



CONTENUTI
EXTRA



PROTEZIONE

Filtri per la navigazione

Internet è alla portata di tutti i bambini e ragazzi: a scuola, a casa, dagli amici e in qualsiasi luogo con un telefonino, un tablet o le nuove tv su cui è possibile fruire dei contenuti presenti in rete.

Un genitore o un insegnante deve intervenire proteggendo la navigazione così come protegge il bambino dal freddo o dalle infezioni. Per quanta fiducia si possa riporre nei ragazzi, spesso una semplice ricerca su Google può offrire contenuti inaspettati e disturbanti. Occorre, quindi, prevedere una serie di protezioni per evitare quanto più possibile il contatto con pagine o contenuti inappropriati.

A tal riguardo esistono dei “filtri famiglia” denominati anche “parental control” (controllo genitori); alcuni sono gratuiti come Safesearch di Google, altri possono avere un costo e sono solitamente abbinati a prodotti antivirus o firewall. Essi permettono di bloccare l’accesso a contenuti dannosi, immagini o video di esplicito contenuto sessuale o particolarmente violenti. Inoltre consentono di monitorare a distanza le attività online dei ragazzi e di impedire la divulgazione dei dati sensibili.

Non solo a casa ma anche e soprattutto a scuola è importante proteggere le reti, anzi, garantire una navigazione protetta è un dovere di ogni istituto. Ogni scuola deve quindi avere personale esperto capace di adottare le essenziali protezioni per la rete scolastica impostando un firewall capace di controllare gli accessi e un sistema di autenticazione crittografato. È necessario, inoltre, gestire e mantenere aggiornati i sistemi antivirus e antispyware, proteggere le mail dallo spam, e curare un sistema idoneo a rilevare le intrusioni e le vulnerabilità della rete.

Blocchi per i siti web

Al fine di evitare la navigazione su siti inadeguati e poco sicuri, è possibile limitare l’accesso a un gruppo di siti web, delimitato e controllato in base all’età dei nostri ragazzi. In ambiente Windows, nel pannello di controllo, vi è uno strumento dedicato: si tratta di “Controllo genitori”, che permette di limitare i tempi

di connessione, i tipi di giochi e i software che i bambini possono utilizzare dal proprio account. Inoltre, è possibile definire il livello di sicurezza per mezzo degli account windows/msn per impedire al proprio figlio di visualizzare determinati siti web o di conversare online in chat. Inoltre è possibile accedere al sito “Family Safety”, un filtro web che permette la navigazione solo su siti verificati. Anche in questo caso esistono numerose alternative, in alcuni casi gratuite e in altri con dei costi.

Anche a scuola è necessario mettere in azione strumenti di prevenzione per la navigazione su siti poco sicuri o inadeguati, con soluzioni software che gestiscono il filtraggio delle pagine web. Gli esperti informatici delle reti scolastiche dovranno predisporre e mantenere aggiornato un elenco di siti non permessi in modo che nemmeno inavvertitamente i ragazzi (e gli insegnanti) possano navigarci. Il sistema di filtraggio deve essere graduato in base alla tipologia di utenti e naturalmente all'età.

Controlli su console (Xbox, Wii, Playstation)

Molti genitori pensano che le console servano solo per giocare e non abbiano alcun rapporto con il web, in realtà negli ultimi anni si sono evolute, permettendo l'accesso a quasi tutti i contenuti web, per cui bloccare e rendere sicura la navigazione da PC, lasciando completamente libera quella attraverso le console, significa lasciare privi di protezione i nostri ragazzi che, per mezzo di esse, avranno accesso senza controllo ai social, a youtube, ai servi di messaggistica istantanea, ecc. Qui di seguito, le pagine dedicate, da ciascuno dei principali marchi di console video, all'impostazione del controllo genitori:

- Xbox
- Wii
- Playstation

Antivirus

Utilizzare un antivirus è un imperativo per chiunque utilizzi un device digitale, per la navigazione del web o l'utilizzo di mail e messaggistica istantanea, ancora di più se utilizzato insieme a minori. Non ci dilungheremo sul funzionamento di un antivirus, ma è utile ribadire che il suo impiego corretto permette di evitare l'attacco di spyware, virus e malware, di mantenere protetti i nostri dati sensibili e quelli della scuola, di impedire l'introduzione indesiderata, nel nostro PC, di hacker o malintenzionati di ogni genere, che potrebbero mirare non solo ai nostri dati e ai nostri soldi ma soprattutto al nostro tesoro più prezioso: i nostri figli.

Regole

Regole precise e condivise sono importanti per l'educazione dei ragazzi a scuola e in famiglia: la sicurezza informatica e i rischi connessi al suo uso irresponsabile sono tematiche che meritano curati approfondimenti.

Sicuramente uno dei primi divieti da utilizzare in ambito scolastico è l'uso del cellulare, almeno durante le ore di lezione, anche il personale docente deve dare il buon esempio e non utilizzare telefoni in classe come segno di rispetto reciproco.

Nelle ore dedicate all'apprendimento informatico o all'utilizzo del laboratorio informatico, anche per le altre discipline, è importante spiegare le regole per una corretta navigazione e controllare che non vi siano trasgressioni. In sincronia con la scuola lavora la famiglia, che deve imporre un preciso limite temporale di permanenza online o di gioco, inframezzato da pause regolari di almeno cinque minuti ogni quarantacin-

que-sessanta minuti, deve insegnare loro a non offrire a nessuno i propri dati personali, come il numero di telefono, l'indirizzo di casa o della scuola, informazioni personali sulla propria famiglia o i propri amici e non registrare le password di mail, social network, skype o altro su PC.

Polizia Postale

Se ci sono sospetti relativi alla sicurezza dei nostri figli o se dobbiamo denunciare attività illecite avvenute per mezzo di internet, è necessario rivolgerci alla Polizia Postale e delle Comunicazioni, l'area specifica della Polizia di Stato che si occupa di fronteggiare i reati telematici e fornisce assistenza e informazioni sia per la prevenzione sia per perseguire penalmente chi commette reati sul web.

Commissario di P.S.

PERICOLI

Adescamento online

Tecnicamente noto anche come “grooming”, è un procedimento utilizzato da chi nutre interessi sessuali verso i minori, a cui rivolge attenzioni particolari con modalità ingannevoli, che spesso sfociano in prestazioni sessuali sia online che in persona. Si comincia contattando i fanciulli su Internet, cercandoli sui social network, ma anche in chat online dedicate a giochi e attività collegate agli interessi dei bambini e dei ragazzi. Gli adescatori spesso li irretiscono con piccoli regali, dedicando loro molte attenzioni fino a ottenere fiducia e confidenze, in una dimensione sempre più privata e intima, per mezzo del cellulare o in alcuni casi con contatti diretti nei luoghi frequentati dal minore (palestra, scuola, ecc.). Poi attraversano la porta della loro innocenza, avanzano richieste presentate come lecite e naturali: foto privi di indumenti o video in pose sempre più esplicite. Situazioni imbarazzanti che spingono i minori a chiudersi nei confronti delle loro famiglie, precludendosi un aiuto importante. Senza contare che spesso l'adescatore continua il rapporto con il minore utilizzando minacce e blandizie, ricatti e abusi psicologici, che imprigionano la giovane vittima nella paura e nella vergogna.

Cyberbullismo

La rete permette contatti sempre più veloci e plurimi, medaglia a due facce, una positiva e l'altra negativa, poiché aumentano, in sincrono, anche le possibilità di interazioni negative.

Il cyberbullismo ne è un esempio, si tratta di mobbing in Internet, infatti, per designarlo, si usano anche i termini “cybermobbing” e “internet mobbing”. Viene messo in atto mediante l'uso dei media digitali e consiste nell'invio ripetuto di messaggi offensivi tramite sms, in chat o su facebook per molestare una persona per un lungo periodo.

Gli autori, i cosiddetti “bulli”, sono spesso persone che la vittima ha conosciuto a scuola e sentendosi protetti dall'anonimato, offendono, minacciano o ricattano le loro vittime direttamente o facendo pressione psicologica su di loro, le diffamano, diffondendo dicerie sul loro conto.

Si tratta di un fenomeno molto grave perché in pochissimo tempo le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, anche perché, i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi. Spesso i genitori e gli insegnanti ne rimangono a lungo all'oscuro, perché non hanno accesso alla comunicazione in rete degli adolescenti.

Virus

Quando si pensa al web, la prima minaccia che ci viene in mente è quella dei virus e dei possibili software o file che dalla rete possono danneggiare il nostro computer. Spesso la navigazione dei più piccoli è più ingenua ed esposta agli attacchi e alle minacce nascoste. In determinate pagine web, particolarmente attraenti per gli adolescenti perché propongono giochi o attività legate alle loro passioni preferite, sono spesso inseriti virus e spyware di varia tipologia che intaccano il sistema operativo, deviano verso pagine commerciali, trafugano i dati che, replicandosi, impediscono il normale funzionamento del computer.

Dipendenza da internet

Come tutti gli strumenti di comunicazione, anche la rete non è esente da cattivi usi e da abusi che, negli ultimi anni, hanno talvolta portato ad osservare nel campo della salute mentale, una moderna forma di dipendenza, definita internet-dipendenza, retomania o anche Internet Addiction Disorder (I.A.D.). L'accesso ad informazioni illimitate, a giochi infiniti e la facile evasione dal mondo reale, possono infatti rendere patologico il rapporto dei giovani con internet.

Dedicare molto tempo alla navigazione, mostrando disinteresse per il mondo reale rappresenta il primo sintomo della patologia. Al di là delle diverse componenti che possono contribuire ad originare i diversi casi di rete-dipendenza, la caratteristica costante che fa da snodo ad ogni dipendenza da Internet è la capacità della rete di rispondere (o illudere di rispondere) a molti bisogni umani, consentendo di sperimentare dei vissuti importanti per la costruzione del Sé e di vivere emozioni sentendosi, al contempo, protetti. Internet, infatti, annulla lo spazio, supera le barriere e i vincoli di tempo e di spazio e consente di realizzare ciò che nella realtà non è possibile o che richiederebbe molto più tempo.

Quando non ha la possibilità di connettersi, il ragazzo appare ansioso e infastidito, le passioni abituali sono trascurate e spesso anche gli impegni scolastici o addirittura l'igiene e la cura personali. Chi è affetto dalla sindrome di dipendenza da internet, tenta di nascondere l'effettivo tempo trascorso online, si collega anche di nascosto, non vuole essere disturbato se è davanti allo schermo e non parla delle attività effettuate mentre è connesso. Si riscontra una tendenza comportamentale definita "solipsismo telematico", ossia la propensione ad eleggere il web come luogo di rifugio in cui appartarsi per trovare sollievo da problemi quotidiani: inevitabilmente la Rete conquista fette sempre più ampie del tempo delle giornate del retomane. Nei casi più gravi possono manifestarsi alterazioni nel comportamento alimentare, disturbi del sonno, cefalee e problemi visivi.

Sexting

Il termine "sexting" deriva dall'unione delle parole inglesi "sex" (sesso) e "texting" (pubblicare testo) e consiste nell'invio e/o ricezione e/o condivisione di messaggi, attraverso qualsiasi mezzo elettronico, con contenuti esplicitamente sessuali: frasi, foto e video osceni. Può cominciare come un gioco per mettersi in mostra, fatto senza pensare alle conseguenze. Le immagini e i video si trasformano in mezzo di ricatto perché chiunque le

abbia ricevute, ha la possibilità di diffonderle sui social network o ad un' ampia cerchia di persone macchiando la reputazione della persona protagonista dei contenuti e creando profondo disagio emotivo e psicologico, oltre che seri problemi legali.

L'invio di foto che ritraggono minorenni in pose sessualmente esplicite, configura il reato di distribuzione di materiale pedopornografico. Le motivazioni che spingono i minori a scambiarsi questo tipo di materiale sono diverse: la condivisione spesso avviene tra fidanzati o amici particolarmente intimi, tra una stretta cerchia di persone, ignorando che le immagini possano diffondersi con estrema facilità, in modo incontrollabile. In altri casi lo stimolo a condividere questo materiale può essere frutto di minacce o ottenuto in cambio di denaro o ricariche telefoniche.

Gioco d'azzardo

Rappresenta un fenomeno in pericolosa crescita, probabilmente anche in risposta della crisi, che purtroppo coinvolge anche i minori, nonostante il gioco online richieda registrazione anagrafica e l'impiego della carta di credito perché esplicitamente rivolto a chi ha almeno 18 anni.

Anche le scommesse online appaiono particolarmente attraenti per i minori, probabilmente per il piacere della sfida insito in esse. I giovanissimi iniziano a giocare per emulare i grandi, ma anche per le laute vincite che spesso dominano i banner pubblicitari onnipresenti sul web. Per i giovanissimi inoltre il valore dei soldi è ancora poco definito, spesso sono molto convinti della possibilità di vincere e quello che in principio è un puro divertimento, si trasforma in una grave dipendenza patologica di difficile risoluzione.

Furto di account

Spesso associato ad altre problematiche, quali ad esempio il cyberbullismo, il furto di account è un rischio frequente. I minori sono ovviamente i più vulnerabili, in quanto più aperti e propensi a fidarsi degli estranei adulti e spesso ignari delle minacce nascoste, presenti nel condividere i propri dati personali. Inoltre per l'ingenuità che è connaturata alla loro tenera età, non hanno difficoltà a trasmettere i dati sensibili dei propri familiari: date di nascita, il nome della madre da nubile, password, codici fiscali, numeri di conto bancario. Eventuali truffatori possono utilizzare questi dati per violare conti online e utilizzare illecitamente i mezzi di pagamento, inoltre possono violare la privacy avviando un percorso di minacce e molestie sul web.

Pagine inadeguate

Internet permette a chiunque di creare contenuti e pubblicare pagine web che possono non essere adeguate ai bambini, ma che possono essere liberamente visualizzate anche da essi. I bambini possono imbattersi in materiale violento o con riferimenti chiaramente sessuali, in contenuti che inneggiano all'odio razziale, che invitano alla condivisione di discutibili abitudini alimentari o, ancora, a siti di gioco d'azzardo.

Webcam

La webcam è la periferica che consente di registrare i nostri video o di effettuare videochiamate. Purtroppo, molti dei reati che riguardano i minori e la loro delicata dimensione sessuale, avvengono per mezzo delle webcam installate sui PC, su tutti i telefoni di ultima generazione e integrate anche nella console per videogiochi. L'attività di questa periferica può essere guidata anche dall'esterno per videosorvegliare, anche fuori

casa o ufficio, un ambiente: certamente un supporto positivo per molti se usato correttamente. Tuttavia potrebbe entrare sotto il controllo di persone indesiderate e invadere la nostra privacy. L'attualità, infatti, ci informa di molte estorsioni a carattere sessuale, avvenute proprio via webcam e i più colpiti sono i bambini e i ragazzi, proprio perché usano la webcam ingenuamente, senza riflettere sugli aspetti positivi e negativi insiti in questo strumento.

Le modalità più frequenti di adescamento riguardano i social network o le chat room, disponibili all'interno di siti attraverso cui si accede ai giochi online. Il malintenzionato, spesso fingendosi coetaneo della vittima, inizia una conversazione amichevole ed entra sempre più in confidenza fino a indurre il ragazzo ad inviargli immagini indecenti tramite webcam. Poi registra il materiale acquisito e minaccia di condividere gli "scomodi" contenuti con gli amici del ragazzo o con la famiglia. I ragazzi per vergogna preferiscono tacere e continuare a subire l'abuso con devastanti ripercussioni a livello psicologico.

Per prevenire non c'è modo migliore che conoscere: i nostri ragazzi devono essere informati sui rischi, occorre invitarli a parlare delle loro attività online, perché internet rappresenta una fonte inesauribile di risorse e materiale formativo e, se usato nel modo corretto, fornisce loro notevoli opportunità.

CONSIGLI

Tempi di navigazione

È fondamentale abituare i nostri figli a contenere il tempo di navigazione online e di utilizzo delle console per videogiochi. Farlo da subito significa impartire regole precise che saranno accettate e comprese anche in seguito e permetteranno un corretto utilizzo del computer. In ogni modo, qualora risulti difficile controllare i tempi di navigazione, è bene utilizzare il sistema di controllo genitori inserito in numerosi software antivirus e nella sezione "Controllo genitori" disponibile nel Pannello di controllo di Windows.

Monitorare

Spesso i bambini e i ragazzi non si rendono conto della pericolosità di un sito web per cui è opportuno controllare spesso la cronologia di navigazione ed eventualmente bloccare i siti pericolosi.

Per i più piccoli è consigliabile consentire la navigazione solo su siti verificati, innalzando il livello di sicurezza del firewall e impostando correttamente il browser per impedire la navigazione su siti dannosi.

Partecipare

Qualsiasi accortezza o sistema adottato per proteggere la navigazione online di bambini e ragazzi, non sarà efficace se non supportato da una partecipazione attiva alle loro attività online. L'unico modo per prevenire molti rischi della rete è essere accanto ai nostri ragazzi, comprendere quello che fanno, giocare e divertirli insieme a loro, dedicare il nostro tempo alle loro attività in Rete, comunicare con loro anche attraverso i social, in modo da monitorare le loro amicizie senza risultare invadenti. Parlare con loro di problematiche legate al download illegale di musica e film, che avviene spesso su siti pericolosi sia per la sicurezza sia per la possibilità di incontri sgradevoli, discutere dell'utilizzo consapevole di carte di credito per evitarne l'uso improprio e

introdurre in famiglia anche le tematiche legate all'educazione sessuale, affinché i nostri ragazzi non cerchino altrove informazioni distorte su temi che, per natura, li interessano.

Social Network

Il loro scopo è quello di creare una rete di comunicazione e socializzazione tra milioni di persone e, proprio come nel mondo reale, è il luogo virtuale più ricco di insidie. Realizzare un profilo falso e richiedere amicizia ai ragazzi su internet è molto facile, basta condividere gli stessi interessi, comportarsi in modo simpatico, offrire quello che i più giovani vogliono: giochi, ricariche e attenzione. Spesso è sui social network che si perpetuano atti di violenza psicologica nei confronti di ragazzi presi di mira perché più fragili o semplicemente non uniformati alla massa. Ecco perché è importante per genitori e insegnanti conoscere il mondo dei ragazzi e farne parte, ascoltando anche i loro piccoli problemi attraverso un dialogo attivo.

I segnali d'allarme più frequenti sono il non voler andare a scuola, chiedere spesso denaro, essere tristi, dormire male, non avere amici, il calo del rendimento scolastico e l'isolamento dagli altri compagni.

Informare

L'importanza dell'informazione è fuori ogni discussione. È fondamentale educare e informare i più giovani su un corretto uso della rete, del Pc e dei device mobile, ribadire quanto più possibile la necessità di proteggere i propri dati personali spiegando che spesso condividerli significa lasciare quelle informazioni nelle mani di sconosciuti come lasciare le chiavi di casa nelle mani di ladri.

Le altre tematiche che meritano molta attenzione in ambito scolastico sono sicuramente quelle legate alla sessualità, per evitare tutti i rischi legati all'adescamento online, al sexting e al cyberbullismo, aspetti che possono essere prevenuti osservando il comportamento dei ragazzi, soprattutto di coloro che appaiono più isolati dagli altri.



Esercitare la cittadinanza significa contribuire in modo attivo al progresso di una comunità, in cui tutti i membri devono sentirsi pienamente inclusi e avere la possibilità di partecipare attivamente alla società dell'informazione e della comunicazione.

La scuola è il primo soggetto che concorre, nella società, a garantire a tutti i membri della comunità una reale inclusione e una concreta possibilità di partecipazione.

In linea con la direttiva del MIUR del 27 dicembre 2012 sui BES (Bisogni Educativi Speciali), si evidenzia che “ogni alunno, con continuità o per determinati periodi, può manifestare Bisogni Educativi Speciali: o per motivi fisici, biologici, fisiologici, o anche per motivi psicologici, sociali, rispetto ai quali è necessario che le scuole offrano adeguata e personalizzata risposta”. Si afferma inoltre che “Va quindi potenziata la cultura dell'inclusione, e ciò anche mediante un approfondimento delle relative competenze curricolari degli insegnanti, finalizzato ad una più stretta interazione tra tutte le componenti della comunità educante”.

Non si tratta solo di fornire delle tecnologie, ma di dotare insegnanti e genitori di una formazione tecnica, affinché possano creare un ambiente facilitante a casa e a scuola attraverso una rete competente (insegnanti-studenti-genitori).

Offrire a tutti i ragazzi le stesse opportunità, consente al Paese di coltivare potenzialità di crescita straordinarie. Se gli studenti sono messi in condizione di avvalersi di tutti gli strumenti informatici, utili per studiare, e di capirne il valore, potranno essere, essi stessi, stimolo per lo sviluppo di nuove applicazioni, consentendo l'attivazione di quel circolo virtuoso che consente di trovare nuove idee nello studio e nella scuola.

Tutto questo fa parte della didattica digitale a scuola, un vero e proprio approccio metodologico, che parla di collaborative learning, flipped classroom, didattica per competenze, ecc.

Ecco alcuni tra gli strumenti da introdurre nelle scuole perché abilitanti per alunni con Bisogni Educativi Speciali:

- Tablet: strumenti educativi che permettono l'installazione di font appositamente studiati per facilitare la lettura.
- Strumenti di sintesi vocale con una corretta pronuncia.

- Strumenti compensativi, quali e-book reader, calcolatrici parlanti, mappe concettuali, vocabolari, ecc., da installare sul tablet in modo che siano subito a disposizione quando occorrono.
- Libri digitali in formato ePub, che consentono al lettore di modificare font, interlinea e dimensione, funzionalità estremamente utili per i dislessici.
- Strumenti multimediali: LIM (Lavagna Interattiva Multimediale) video e dvd, che rappresentano un valido strumento per rendere più attraenti le lezioni scolastiche e per fissare meglio, attraverso l'uso delle immagini, alcuni concetti.



App e Tablet su misura per bambini e ragazzi, è possibile? Certo che sì!

Molti genitori si mostrano diffidenti verso ogni tipo di strumento tecnologico messo nelle mani dei più piccoli, pensano che siano diseducativi e che i giochi da consigliare ai bambini siano solo macchinine, bambole, puzzle e Lego, dimenticando che le nuove generazioni sono immerse nelle nuove tecnologie fin dalla nascita e che, se integrate consapevolmente ai giochi tradizionali, sono in grado di sviluppare dinamiche di apprendimento più efficaci, multitasking, in grado cioè di sviluppare la capacità di svolgere più compiti simultaneamente, stimolando continuamente il pensiero computazionale e il coding. Tablet e App rappresentano per i genitori un'ottima opportunità per guidare i bambini nei giochi, nelle letture, nell'apprendimento della lingua, parlata e scritta, e nel calcolo in maniera economica, efficiente e divertente.

Le applicazioni messe a disposizione dai market sono centinaia, adatte ad ogni età: album da colorare, libri di fiabe animati, app che aiutano a familiarizzare con le parole e con la musica e quelle che insegnano i primi vocaboli in una lingua straniera. Molte sono le applicazioni che consentono al bambino di stimolare processi cognitivi e di migliorare la vita offline: saper scegliere quelle giuste è quindi determinante.

Le app si acquistano o si scaricano gratuitamente dopo aver inserito una password che il genitore detiene. Questa è una grande responsabilità, ma anche una grande fortuna perché i genitori contribuiscono concretamente al particolare processo di sviluppo e crescita intellettuale dei propri figli.

Non esiste app, infatti, che possa funzionare in assenza di una buona interazione tra adulto e bambino. È importante che i genitori partecipino all'esperienza digitale del figlio non per controllarli o sorvegliarli, ma perché la narrazione ha bisogno di relazione, anche in campo digitale.

In questa sezione dedichiamo uno spazio a tutte le mamme, ai papà, ai nonni e agli insegnanti e, perché no, anche ai ragazzi, che vogliono consigliarci le app migliori, gratuite o meno, su cui vale la pena investire per il futuro dei nostri ragazzi.



L'esperto risponde

La figura dell'Esperto è riservata all'utente che, al fine di tutelarlo, ci poniamo come punto di riferimento per:

- Richiedere informazioni su caratteristiche e contenuti del Programma Eipass Junior, delle certificazioni Eipass e sugli standard qualitativi e di qualificazione professionale dei percorsi di certificazione erogati da Certipass;
- Richiedere informazioni sull'organizzazione, il funzionamento e le attività svolte da Certipass e dal network degli Ei-Center;
- Segnalare eventuali abusi e/o irregolarità.

È possibile contattare l'Esperto al Numero Verde 800.088.331 o compilare il form mediante la pagina <http://it.eipass.com/sportello-del-cittadino/>