteca dei ragazzi solo libri di qualità. Molti programmi offrono questa possibilità;

- ***programma installato su PC che filtra i contenuti***

Esistono molti programmi di filtraggio che utilizzano criteri e metodi diversi. Spesso combinano più criteri per svolgere al meglio la loro funzione.

Essi sono costituiti da un elenco di siti da bloccare, con la possibilità di abilitare quelli che si ritengono utili. L'elenco necessita di un aggiornamento continuo e non è mai completo, poiché ogni giorno vengono messi in rete moltissimi nuovi siti nel mondo ed è impossibile controllarli tutti. Per questo motivo tutti i programmi attuali utilizzano anche l'analisi dell'indirizzo o del contenuto.

Quelli che utilizzano l'analisi del contenuto sono i più efficaci, perché decidono in tempo reale se i contenuti rientrano in una delle categorie che l'utente ha vietato. Questo tipo di filtro offre una protezione anche per quanto riguarda i siti dinamici come i giornali elettronici, in quanto concede l'accesso al sito solo se il contenuto cercato è adatto ai minori. L'analisi del testo è di tipo intelligente, in quanto blocca il sito solo se c'è una combinazione di parole negative e non solo una singola parola. I limiti di questo tipo di filtro stanno nel non poter bloccare le immagini non corredate da parole negative e nel non poter analizzare tutte le lingue del mondo. Inoltre, la comprensione automatica del testo è limitata in quanto il programma non capisce quello che legge, ma sceglie in base a criteri predefiniti. Quindi, ad esempio, non sempre sa distinguere se il contesto in cui si parla di un argomento può essere educativo oppure pornografico;

- ***servizio fornito dall' ISP: il parental control***

Si può utilizzare un ISP che dispone di un filtro di parental control, talvolta attivabile a richiesta con una password. In quest'ultimo caso è importante che la password non sia conosciuta da coloro che devono navigare in modalità protetta. La capacità di filtraggio dipende dal filtro utilizzato dall'ISP. Questo tipo di filtro è aggirabile se l'utente può collegarsi alla

rete in un altro modo. In alcuni casi è facilmente rimovibile se la navigazione è impostata attraverso un proxy, poiché per eliminarlo basta togliere l'obbligo di uso del proxy nelle impostazioni del browser utilizzato.
Se invece il servizio è gestito per una rete locale, le impostazioni sono inaccessibili agli utenti, che possono perciò navigare solamente attraverso quel canale filtrato. È quindi una soluzione valida per le scuole o le aziende;

- ***server DNS***

Sono servizi gratuiti o a pagamento che filtrano gli indirizzi, al fine di evitare i siti indesiderati secondo categorie predefinite o definibili dall'utente. Questo filtro può essere impostato su ogni singolo pc o sul dispositivo che consente l'accesso alla rete. Nel primo caso è importante che vengano attivati dei meccanismi che non consentano al minore di accedere alle impostazioni per cambiarle, ad esempio creando un account "amministratore", al quale può accedere solo l'adulto. La soluzione migliore è quella di attivare sul router o proxy il DNS del fornitore di servizio, applicando anche delle impostazioni che impediscono l'uso di altri DNS dall'interno della rete collegata a quel router o proxy.

- ***motori di ricerca con controllo dei contenuti***

Molti motori di ricerca permettono di attivare un filtro per eliminare immagini o contenuti non adeguati ai minori. Essi consentono di impostare il filtro a vari livelli.
Verifica sul motore di ricerca che utilizzi se esiste questo servizio e le modalità per attivarlo. Di solito, nei motori di ricerca che lo contengono, il filtro è già attivo in modalità "media".

Le tipologie di filtro elencate presuppongono che l'adulto abbia un po' di dimestichezza con le nuove tecnologie.
Se il filtro è sicuramente consigliato per quanto riguarda i più piccoli, va ponderato bene il tipo di utilizzo che se ne può fare se i ragazzi sono più grandi, poiché essi spesso hanno le competenze tecniche per "aggirarlo" e possono essere ulteriormente invogliati a farlo se il grado di rigidità del filtro è troppo ele

vato, in quanto impedisce di soddisfare quelle curiosità tipiche dell'età adolescenziale. Un filtro troppo rigido, inoltre, potrebbe portarli a reperire le informazioni a cui sono interessati in maniera alternativa, utilizzando un pc senza filtri di un amico o connettendosi da un internet point, rendendo così impossibile la supervisione dell'adulto. Quindi, è fondamentale **adattare il filtro** all'età del minore. Inoltre, è consigliabile **condividere** con il minore la scelta di installare il filtro, spiegandogli le motivazioni e i vantaggi che ne conseguiranno.
È fondamentale tenere presente che **il filtro non garantisce una protezione al 100%**. Quindi si rivela utile affiancarlo ad altre strategie di protezione.

Supervisione e dialogo

Le possibili soluzioni alle quali un adulto può ricorrere per arginare il rischio che il minore si imbatta in contenuti non adeguati dipendono dall'età del ragazzo. Se si tratta di un bambino una soluzione potrebbe essere quella di utilizzare il computer insieme a lui. Se invece il minore è più grande è probabile che abbia bisogno di vivere la sua esperienza virtuale in autonomia e che quindi non ci consenta di navigare con lui.
In generale, è utile posizionare il pc in un punto della casa in cui sia facilmente controllabile (salotto, spazi comuni, ecc.).
Inoltre, è importante tenere d'occhio i contatti e i contenuti con i quali il minore si intrattiene e dargli modo di rivolgersi, se necessario, all'adulto di riferimento, **aprendo la strada a un dialogo**, finalizzato a:
- responsabilizzarlo nell'utilizzo della rete;
- aiutarlo a sviluppare un senso critico nei confronti di ciò che vede online;
- spiegargli i possibili rischi ai quali potrebbe essere esposto;
- incoraggiarlo a **segnalare** eventuali contenuti che potrebbero turbarlo.

3 Adescamento online

La rete accresce la possibilità di socializzare grazie ai social network, social blog, forum e giochi online. Molto spesso i minori mantengono i contatti con persone che conoscono nella vita reale, ma può accadere che facciano amicizia con persone che non hanno mai visto. In quest'ultimo caso si può celare il rischio di **"grooming"** (dall'inglese grooms: "cura"), termine con il quale si indica l'adescamento online di un minore da parte di un adulto potenziale abusante, che avviene principalmente tramite le chat. L'adulto adesca il minore spesso fingendosi un suo pari e creando un **legame di fiducia**, che si fa sempre più intimo e confidenziale, per essere poi spesso seguito dallo scambio di foto intime e messaggi sessualmente espliciti (**sextig**) il cui scopo finale è quasi sempre quello di portare il minore ad un incontro offline. Le conversazioni e le foto inviate dalla vittima vengono poi utilizzate dall'adulto per far tacere il minore.

Per evitare che un minore incorra in tale rischio è importante:

- informarlo sul possibile pericolo, mettendolo in guardia su quanto sia facile creare una falsa identità online e la conseguente possibilità che chi è online non è detto che sia chi dice di essere;
- controllare il modo in cui utilizza la rete;
- spiegargli i motivi per i quali non deve mettere online o scambiare con persone conosciute in rete dati personali o foto, anche se si pensa che queste siano amiche e che ci si possa fidare di loro;
- dirgli di segnalare all'adulto se riceve una proposta di incontro offline o se gli viene richiesto l'invio di foto o video da parte di qualcuno conosciuto online;
- dirgli di non fissare appuntamenti con persone conosciute online o, se si desidera davvero conoscerle, comunicarlo all'adulto e andarci con lui o, se l'età lo consente, lasciare al ragazzo la possibilità di scegliere con chi andare e assicurarsi che incontri il soggetto in luoghi pubblici e sicuri preventivamente comunicati all'adulto;
- informare il minore sulla possibilità di rivolgersi alle Autorità o

ad associazioni di tutela dei minori se è vittima di adescamento.

Cyberbullismo

Il termine cyberbullismo indica una serie di comportamenti assunti in rete, messi in atto da un singolo o da un gruppo, finalizzati a danneggiare una persona. Il cyberbullismo è ancora più insidioso del bullismo, poiché la rete offre tante facilitazioni all'abusante, come ad esempio l'anonimato e la possibilità di colpire la vittima in qualsiasi ora del giorno e della notte, invadendo profondamente la sua privacy. Inoltre, i metodi per attuare tale forma di prevaricazione sono molto più potenti, basti pensare che il cyberbullo può cambiare spesso identità o può addirittura creare un falso profilo con l'identità della vittima e spacciarsi per lui. Da non sottovalutare poi la portata del fenomeno, che, date le potenzialità della rete, può raggiungere una vasta utenza.
La rete offre diverse modalità attraverso le quali compiere atti di cyberbullismo. Alcuni esempi sono:
- pettegolezzi o insulti diffusi tramite messaggi su e-mail, chat, social network e blog;
- mettendo in rete informazioni, immagini o video (a volte anche falsi) imbarazzanti;
- costruendo un falso profilo o spacciandosi per qualcun altro, al fine di veicolare messaggi che mettano in imbarazzo o danneggino la reputazione della vittima;
- facendo minacce fisiche alla vittima attraverso la rete.

In genere la vittima prescelta è una persona che non riesce a reagire e a difendersi e le azioni ai danni di quest'ultima vengono reiterate nel tempo.
Tale fenomeno spesso è difficile da rilevare per gli adulti, poiché la maggior parte delle volte è consumato solo in rete.
Per combattere il cyberbullismo è fondamentale agire su due fronti: quello della **potenziale vittima** e quello del **potenziale abusante**.

- **Prima regola: rispetto**. Gli adulti di riferimento (genitori, insegnanti, educatori, ecc.) devono insegnare ai ragazzi il rispetto per gli altri sia "online" che "offline". È importante far capire loro che offese e pettegolezzi feriscono anche in rete e che tali comportamenti non sono tollerati in alcun caso.
- **Tenere sotto controllo l'attività online dei minori**. È importante che l'adulto controlli l'uso che fanno i ragazzi della rete. In particolar modo, è opportuno che cerchi eventuali segni di cyberbullismo nei casi in cui il comportamento dei ragazzi si modifichi negativamente quando sono online.
- **Insegnare al minore a tenere al sicuro i propri dati**. Suggerire ai ragazzi di tenere al sicuro i dati di accesso agli account personali o altre informazioni che potrebbero renderli vittime di episodi di cyberbullismo.
- **Gli atti di cyberbullismo devono essere denunciati**. Bisogna incoraggiare i ragazzi a denunciare immediatamente eventuali atti di cyberbullismo subiti, chiedendo aiuto ad un adulto di fiducia, in modo da bloccare tempestivamente l'attività dell'abusante.

Se il minore è vittima di cyberbullismo è importante:
- **Agire subito.** Non bisogna aspettare nell'eventualità che tali atti cessino senza alcun intervento, è importante mostrare al minore sostegno e protezione;
- **Consigliare al minore di ignorare i messaggi e le provocazioni**. I cyberbulli cercano una reazione da parte delle vittime che è importante non offrire per non alimentare tali comportamenti;
- **Cercare di individuare l'identità del bullo per denunciarlo e segnalarlo** ai siti in cui sono avvenuti tali atti. Molti siti hanno, infatti, in vigore policy che permettono di affrontare subito il problema. YouTube, ad esempio, non solo consente di segnalare un utente o un contenuto molesto, ma permette anche di eliminare i commenti e bloccare un utente affinché non interagisca con i propri contenuti oppure di disattivare i commenti o attivarli solo previa approvazione;
- **Conservare le prove.** È importante salvare e-mail, messaggi e immagini inviate dal cyberbullo nell'eventualità che possano ser

vire alle autorità per le indagini.
Per segnalare atti di cyberbullismo e altre situazioni di pericolo o di grave disagio che riguardano un minore, adulti e ragazzi possono chiamare il 114 Emergenza Infanzia, la linea di emergenza del Dipartimento per le Pari Opportunità gestita da Telefono Azzurro.
In generale, per la richiesta di informazioni o per segnalazioni di violazione online di norme penali è possibile contattare la Polizia Postale e delle Comunicazioni agli indirizzi e-mail degli uffici di tutta Italia.