Guida alla Sicurezza Online per le Famiglie

di **Marian Merritt**
Introduzione di **Ida Setti**

STOP | THINK | CONNECT™

Norton™ by Symantec

Ida Setti

Introduzione

Internet è un luogo variegato e meraviglioso, che offre risorse informatiche incredibili e milioni di opportunità per stringere nuove amicizie e creare comunità online. Eppure spesso, per molti genitori che hanno un'esperienza più limitata, il Web può essere fonte di grande apprensione. Temiamo infatti per quello in cui i nostri figli si possono imbattere durante la navigazione e ci chiediamo come sia possibile proteggerli.

I nostri figli sono cresciuti utilizzando tecnologie sorprendenti che noi, da giovani, non avremmo mai neppure sognato. Per loro, Internet è solo un altro posto dove informarsi e scambiarsi opinioni, dove giocare e creare o semplicemente dove 'intrattenersi' con gli amici. È importante conciliare i nostri timori in merito alla loro sicurezza online con la loro libertà di esplorare il Web.

Il mio ruolo in quanto Responsabile della Sicurezza Online di Norton prevede il tentativo di aiutare genitori e figli a sfruttare Internet al meglio e con la massima sicurezza, divertendosi il più possibile. Il presente opuscolo è un punto di partenza di questo entusiasmante percorso, nel quale tu e i tuoi figli potete imparare e crescere insieme. Cercherò d'illustrare alcune delle destinazioni e delle tendenze online più diffuse, sottolineando nel contempo gli eventuali aspetti da prendere in considerazione e consigliandoti modi per proteggere tuo figlio nello svolgimento di questa attività.

Sia che si tratti di un bambino che si avventura per la prima volta in rete o di un adolescente che è rimasto affascinato da un sito di social network, il mio consiglio è di non avere timori e d'imparare insieme a lui con l'aiuto di guide come questa.

Ida Setti
Responsabile della Sicurezza Online di Norton
http://it.norton.com/family-resources/

Indice

Guida alla Sicurezza Online per le Famiglie

Le diverse età

Bambini della scuola primaria (5-7 anni)
È l'età in cui oggi molti bambini entrano in contatto con Internet. I genitori condividono video-chat con i parenti o mostrano ai loro figli siti di giochi e video online. Secondo un' indagine europea[1], l'età media in cui un bambino usa per la prima volta Internet è sempre più bassa (si parte dagli 8 anni in Inghilterra dove si registra anche il più alto numero di connessioni da scuola). Anche senza una connessione a casa, tuo figlio potrebbe quindi partecipare a laboratori d'informatica, avere un PC o un Mac® in classe e un curriculum informatico completo già in tenera età. Altri, invece, spesso fanno la prima esperienza con il computer di casa, imparando dai genitori o dai fratelli.

I bambini più piccoli, anche di due o tre anni, sono attirati da siti che contengono giochi online (come ad esempio Lego o Disney). Alcuni di questi sono quasi forme semplificate di social network, in quanto contengono chat e altre funzioni di comunicazione. I genitori di bambini piccoli dovrebbero inizialmente escluderle. Negli Stati Uniti, alcuni siti importanti come Webkinz (costruito intorno ai pupazzi Webkinz) sono diventati famosi grazie allo sforzo di creare un ambiente sicuro. Nel Webkinz World, i genitori non devono disabilitare la chat per i più piccoli, in quanto questa sfrutta un metodo particolare basato su un copione, così che i genitori possono consentire ai figli d'inviare messaggi o altro e 'chattare' con gli amici senza preoccupazioni. È un ottimo modo per introdurre il concetto di chat e cominciare a discutere di 'netiquette' (il galateo online) e di procedure di sicurezza. Kinz Chat Plus è una chat monitorata, per l'uso della quale anche i genitori che ritengono i propri figli abbastanza maturi devono comunque dare espressamente il permesso, che può essere sempre revocato.

Fai in modo che i tuoi figli più piccoli capiscano che intendi limitare l'uso della chat online, anche se si svolge entro l'interfaccia amica del gioco o del club preferito. In seguito potrai introdurre il concetto di chattare con persone che conoscono, come zie, zii o amici, insistendo sempre sul fatto che devono chiedere il permesso prima di parlare con chiunque in rete.

[1] Livingstone, S., Haddon, L., Görzig, A. y Ólafsson, K. (2011). Risks and safety on the Internet: the UK report. LSE, Londra:EU Kids Online

Con i bambini di questa età, l'ideale sarebbe partecipare attivamente alle loro attività online, proprio come fai con i compiti a casa. Ad esempio, è importante che il computer che usa il bambino sia sempre visibile, collocato in uno spazio comune come la cucina, lo studio o la stanza in cui la famiglia si riunisce. Il software di controllo parentale ti può aiutare a limitare l'accesso ad alcuni siti anche quando tu non sei presente. Il controllo blocca, inoltre, qualsiasi informazione che non vuoi che tuo figlio riveli, quale il nome, l'età, il numero di telefono o altri dati personali. Abilita tutte le funzioni di filtro e di sicurezza offerte dal motore di ricerca installato sul computer (come la funzione di Google SafeSearchTM) per evitare che il bambino finisca inavvertitamente su un sito per adulti o su altri siti inadeguati mentre svolge i compiti. Mostra chiaramente al bambino come chiudere una finestra del browser e fagli capire che è sempre giusto chiudere un sito se si verifica qualcosa di strano o di fastidioso. Raccomandagli di non chattare, digitare messaggi o condividere informazioni con chiunque incontri in questi siti, a meno che tu non sia con lui.

ATTENZIONE: Insegna ai tuoi figli più piccoli a non rivelare mai le password, nemmeno al loro amico più caro! Il furto dell'account (una versione semplificata del furto d'identità) colpisce anche i bambini della scuola elementare.

RACCOMANDAZIONI IMPORTANTI:

- Usa il controllo parentale per limitare l'accesso ai siti approvati e il tempo trascorso online.
- Imposta rigidi parametri di sicurezza nei browser e nei siti di social network.
- Installa e aggiorna regolarmente il software per la sicurezza di Internet e i controlli parentali.
- Monitora l'uso del computer da parte di tuo figlio e stai insieme a lui quando è connesso.
- Parlagli di protezione dei dati personali (nome, numero di telefono ecc.) e spiegagli che non deve mai rivelare le password agli amici.
- Inserisci "Il Discorso" nei normali preparativi per il ritorno a scuola (vedi pag. 14).

Bambini della scuola secondaria (8-12 anni)

A questa età i bambini hanno un atteggiamento più sociale e avventuroso nell'uso del computer. Conversano con i compagni di scuola, scoprono i siti più nuovi e più "giusti" e creano per la prima volta un account di posta e di messaggistica istantanea. Chiedi informazioni a tuo figlio su questi account e quali sono le password, in modo che tu possa monitorare le sue attività e sapere con chi comunica. A questa età a volte i ragazzini cominciano a visitare i siti di social network più popolari tra gli adolescenti e gli adulti. Nella maggior parte dei casi creano un account solo quando sono un po' più grandi (e in genere l'età minima legale è 13 anni), ma tendono a visitare le pagine e i post degli amici, dei fratelli più grandi e di altri parenti che hanno pagine e profili propri. Se tuo figlio si iscrive a una social network prima di avere raggiunto l'età legale e l'azienda lo scopre, il suo account viene cancellato.

ATTENZIONE: Usa NortonTM Online Family per monitorare la creazione e l'uso degli account di social network. Così puoi anche vedere che età tuo figlio ha dichiarato di avere.

I ragazzini sono anche interessati alla musica e Internet offre un modo semplice per ascoltare, scoprire e scaricare nuovi brani, ma anche per incontrare altre persone che condividono gli stessi interessi musicali. Talvolta leggono le notizie sui gruppi o le celebrità preferite visitando il loro blog o sito, visitano vari siti per leggere gli ultimi pettegolezzi e scaricare foto, oppure scrivono su Twitter.

I siti di video sono estremamente popolari. Alcuni video contengono un linguaggio scurrile o materiale violento ed è pertanto necessario controllare attentamente i siti visitati da tuo figlio. Ricordagli anche di non cliccare sui link contenuti nei commenti ai video, che li potrebbero dirigere verso siti pericolosi o inadeguati. I ragazzini più creativi imparano a scattare le proprie foto digitali, elaborare i video e condividere quanto creato con amici e parenti. Con il tuo aiuto o con l'aiuto di un amico più esperto, cominciano anche a pubblicare online le proprie creazioni.

ATTENZIONE: Controlla la cronologia del tuo browser per sapere quali siti tuo figlio visita e con quale frequenza. Norton Online Family ti aiuta a monitorare l'attività in rete e impedisce al bambino di tentare di cancellare i siti visitati dalla cronologia.

RACCOMANDAZIONI IMPORTANTI:

- Controlla spesso la cronologia di Internet sul tuo computer (o la cronologia del controllo parentale) per sapere quali siti tuo figlio ha visitato e controlla gli account di posta e di messaggistica istantanea (MI) per sapere con chi comunica. Nota: se tuo figlio usa un telefono cellulare o una social network, potrebbe comunicare con questi mezzi anziché con l'e-mail tradizionale.
- Fissa regole per la comunicazione online e fai attenzione al downloading illegale e ai fenomeni di bullismo informatico.
- Spiega a tuo figlio che non deve mai cliccare su un link contenuto in un'e-mail o in un messaggio istantaneo, in quanto così facendo potrebbe ricevere virus o rivelare informazioni riservate e preziose ai criminali.
- Parlagli dei rischi e dei problemi legati alla pubblicazione e alla condivisione d'informazioni personali, video e foto.
- Fai attenzione ai segnali di comportamento ossessivo o dipendente (vedi Gioco online e segnali di dipendenza a pag…).
- A casa tieni computer e telefoni cellulari in vista.
- Favorisci una comunicazione aperta e stimola tuo figlio a dirti se c'è qualcosa in Rete che lo mette a disagio.
- Comincia a fare "Il Discorso" (a seguire ulteriori dettagli sul Discorso)

Adolescenti (13-17 anni)

Gli adolescenti diventano sempre più autonomi, il che si riflette nella loro vita in rete. Questa autonomia porta con sé alcune responsabilità, come ad esempio usare cautela nel frequentare il mondo online. La maggior parte degli adolescenti hanno ormai già creato uno o più account nelle social network. Alcuni diventano amici dei genitori senza problemi, mentre altri si oppongono strenuamente a questa relazione virtuale. Altri ancora creano un "falso" profilo che usano per stringere amicizia e connettersi con genitori e parenti, mentre le attività vere e più discutibili avvengono con un altro account. L'uso di un programma come Norton Online Family permette ai genitori di scoprire questo tipo di sotterfugi.

Dove sta dunque il grande fascino delle social network e di altri interessi online degli adolescenti? Con screen name, iscrizioni, blog, profili e altri elementi di Internet che visitano ogni giorno, i teenager comunicano ogni dettaglio della loro vita, lasciando tracce dei loro pensieri in tutto il Web. Spesso non sanno – o dimenticano – che qualunque cosa pubblichino in rete è visibile a tutti e probabilmente vi rimane a tempo indeterminato. Basta una singola ricerca da parte di un potenziale compagno di stanza, di un corteggiatore, di un responsabile delle ammissioni in università o di un potenziale datore di lavoro – tra cinque, dieci, anche vent'anni – per far sì che tutte le foto, le opinioni e i pensieri di tuo figlio adolescente rimangano lì, visibili a tutti e per sempre. Ecco perché è così importante fare attenzione!

Dobbiamo insegnare ai nostri figli come affrontare i rischi senza mettersi nei guai. È per lo stesso motivo, ad esempio, che vanno a scuola guida prima di cominciare a guidare un'auto, o che tu passi ore seduto pazientemente a bordo piscina durante le lezioni di nuoto. Internet richiede lo stesso tipo di cautela. Se tuo figlio alza gli occhi al cielo quando cerchi di spiegargli il "codice della strada" da applicare in rete, potresti invece provare, ad esempio, a organizzare presentazioni da parte dei genitori sulla sicurezza di Internet insieme alla scuola. La migliore educazione alla sicurezza online degli adolescenti è quella che proviene dai loro simili, opportunamente addestrati. Invita la scuola a coinvolgere i più grandi per insegnare ai giovani come gestire la propria reputazione digitale, comportarsi educatamente online e altre lezioni importanti. Potresti scoprire che tuo figlio presta più attenzione alla stessa informazione quando proviene dal di fuori della famiglia. E non dimenticare di organizzare una presentazione analoga per genitori e insegnanti. Abbiamo tutti così tanto da imparare!

ATTENZIONE: Cerca i tuoi figli su Internet e mostra loro quello che trovi. Oppure cerca te stesso come momento educativo e sii onesto su qualsiasi dato discutibile emerga. Dopo tutto, forse tuo figlio ti ha già cercato su Google!

RACCOMANDAZIONI IMPORTANTI:

- Insisti sulle regole di buona condotta online (linguaggio, dati personali, immagini, etica informatica, downloading illegale, limitazione al tempo di utilizzo ed esclusione dei siti per adulti).
- Tieni d'occhio l'attività online dei tuoi figli adolescenti (siti di social network, foto, dati personali, club e attività sportive).
- Esamina i siti che i tuoi figli visitano; non avere paura di discuterne ed eventualmente di limitare l'accesso a quelli che non ritieni opportuni.
- Ricorda che tuo figlio adolescente accede a Internet da casa, da scuola, da casa di amici, dalla biblioteca, via cellulare e persino attraverso i sistemi di gioco.
  Pertanto parla con lui delle sue attività in tutte queste situazioni.
- Invitalo a non scaricare file (musica, giochi, salvaschermo, suonerie) e a non effettuare operazioni finanziarie senza il tuo consenso.
- Insegnagli a non rivelare mai le password e a usare cautela nell'inserire dati riservati quando utilizza un computer in condivisione o pubblico, oppure un computer che potrebbe non essere sicuro. Deve sempre disconnettersi dagli account, anche quando è a casa.
- Insegnagli a non cliccare mai su un link contenuto in un'e-mail o in un messaggio istantaneo – è così che spesso si diffondono i virus o vengono divulgate informazioni riservate e preziose ai criminali.
- Ove possibile, tieni computer e cellulari in una zona comune della casa anziché nella stanza di tuo figlio.
- Favorisci una comunicazione aperta e stimola tuo figlio a informarti quando s'imbatte in rete in qualcosa che lo mette a disagio. Ricorda che è un adolescente, ma è ancora un bambino.
- Ricorda a tuo figlio di provvedere ad aggiornare il software per la sicurezza di Internet, per proteggere se stesso, ma anche te.
- Fai "Il Discorso" e chiedi a tuo figlio d'insegnarti qualcosa di nuovo su Internet.

Studenti universitari e oltre

Una volta cresciuto e uscito di casa, per motivi di studio o di lavoro, tuo figlio dovrà conoscere gli ulteriori obblighi che spettano agli adulti nel mondo online, quali proteggere la propria privacy, in particolare i dati del passaporto e i dati personali e finanziari, impedire il furto d'identità e prevenire il rischio di compromettere la sua affidabilità, particolarmente importante per un giovane adulto. Se tuo figlio adolescente usa un laptop all'università o per il nuovo lavoro, accertati che abbia compreso i rischi aggiuntivi legati all'uso di connessioni wireless e invitalo ad acquistare il software di sicurezza necessario, comprensivo di una soluzione di back-up affidabile. Dal momento che forse avrà la tentazione di rinunciare a questi elementi opzionali, è importante insistere sulla cautela quando di tratta di sicurezza del laptop.

ATTENZIONE: Controlla sul tuo account Norton **(www.mynortonaccount.com)** se il software di sicurezza che hai a casa può essere installato su un altro computer. Alcuni programmi di sicurezza Norton prevedono l'installazione su più computer appartenenti alla stessa famiglia.

Se tuo figlio frequenta un'università lontano da casa, cerca di capire quali sono le politiche relative all'uso del computer. Alcune università impongono ai nuovi studenti determinati sistemi operativi o configurazioni del software ed è quindi importante avere queste informazioni prima di andare ad acquistare il computer. Alcune classi e alcune residenze sono provviste di reti wireless (comunemente dette WiFi); devi quindi procurarti l'apposita scheda WiFi affinché tuo figlio possa usufruire di questi servizi.

“Il Discorso”

Quando si tratta dei nostri figli e delle loro attività in rete, non crediamo veramente al detto “ciò che non conosci non ti può far male”. Eppure molti di noi agiscono come se negassero l’ampia varietà di pericoli insiti nell’uso di Internet. La maggior parte dei genitori non sono esperti di Internet, né abili a navigare come i loro figli. Non c’è problema. In effetti non è necessario essere grandi esperti per poter aiutare i propri figli a utilizzare la rete in maniera sicura. Quello che conta è PARLARE con i figli di quello che fanno quando sono connessi e illustrare loro le regole da applicare. E poi ripetere tutto il discorso una volta all’anno, oppure con la frequenza che ritieni necessaria per fare sì che comprendano l’importanza delle informazioni che dai loro.

Inutile nasconderlo: è difficile indurre i tuoi figli a dirti onestamente cosa fanno su Internet. Un bambino su cinque nel mondo ammette di fare cose che i suoi genitori non approverebbero. Eppure il 62% dei bambini in tutto il mondo (secondo il Norton Online Family Report: **www.norton.com/nofreport**) hanno già avuto un’esperienza online negativa. Se non sei tu a chiederglielo, magari tuo figlio non te lo dirà mai. Quindi è il momento di chiedere!

La metà di tutti i genitori affermano di parlare di sicurezza di Internet con i figli, ma in genere lo fanno una sola volta, e il tutto si risolve a due consigli: “La gente che c’è in rete non è sempre chi dice di essere” e “Non dare confidenza agli estranei in rete.” I bambini temono che, se raccontano ai genitori dei loro errori online, questi reagiranno privandoli del computer, della connessione a Internet e dell’accesso agli amici e al resto del mondo. Immaginano che papà e mamma “non ci arrivano” quando si tratta di Internet.

Attraverso una serie di studi e ricerche a livello mondiale, noi di Norton abbiamo quantomeno scoperto che i figli vorrebbero che i genitori ne sappiano di più di Internet e che sono anche più che disposti a parlarne con loro. È una buona notizia.

Ora che sai che i tuoi figli sono disposti a parlare con te e sei consapevole di voler sapere di più di ciò che fanno, da dove devi partire? Come puoi rapportarti con i tuoi figli in maniera tale da stimolarli a essere sinceri con te? Come puoi evitare di giudicare, di reagire in maniera eccessiva o di temere quello che potresti sentire?

Come puoi avviare una discussione amichevole, priva di contrasti e abbastanza produttiva da ripetere ogni anno?

Vorrei introdurre una nuova versione di un vecchio concetto del “Discorso”. Io raccomando di parlare subito con i figli delle loro attività in rete e poi di farlo nuovamente, ogni anno. Le attività in rete dei tuoi figli cambiano continuamente. A mano a mano che crescono, visitano siti diversi, provano nuove attività e creano nuovi account nelle social network. Ieri, ad esempio, tutti comunicavano attraverso la posta, mentre oggi usano la messaggistica incorporata nelle social network o gli sms sul cellulare. A mano a mano che tuo figlio cresce, il suo bisogno di privacy aumenterà, ma aumenteranno anche i rischi che correrà in rete. Assumersi rischi fa parte del processo di maturazione di un adolescente, ma come genitore, è tuo compito mettere un limite a questi i rischi senza compromettere la reputazione o il futuro di tuo figlio. Devi però essere consapevole che probabilmente, di tanto in tanto, questi limiti verranno superati.

“Il Discorso” si basa sostanzialmente su cinque domande, che in genere funzionano con bambini di ogni età adeguando il contenuto di conseguenza. Lascia spazio (sia fisico sia temporale) a tuo figlio per rispondere a queste domande. Personalmente amo fare questo tipo di conversazione con i miei figli in auto (per qualche motivo, quando tutti sono impegnati a guardare la strada, sembra più facile per i figli parlare apertamente con i genitori).

1. Che cosa fanno i tuoi amici online? Questa domanda allontana l'attenzione da tuo figlio e la sposta verso le attività in rete svolte in generale dalla sua cerchia di amici o compagni. È un buon modo per cominciare in maniera neutra e generica. Il tuo scopo è che tuo figlio ti dia un riscontro sincero e devi rassicurarlo rispetto al fatto che non sarà punito per le risposte che ti darà. Comincerà a parlare di attività come giocare, chattare, creare reti sociali, anche svolgere compiti e ricerche.

2. Quali sono i siti più giusti o più nuovi? Chiedi a tuo figli di dirti perché questi siti sono giusti. Puoi anche informarti su quali siti non sono più in auge e perché.

3. Puoi mostrarmi i tuoi siti preferiti? Proprio così, voglio che dedichi 20 minuti della tua vita terribilmente frenetica a guardare pinguini che scivolano giù da una collina innevata o il guerriero avatar di tuo figlio che brandisce la spada. Chiedi come si fa a impostare i parametri di sicurezza o di privacy (cerca queste aree in alto o in basso sullo schermo). Magari sarai tentato di giocare e d'impostare un tuo account. (Se lo fai, fallo sapere a tuo figlio). Chiedi a tuo figlio come usa il sito e perché lo preferisce rispetto ad altri.

4. Hai sentito parlare di 'bullismo informatico' e lo hai mai subito quando sei connesso? Forse tuo figlio non conosce il termine 'bullismo informatico', ma sa come avviene e che effetto fa. Raccontagli storie che hai letto o visto nei notiziari in merito a e-mail sgradevoli, foto imbarazzanti o dati personali divulgati o inviati ad altri bambini. Fagli domande sui falsi profili nelle social network. Scopri se tuoi figlio ha mai sentito parlare di queste cose. Accertati che sappia che il bullismo informatico è incredibilmente diffuso e che, se non lo ha ancora subito, è solo questione di tempo prima che accada. Fai in modo che sappia come reagire se succede (non deve rispondere a e-mail o messaggi instantanei che contengono forme di bullismo informatico, ma deve cercare di stamparli per mostrarli a qualcuno; deve bloccarli, se sa come fare, e soprattutto deve SEMPRE parlarne a mamma e papà o a un altro adulto di fiducia.)

5. Ti è mai successo di sentirti strano, triste, impaurito o a disagio per qualcosa che hai visto in rete? È un'occasione per discutere di bullismo informatico, scoperte accidentali fatte durante la navigazione (come siti pornografici o razzisti) o fatti strani che coinvolgono amici o compagni. Lo scopo è accertarti che tuo figlio sappia di potersi sempre rivolgere a te senza essere punito quando gli succede qualcosa di strano o di brutto durante la navigazione. Quando si opera su Internet è quasi inevitabile imbattersi in qualcosa di negativo. Fai in modo che tuo figlio sappia di poterti chiedere aiuto senza suscitare in te una reazione eccessiva.

Altre domande per genitori con figli più grandi:

- Conosci veramente tutti gli 'amici' della tua lista?
- Sai come usare e impostare i parametri di privacy e sicurezza? Mi fai vedere come si fa?
- Ricevi mai messaggi da estranei? Se sì, come li gestisci?
- Conosci qualcuno che abbia programmato d'incontrare dal vivo persone con cui ha parlato online?
- C'è qualcuno nel tuo gruppo di amici che si comporta scorrettamente in rete o al telefono? Se sì, cosa fa? Qualcuno si è mai comportato male con te? Se fosse successo, me lo diresti?
- Talvolta i bambini scattano foto sexy o di nudo e le inviano ad altri. È mai successo nella tua scuola o con qualcuno che conosci?

Ecco, questo è "il Discorso". Non è difficile, non è tecnico, è perfettamente fattibile e spero che proverai a farlo. Se sei un insegnante puoi provare a inserirlo in una discussione con la classe.

Aspetti fondamentali

Nel parlare di rischi legati a Internet, vedrai che ne esistono fondamentalmente di tre tipi: criminalità informatica, problemi interpersonali e questioni legate a reputazione e privacy. Nelle prossime pagine della presente guida, parleremo degli aspetti che concorrono a creare ciascun tipo di rischio, ma forse ti sarà utile pensare ai problemi in rete come causati da "estranei malvagi," "persone che conosci" e "errori commessi da te."

La criminalità informatica è vera criminalità

La criminalità informatica è un fenomeno reale, mondiale e in crescita. Norton ha condotto vari studi e intervistato migliaia di adulti e bambini in tutto il mondo, scoprendo che 2/3 di tutti gli adulti hanno già subito qualche atto di criminalità informatica[2], ad esempio sotto forma di virus, worm, Trojan Horse o altro malware, oppure truffa, deviazione di rete sociale o sottrazione di account di posta. Norton offre numerosi strumenti per combattere la criminalità informatica, ma il passo più importante da fare è installare un buon software di sicurezza su tutti i computer prima ancora di connetterti.

Virus, worm e spyware

I virus informatici esistono da più di 25 anni in varie forme, ma con la diffusione di e-mail e scambio di file via Internet, la loro incidenza è aumentata enormemente. I creatori di virus e di altre forme di codice maligno o "malware" erano soliti farsi in quattro per dimostrare la loro abilità con il software o vantarsi con gli altri. A quell'epoca i virus erano dunque creati per la "Fama". Ma oggi la posta in gioco è molto più alta e molti dei vecchi "cattivi" sono oggi in realtà veri e propri criminali informatici internazionali motivati dal profitto finanziario ottenuto attraverso le attività illegali. Siamo dunque nell'era della creazione di virus a scopo di lucro. Secondo le stime di alcuni analisti della sicurezza, un criminale informatico riesce a guadagnare svariate migliaia di dollari all'anno attraverso le sue attività.
Il tipo di malware più recente, emerso nel 2010, dimostra la possibilità di causare problemi nel mondo reale attaccando le infrastrutture fisiche. Il worm "Stuxnet" ha questa capacità. I dettagli dell'attacco sono ancora da chiarire, ma secondo le stime le vulnerabilità hanno permesso agli aggressori di sottrarre progetti riservati e documenti d'uso di sistemi industriali come quelli utilizzati dal settore dell'energia. L'incidente di Stuxnet rappresenta un caso reale di come si può verificare questo tipo di attacchi informatici strutturati a sistemi infrastrutturali critici.

In ogni caso, questi attacchi mirati non sono rivolti agli utenti comuni. Devi invece preoccuparti per il malware, come spyware, keystroke logger e bot, che ti può provocare gravi danni. Spyware e keystroke logger monitorano la normale attività svolta sul computer e inviano i tuoi dati riservati via Internet ai criminali. Link pericolosi contenuti nella posta, nei messaggi istantanei o nelle reti sociali possono installare tacitamente malware sul tuo computer o indurti a visitare siti che lo ospitano. Per garantire la sicurezza dei computer tuoi e dei tuoi figli, puoi installare un software di sicurezza e tenerlo aggiornato con le ultime funzioni di protezione. Raccomanda ai tuoi figli di non disattivare lo scanner per i virus o il firewall, anche se pensano che possa velocizzare un gioco. È un rischio da evitare.

[2] Fonte: Norton Cybercrime Report, www.norton.com/cybercrimereport

Scamware

Lo scamware (antivirus falsi o contraffatti) è un tipo di malware in grado di compromettere tanto il computer quanto il portafoglio. In genere il problema inizia quando un innocente navigatore s'imbatte in rete in uno strano pop-up pubblicitario che simula un messaggio di sistema operativo o un avviso di presenza di virus nel computer. Il messaggio indica che il computer "ha rilevato un virus" e ti invita a far partire lo scanner per trovarlo. Molti seguono le istruzioni credendo che l'avviso sia autentico. I bambini, in particolare, sono vulnerabili a questa minaccia, perché spesso credono di aiutare i genitori "eliminando il virus".

Quello che succede dopo è pura genialità criminale. La "scansione" ti mostra che il computer è infettato da molti elementi e ti dice di acquistare gli strumenti per la pulizia. Molti ci cascano e scaricano un file pericoloso contenente altro malware, rivelando nel frattempo i dati della propria carta di credito ai truffatori. Lo scamware o l'antivirus contraffatto devia poi il computer impedendo al software di sicurezza installato di funzionare e all'utente di cercare aiuto via Internet. E probabilmente a questo punto la tua carta di credito sia già in vendita sul mercato nero internazionale.

Fai in modo che né tu né i tuoi figli subiate queste truffe pericolose. Se avete un computer infetto, Norton vi può aiutare grazie a uno strumento gratuito, Norton Power Eraser (**http://it.norton.com/support/DIY/**), studiato per eliminare questi codici maligni. Se il tuo computer è così compromesso che non puoi accedere a Internet, dovrai scaricare il software da un secondo computer (chiedi a un amico), per poi trasferirlo su un disco o una chiavetta. I tecnici di NortonLive sono eventualmente a tua disposizione (in questo caso a pagamento) per svolgere l'operazione al tuo posto ed eliminare il virus.

Un discorso serio sui bot

La sai quella dei robot che assumono il controllo di tutti i computer del mondo? Non è una barzelletta. "Bot" e "botnet" sono gravi minacce per la nostra sicurezza in rete. I bot (abbreviazione di robot) sono forme di software nascosto in grado di penetrare nel computer e indurlo a inviare e-mail di spam e di phishing. Sono così diffusi che, secondo una stima del Security Response Center di Symantec, l'11% dei computer negli Stati Uniti sono già infetti.

Molte attività illegali prosperano grazie ai bot che si diffondono come un rogo, sfruttando la potenza di calcolo di centinaia di migliaia di personal computer ignari al solo scopo di rubare dati personali e truffare l'utente rubandogli soldi guadagnati con fatica.

Come fanno? Un bot è un tipo di software maligno, che si insinua nella macchina a opera dei criminali informatici e permette loro di assumerne il controllo. Questi "Web robot" fanno solitamente parte di una rete di macchine infette utilizzate per svolgere una serie di mansioni automatiche, quali la diffusione di virus, spyware, spam e altri codici maligni. Come se non bastasse, i bot vengono utilizzati per rubare dati personali e possono compromettere la tua situazione creditizia attraverso l'uso non autorizzato di carte di credito e conti bancari. Possono infine visualizzare siti web contraffatti facendoli passare per veri, e indurti a trasferire fondi e a rivelare user name e password che verranno utilizzati per altre attività illegali.

La migliore difesa da questi orribili piccoli bot è installare un software di sicurezza di qualità e impostarne con cura i parametri affinché si aggiorni automaticamente per fornire sempre il livello di sicurezza più completo. Gli esperti consigliano inoltre di non cliccare mai su allegati o link contenuti nelle e-mail, a meno che tu non ne conosca la fonte, un'altra cosa importante da insegnare ai bambini. Una volta infettati con un bot, questi subdoli programmi cercano di nascondersi dal software di sicurezza; è pertanto necessario visitare il sito Norton e scaricare appositi strumenti gratuiti per rimuoverli.

Dati personali e furto d'identità

I tuoi figli non sanno automaticamente che cosa sono i dati "personali". Sta a te spiegare loro il concetto che si tratta di qualsiasi dato che permetta a un estraneo di accedere a informazioni personali o finanziarie. I dati personali comprendono dati reali quali nome, numero di telefono, indirizzo, cognome da nubile della madre, circolo sportivo, scuola, persino il nome del medico. I cattivi possono trasformare anche un minimo indizio in un rapporto completo su genitore e figlio, vendendo poi dati personali a fronte di un profitto. È facile per questi individui richiedere un credito a nome di tuo figlio e acquistare merci o procurarsi denaro vero, rovinando nel contempo la tua credibilità, il tuo buon nome e quelli di tuo figlio.

Problemi interpersonali

Internet connette tra loro le persone in modi che non avremmo neppure immaginato fino a qualche anno fa. E con tutte queste connessioni e nuove forme di comunicazione, pochi attori sleali possono rendere la cosa particolarmente sgradevole e dolorosa per molti di noi. L'anonimato stesso garantito da Internet

offre una libertà d'espressione che va spesso oltre ogni limite, provocando guai e sofferenze. Fortunatamente la maggior parte dei giovani sono intenzionati a comportarsi correttamente online e offline. Con un poco di educazione alla sicurezza di Internet possiamo aiutare i nostri figli a imparare quali sono i modi giusti per navigare e come comportarsi con persone poco corrette. I cosiddetti problemi "interpersonali" che s'incontrano su Internet sono, ad esempio, bullismo informatico, furto di password e "sexting".

Bullismo informatico e stalking informatico

La tecnologia mette a disposizione dei nostri figli molti modi per connettersi, socializzare e creare. Purtroppo alcuni di loro usano e-mail, messaggistica istantanea, foto sul cellulare e messaggi di testo per mettere in imbarazzo o molestare gli altri bambini. Inoltre i loro messaggi digitali possono essere modificati per alterarne il significato, e in seguito inoltrati ad altri per metterli in imbarazzo, intimidirli o insultarli. Non succede spesso che i bambini riferiscano le loro esperienze di bullismo informatico, pertanto è difficile disporre di statistiche affidabili sul problema. Secondo BeatBullying (un'organizzazione inglese dedita a combattere il bullismo virtuale e reale), il 50% dei bambini hanno subito questo fenomeno in rete[3]. La maggior parte degli studi americani valutano 1 su 5 il numero di bambini soggetti regolarmente a episodi di bullismo informatico.

Accertati che tuo figlio sappia di doversi guardare anche dal messaggio di testo più banale e di dover curare attentamente quanto scrive lui stesso. Non deve mai comportarsi da bullo informatico e deve sempre riferirti se e quando subisce atti di bullismo.

ATTENZIONE: Se tu o tuo figlio siete oggetto di bullismo informatico non rispondete. La risposta dà al bullo la reazione che cerca, mentre il silenzio lo confonde. Se chiede a tuo figlio "hai visto quel post o messaggio?" insegnagli a dire che non l'ha visto, oppure anche "Ieri sera mia madre lavorava sul mio computer. Forse l'ha visto lei."

[3] http://www.ncpc.org/resources/files/pdf/bullying/Teens%20and%20Cyberbullying%20Research%20Study.pdf

Conserva una copia di eventuali messaggi provenienti da bulli utilizzando il tasto “Stampa schermata” sulla tastiera e copiandoli nel programma di elaborazione testi. Non si sa mai quando a un funzionario della scuola o della legge potrebbe tornare utile un rapporto completo degli eventi.

Se opportuno, segnala l’atto di bullismo informatico al sito, al provider, alla scuola ecc. Se l’azione coinvolge i bambini a scuola, lo puoi segnalare al preside, a un insegnante, a un consulente scolastico o al personale dell’ufficio della scuola.

Alcune scuole oggi dispongono di una politica per affrontare il bullismo informatico che illustra esattamente come avviene. Se il bullismo comporta minacce di ulteriori violenze, potrebbe essere opportuno rivolgersi alla polizia, che spesso ti può aiutare a contattare i gestori del sito per far eliminare il materiale offensivo. In ogni caso dovrai gestire il tutto in maniera molto decisa, senza sottovalutare il problema.

Le scuole stanno cercando di rispondere alla crescente diffusione del bullismo informatico creando politiche e attività per affrontare il problema. Il tragico suicidio della teenager americana Megan Meier come conseguenza, tra l’altro, di questo fenomeno ha fatto molto scalpore in tutto il mondo. Storie che legano il bullismo informatico a suicidi tra gli adolescenti hanno recentemente riguardato anche paesi europei. È importante ricordare che, per quanto una situazione di bullismo informatico sia grave, raramente il suicidio è dovuto a un’unica causa o a un unico evento. Se ti capita di vedere un commento online da cui sembra che l’autore stia pensando al suicidio, prendilo sul serio e denuncialo alle autorità, all’host del sito o al servizio. Se un bambino o un adulto sono in cerca di aiuto sul tema possono contattare le autorità specifiche.

Ovunque ci siano un bullo online e un obiettivo, ci sono anche osservatori silenziosi che assistono alla molestia e che la rendono ancora più potente grazie alla presenza del pubblico. Fai in modo che tuo figlio sappia di non dover mai farsi coinvolgere in atti di bullismo informatico, anche se gli chiedono solo di visitare un sito, aprire un’e-mail, inoltrare un messaggio offensivo o aggiungere commenti a una pagina di una social network. Dai a tuo figlio tutte le informazioni necessarie per rispondere a un obiettivo o a una vittima con gentilezza, comprensione e

amicizia. Quanto fa bene chiamare una persona che sta subendo atti di bullismo informatico solo per dire “Ho visto cosa ti hanno fatto. Sono stati cattivi e mi dispiace.”

Lo stalking informatico rappresenta un’estensione pericolosa del bullismo ed è compiuto da coloro che lo praticano anche nel mondo reale o “offline”. Secondo il Ministero della Giustizia americano, una donna americana su 12 è destinata a subire atti di stalking nel corso della vita. Dalla British Crime Survey è emerso che il 23% delle donne riferiscono di subire atti di stalking dall’età di 16 anni. Anche in Italia il fenomeno è in allarmante crescita e sempre più spesso occupa le pagine di cronaca di giornali e notiziari televisivi con casi limite . Conoscendo il problema, i nostri adolescenti più grandi possono imparare a difendersi e i genitori devono sapere come aiutarli. Lo stalker può deviare un account di posta e fingersi il titolare dello stesso, oppure può cancellare una pagina di social network o inviare messaggi di odio agli amici della vittima, commettere un furto d’identità vero e proprio o cercare di distruggere il credito e la reputazione di una persona.

Lo stalking informatico può essere pericoloso e deve essere denunciato alle autorità, ai service provider di Internet e agli host dei siti. Conserva tutte le prove sia dello stalking sia del bullismo informatico.

Come proteggere le password

Quando parlo con i bambini nelle scuole, spesso chiedo loro se abbiano mai visto qualcuno usare la loro password o modificarla senza il loro permesso. Anche tra i bambini di soli cinque o sei anni anni, molti alzanono la mano. Succede spesso che i bambini ripongano male la loro fiducia, anche quando si tratta di buoni amici o fratelli. Anche se è inteso come scherzo, questo fa sì che gli account dei piccoli vengano gestiti nel modo sbagliato, che i loro dati vengano divulgati e che le loro reti sociali siano utilizzate per fare guai. Disconnettersi è un altro modo efficace per far sì che nessuno possa accedere ai nostri account. Mio figlio lo ha scoperto dolorosamente una volta che ha dimenticato di disconnettersi dalla social network a casa di un amico, e quest'ultimo ha pubblicato commenti volgari sulla sua pagina!

Insegna ai tuoi figli a usare password che solo tu conosci. Considera prioritarie le password per la posta e le social network e rendile più complesse ed esclusive. Evita di utilizzare password facili da indovinare, come parole tratte dal dizionario, nomi o date che tuo figlio o un hacker potrebbero scoprire.

Ecco un buon modo per gestire le password. Scegli un'unica password principale che ricordi facilmente, poi personalizzala per i diversi siti. Il primo passo è scegliere una buona parola principale che abbia più di sei caratteri e varie combinazioni di lettere e numeri (anziché parole vere).

In questo caso proviamo a usare la frase inglese "I want to go to America" (Voglio andare in America). Riduciamola a ciascuna delle iniziali, usiamo il numero "2" al posto della parola "in" (in inglese "to", che si pronuncia come il numero "2", N.d.T.) e otteniamo "Iw2g2A". Poi aggiungiamo la prima e l'ultima lettera del sito (il sito di Symantec.com sarebbe: "SIw2g2Ac"). Questo trucchetto mi aiuta a ricordare tutte le diverse password e a mantenerle abbastanza complesse affinché neppure un hacker riesca a scoprirle. La sequenza ha senso per me ma non per gli altri. È utile anche usare password diverse per i diversi account. Se la password di un account viene compromessa, le altre sono comunque al sicuro.

Anche con password complesse ed esclusive è facile essere sopraffatti da quante ne dobbiamo usare in un solo giorno per accedere ai vari siti. Ci sono applicazioni per computer che gestiscono le password e alcuni browser sono in grado di salvarne diverse. È poco sicuro annotare le password in un elenco salvato nel computer, su fogli di carta accanto al computer e così via. Io uso Norton Identity Safe, una funzione di gestione password incorporata nel software Norton 360 e Norton Internet Security.

Come ho detto sopra, è opportuno assegnare password esclusive e complesse soprattutto a e-mail e social network, ma non ti sei chiesto perché? Se un hacker assume il controllo della tua posta, può cambiare tutte le altre password cliccando sul link "ho dimenticato la password" negli altri siti. E se assume il controllo della tua social network, può truffare o inviare link pericolosi a tutti i tuoi contatti.

Nota per i genitori: È importante che ti procuri la password della posta, della messaggistica instantanea e dei siti di social network di tuo figlio. In questo modo puoi sapere con chi comunica e, in caso di guai, disponi di una via di accesso importante.

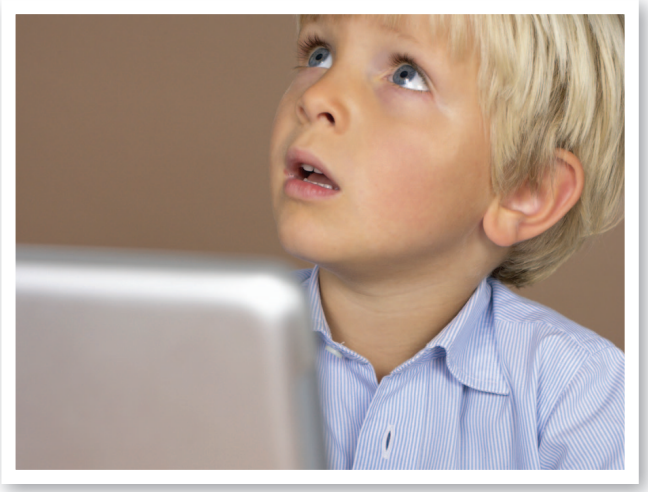
Predatori in rete

Statisticamente è improbabile che un predatore sessuale approcci tuo figlio in rete, ma questo è comunque un timore di molti genitori. Ogni volta che parlo con gruppi di genitori, mi chiedono di consigliare loro come tenere lontani i bambini dagli estranei in rete. Nel 2006, il Centro Nazionale per i Bambini Scomparsi e Sfruttati ha condotto uno studio negli Stati Uniti da cui è emerso che un bambino su 7 riceve sollecitazioni sessuali online, ma la maggior parte dei contatti provengono da altri bambini anziché da estranei, e non sono motivo di apprensione per il bambino stesso.[4] Una ricerca condotta da Norton in giugno 2010 ha rilevato che a un bambino inglese su 10 in rete capita che qualcuno che non conosce gli chieda d'incontrarsi offline.

Accertati che i tuoi figli sappiano che non devono mai scambiare e-mail, chattare o inviare messaggi di testo a estranei e che non è mai giusto incontrare un estraneo dal vivo. Fai capire loro che una persona che vedono o incontrano online è comunque un ESTRANEO, indipendentemente da quanto spesso lo vedono in rete.

[4] http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=40616

C'è apprensione soprattutto per l'eventualità che un bambino parli di sesso in rete con estranei, in quanto è dimostrato che questo sfocia ancora più spesso in un incontro dal vivo. Insegna a tuo figlio a segnalare a te o a un altro adulto di fiducia ogni richiesta di "E/S/L" che sta per "età, sesso e luogo" o qualunque cosa di simile.



Sexting

Il "sexting" è un fenomeno relativamente nuovo per cui un'immagine o un video di carattere sessuale vengono inviati per via telematica. In genere l'immagine è creata utilizzando la videocamera incorporata nel computer o quella del telefonino, poi viene inviata come messaggio multimediale (MMS). Secondo Pew Research, società di ricerca americana, il 4% degli adolescenti dotati di telefonino hanno inviato "sext" e il 15% li hanno ricevuti. Lo scopo di questo invio d'immagini di carattere sessuale viene descritto come una sorta di "valuta relazionale" impiegata per creare intimità, segnalare disponibilità o interesse affettivo. Lo studio di Pew suddivide gli scenari del sexting in tre categorie:

1. Scambi d'immagini esclusivamente tra partner di una coppia;
2. Scambi d'immagini tra partner che vengono poi condivise al di fuori della coppia;
3. Scambi tra persone che non hanno ancora una relazione, ma delle quali spesso una spera di averla.

Da una ricerca inglese condotta da Ofcom (aprile 2011) è emerso come il 29% dei bambini tra 12 e 15 anni abbiano saputo di qualcuno che ha pubblicato o inviato immagini imbarazzanti ad altri contro la loro volontà.

Puoi immaginare quali forze siano in gioco quando un gruppo di bambini popolari prende di mira un ragazzino meno forte per sollecitare un'immagine di carattere sessuale. Quest'ultimo di solito cede allo scopo di avvicinare un ragazzo, un gruppo o uno status sociale.

Il fatto più preoccupante è che l'immagine può essere considerata una forma di pedopornografia, il che pone sia chi l'ha realizzata sia chi la riceve in una situazione legalmente rischiosa. Una volta che la foto lascia il computer o il telefonino, non può più essere richiamata. Spesso le bambine ricevono pressioni dai ragazzi più grandi a scuola perché scattino queste foto in una sorta di episodio di confusione mentale. In Nuova Zelanda, una dodicenne è stata ricattata perché realizzasse queste immagini da qualcuno che aveva cancellato il suo account in un gioco online. La legge è al corrente di questa tendenza, ma è ancora incerta su come procedere. Il suo compito è bloccare la creazione di materiale pedopornografico, ma quando un bambino è sia il creatore sia una potenziale vittima, a volte è difficile decidere il passo successivo. Si comincia a notare un approccio più equilibrato da parte del sistema legale nell'affrontare queste situazioni, offrendo consulenza e servizi comunitari nei casi in cui, anche solo qualche mese fa, sarebbe stato previsto il carcere o l'iscrizione nel registro dei reati sessuali.

Navigare in sicurezza

Accertati che il tuo browser sia impostato per offrirti tutte le funzioni di sicurezza incorporate. Ad esempio, in Microsoft Internet Explorer (il browser più diffuso) i parametri di sicurezza e di privacy si trovano sotto "Strumenti" e "Opzioni Internet". Anche i motori di ricerca più usati, come Google, offrono funzioni di sicurezza. Ad esempio, SafeSearch di Google è studiato per rilevare i siti che riportano contenuti sessualmente espliciti e rimuoverli dai risultati della ricerca. Non esiste filtro che funzioni al 100%, ma SafeSearch aiuta a evitare contenuti sgradevoli in cui non vorresti che i tuoi figli si imbattessero.

SafeSearch è attivo automaticamente, il che aiuta a escludere le immagini esplicite dai risultati della ricerca. Se preferisci, puoi modificare i parametri impostandoli su un livello di filtro più alto per escludere, oltre alle immagini, anche i testi espliciti. Puoi modificare i parametri di SafeSearch sul tuo computer cliccando su Parametri di Ricerca in alto a destra nella home page di Google. Norton Online Family ti aiuta a impostare e a salvare parametri di ricerca sicuri.

Come mettere al sicuro la rete wireless

Le reti wireless domestiche pongono altri problemi di sicurezza, ma puoi fare molto per tenerle al riparo dalle intrusioni di estranei che potrebbero usare la tua banda o, peggio, far partire spam e altri attacchi dal tuo sistema. Inoltre, laptop e rete wireless permettono a tuo figlio di accedere a Internet da qualsiasi punto della casa, il che rende più difficile per te tenere sotto controllo le sue attività.

Se hai una rete wireless ("WiFi") a casa, fai tutto quanto è possibile per metterla in sicurezza: reimposta la password del router secondo le regole per una password efficace affinché non sia troppo facile da indovinare; abilita la codifica wireless per evitare che estranei identifichino la tua rete da Internet; limita l'accesso condiviso alla rete dal tuo sistema e aggiorna regolarmente il software di sicurezza. A casa mia, di tanto in tanto abbiamo usato i comandi del router per bloccare l'accesso ai laptop, alle console di gioco e ai lettori di musica abilitati al web dei bambini all'ora di andare a dormire, il che li ha aiutati a resistere alla tentazione di chattare e pubblicare post durante la notte. Alcuni genitori arrivano persino a disconnettere il router e a portarlo in camera con loro di notte. Qualunque cosa funzioni va bene.

Software di controllo parentale

Il software di controllo parentale ti permette di scegliere dove e quando tuo figlio si connette e di evitare che visualizzi materiale inadeguato. I controlli parentali sono diversi a seconda dell'applicazione che offre la funzione. Generalmente prevedono vari livelli per poter personalizzare il programma a seconda del bambino da proteggere. Ad esempio, per un bambino di cinque anni puoi creare una "lista bianca" di siti preselezionati e approvati che intendi permettergli di visitare.

Puoi anche creare account che richiedono il login di un genitore per permettere al bambino di navigare in rete, oppure puoi impostare limiti di tempo. Ai bambini più grandi e agli adolescenti puoi concedere un accesso più ampio e una maggiore flessibilità. Puoi limitare l'accesso alla rete per categorie di siti all'interno del programma per evitare di esporli a materiale razzista, pornografico o comunque non raccomandabile, e infine puoi anche provare il nostro programma gratuito Norton Online Family.

Norton Online Family è un servizio di sicurezza per famiglie, che funziona sia su PC sia su Mac ed è disponibile in 25 lingue. Quello che adoro di questo programma è la sua facilità d'uso. È stato veramente studiato pensando all'"uomo comune". Lo puoi installare su tutti i computer di casa, poi connetterti da qualsiasi punto, anche dallo smartphone. Puoi fissare limiti al tipo di siti a cui ogni bambino può accedere, personalizzarli con limiti di tempo, monitorare le attività di social network e le ricerche e visualizzare la cronologia. Dal momento che le informazioni sono salvate "nel cloud", tuo figlio non può nascondere quello che fa cancellando la cronologia.

Il nostro comitato consultivo di esperti comprende pedagogisti, legali ed esperti di sicurezza online, e persino un "giovanista" (ovvero un esperto di giovani), che collaborano con il nostro team Norton Online Family per progettare un programma potente ma flessibile. Obiettivo del team è favorire la comunicazione tra genitori e figli. Infatti non puoi usare il programma per spiare tuo figlio, dal momento che è sempre visibile a lui e compare ogni volta che il computer viene avviato e come icona nella barra strumenti. Auspichiamo che i genitori s'impegneranno a spiegare ai bambini come funziona e cosa possono vedere, e a concordare insieme le regole d'uso. Dal momento che Norton Online Family è gratuito, perché non lo provi? Per creare un account, basta visitare il sito **http://it.norton.com/family-resources/** e registrarsi. Ricorda però che non esiste software che protegga da tutti i possibili rischi legati a Internet. È necessario mettere in campo una combinazione di software, educazione, controllo e comunicazione per proteggere i propri figli, indipendentemente dall'età. Il Web è una risorsa ricchissima e sfugge al proposito di bloccarlo completamente. I genitori devono parlare con i propri figli per fare sì che mettano in pratica le loro credenze, i loro principi morali e i loro valori ogni volta che navigano in rete.

Rischi

Plagio e truffe
È molto facile trovare guide online ai compiti per tutti i principali testi scolastici e molti siti offrono temi e tesi in vendita. Imbrogliare non è mai stato così facile, accessibile e allettante per i nostri figli. Ricorda a tuo figlio che è molto importante usare Internet solo per le ricerche. Spiegagli perché i contenuti generati dagli utenti come quelli offerti da Wikipedia® non sempre sono affidabili. Insegnagli a usare queste risorse online come punto di partenza e mostragli come trovare i siti di ricerca più credibili e affidabili.

Condivisione di file, download di musica e video
I bambini scoprono presto il piacere di condividere la musica e spesso è proprio nell'adolescenza che cominciano a sentir parlare di siti di condivisione, soprattutto di quelli gratuiti. Fai sapere ai tuoi figli quali sono i rischi dei siti e dei programmi di condivisione di file che, per definizione, permettono a estranei di accedere a parti del loro computer. L'uso di siti di condivisione file può esporre il computer e i dati a software "bot", spyware, keystroke logger, virus e altri codici maligni e pericolosi.

Una volta ho partecipato a un seminario legale in cui si dimostrava con quanta facilità si possono trovare documenti finanziari sensibili estratti dai più comuni siti di condivisione file semplicemente lanciando una ricerca. L'oratore ha aperto uno di questi programmi, ha inserito la frase "dichiarazione dei redditi" e nel giro di qualche secondo erano disponibili centinaia di dichiarazioni dei redditi reali. Ha cliccato due volte su una di queste e abbiamo potuto assistere alla divulgazione involontaria dei dati personali e finanziari del malcapitato. Inoltre, spesso è illegale scaricare musica o video gratuiti. Mostra a tuo figlio come scaricare legalmente musica e video da siti come iTunes® e Amazon.

Siti di social network
I siti di social network rappresentano uno dei fenomeni a più rapida crescita su Internet, per i bambini come per gli adulti, ma questo successo è favorito soprattutto dai ragazzini e dagli adolescenti. Il sito più conosciuto, Facebook, è arrivato all'incredibile numero di 800 milioni di iscritti. Tutte i social network offrono ai bambini un luogo dove incontrarsi online con amici vecchi e nuovi. Se usati con cautela, sono un ottimo modo per comunicare e condividere le proprie esperienze. Se usati in maniera sconsiderata possono invece, come qualsiasi altro sito, esporre amici, familiari e l'intera rete a malware, criminalità informatica e persino furti d'identità.

Insegna a tuo figlio a non pubblicare informazioni private o foto inappropriate o fuorvianti. Queste informazioni, una volta pubblicate, sono di dominio pubblico e possono essere salvate nei PC e nella cronologia altrui. Anche se le rimuovi, queste informazioni e queste foto rimangono sempre da qualche parte su Internet e nelle mani di persone che possono usarle e abusarne. Se a te o a tuo figlio viene chiesto di "eliminare il tag" su una persona o di rimuovere un commento o altro dato, dimostrate entrambi una buona conoscenza del galateo online e fatelo immediatamente.

I siti di social network permettono ai bambini di creare reti di amici che comunicano liberamente tra loro. Accertati che i tuoi figli non consentano a persone che non conoscono di entrare nelle loro reti. Devono mantenere riservate le loro pagine, affinché solo gli amici invitati li possano trovare nel sito. Rivedete insieme i parametri di privacy e sicurezza del loro account.

Tu e la tua famiglia dovete sempre usare cautela nell'accettare richieste di amicizia e dovete comunque non accettarle mai da persone che non conoscete. Questi estranei, una volta ammessi nella vostra rete, possono esporre voi e i vostri amici a malware e atti di criminalità informatica. Accertati che tuo figlio imposti correttamente i parametri di sicurezza per limitare la visibilità delle foto o dei video pubblicati sulla sua pagina, riducendo in tal modo anche la possibilità che un amico pubblichi una foto divertente ma imbarazzante, o faccia un commento non adatto a tutti. Il sito ConnectSafely.org offre alcuni consigli utili per impostare

correttamente i parametri di sicurezza nei siti di social network. Anche Facebook offre molti consigli utili per la sicurezza, come ad esempio registrare più indirizzi e-mail sullo stesso account o abilitare gli avvisi per i nuovi accessi. Per ulteriori informazioni sui metodi più nuovi per proteggere il tuo account, visita il sito **www.facebook.com/security.**

Un problema grave nel mondo delle social network è rappresentato dallo spam e dagli attacchi di phishing. Occorrono attenzione e cautela nel rispondere a strani messaggi o cliccare su link all'interno dei siti di social network. Nella maggior parte dei casi il software di sicurezza è in grado di bloccare i siti pericolosi a cui il link ti porta, oppure d'impedire il download di spyware, keystroke logger o altri codici maligni. Ma se un hacker assume il controllo della tua rete sociale, può indurre amici meno protetti a cliccare su link pericolosi o a visitare siti pericolosi. Le comuni truffe online in cui il truffatore finge di essere te per fare soldi grazie alla tua rete aumentano grazie alla loro efficacia. Se nel tuo news feed trovi link che sospetti essere spam, eliminali subito e contrassegnali come spam per proteggere anche gli altri. Norton Safe Web è uno strumento gratuito a disposizione su Facebook in grado di effettuare la scansione di tutti i link presenti sulla tua pagina di Facebook per rilevare quelli potenzialmente pericolosi.

Siti di pornografia, gioco d'azzardo, razzismo, anoressia e istigazione all'odio

Gli angoli più bui del mondo di Internet ospitano elementi pericolosi e illegali. Dalle ricerche è emerso che la maggior parte dei bambini di 11 anni hanno già visto materiale pornografico in rete.[5] Senza controlli parentali o filtri di navigazione è quasi inevitabile che tuo figlio si imbatta in qualcosa che lo può turbare. Accertati che tuo figlio ti dica se e quando succede e rassicuralo rispetto al fatto che non ti arrabbierai se lo farà. La cosa più importante è affrontare il problema ed evitare che si ripeta.

Alcuni bambini e adolescenti sono curiosi dei siti che contengono messaggi razzisti o di odio, o che promuovono comportamenti rischiosi o dannosi come l'anoressia e il "cutting". Lo puoi scoprire solo parlando regolarmente delle loro motivazioni nel visitare questi siti. Se durante la conversazione tuo figlio rivela problemi come depressione o autolesionismo, rivolgiti senza indugio a un terapeuta professionale o ad altro specialista per affrontarli.

[5] http://news.cnet.com/8301-17852_3-20006703-71.html

Reputazione digitale

La tua reputazione digitale è l'impressione che crei quando la tua vita viene visualizzata attraverso i risultati di un motore di ricerca. I notiziari parlano spesso di bambini che hanno pubblicato informazioni online causando danni scolastici, finanziari o affettivi. Uno studente di una scuola secondaria americana ha pubblicato una sua foto con in mano una bottiglia di birra, il che gli è costato la perdita di una borsa di studio. Un dipendente ha pubblicato commenti sul capo in una social network ed è stato licenziato. Anche se tuo figlio fa attenzione a ciò che pubblica, è importante che tu esamini le sue attività online per capire se qualcosa che ha detto, caricato o commentato possa nuocergli in futuro. Non è mai troppo tardi per modificare i parametri di sicurezza del social network o per cancellare commenti, foto, video e messaggi offensivi, puerili o semplicemente sciocchi se visualizzati da un estraneo.

A volte è difficile eliminare elementi da altri siti o evitare che compaiano tra i risultati delle ricerche. Vale comunque la pena di vedere com'è la tua reputazione online e fare in modo che sia corretta. Se sei bravo nello sport, fai in modo che i tuoi risultati siano visibili in rete. Se hai vinto una gara di oratoria, pubblica un video in un sito di condivisione e taggalo con il tuo nome. Hai raccolto fondi per un ente di beneficenza partecipando a una maratona? Bravo, assicurati che nel sito il tuo nome sia scritto correttamente. In questo modo puoi essere certo che i primi risultati che compaiono su di te sono positivi e che spingono eventuali elementi negativi più in basso nella lista dei risultati.

Privacy online degli adolescenti

Insegna a tuo figlio adolescente a usare Internet. A questo punto è (o dovrebbe essere) abbastanza informato per sapere che le persone connesse non sempre sono chi dicono di essere. In rete è facile mentire su età, sesso e luogo, così molti lo fanno per motivi innocenti e non. Ricorda continuamente a tuo figlio che non si deve fidare degli estranei incontrati in rete più di quanto non si fidi nei contatti faccia a faccia. Non deve mai ammettere un estraneo nella lista degli amici, né permettergli di partecipare a una conversazione in chat o MI (messaggistica istantanea) , e non deve mai accettare software gratuito, suonerie o salvaschermo da estranei.

Ricorda a tuo figlio che indirizzi e-mail, nomi utente e nomi usati nella messaggistica istantanea non devono mai contenere il loro vero nome, il nome della loro scuola o una combinazione tra i due; non devono neppure essere provocatori o altrimenti invitanti per i predatori, ma devono essere più anonimi possibile. Inoltre non deve mai rivelare le sue password, neppure agli amici. Può apparire ovvio, ma gli adolescenti più grandi tendono a scambiarsi le password come prova di "amicizia". Pessima idea!

Accertati che il sito della scuola di tuo figlio sia protetto da password o richieda un login per le informazioni meno pubbliche e superficiali. Ad esempio, una scuola nella mia città ha pubblicato nel proprio sito un piano di viaggio con informazioni sui voli e i nomi degli studenti partecipanti a una gita per una gara sportiva. Altri problemi possibili riguardano gli elenchi di nomi, indirizzi e numeri di telefono degli studenti pubblicati nel sito.

E-mail

Bambini e adulti dovrebbero avere indirizzi e-mail diversi per scopi diversi. Ad esempio, è una buona idea avere un indirizzo per lo shopping online, un altro per l'online banking e un altro ancora per la corrispondenza con amici e parenti. In questo modo, ad esempio, se ricevi un avviso dalla tua banca all'indirizzo dedicato ai parenti, saprai che si tratta di spam da cancellare.

Accertati che gli account di posta di tuo figlio siano impostati sul massimo livello di filtro dello spam. Secondo una ricerca di Norton, l'80% dei bambini riferiscono di ricevere spam quotidianamente. Il nuovo Norton Cybercrime Index, uno strumento gratuito per valutare il rischio attuale di subire un attacco di criminalità informatica, riferisce che lo spam costituisce regolarmente circa l'80% delle e-mail inviate nel mondo. Se tuo figlio non è abbastanza grande per ignorare o cancellare lo spam (che in alcuni casi può riportare immagini e contenuti fortemente offensivi), non consentirgli di gestire da sé il proprio account. Non pubblicare online il tuo indirizzo e-mail per evitare che venga preso di mira da uno spammer. Inserisci il tuo indirizzo online come "nome presso isp punto com". Ad esempio, il mio indirizzo sarebbe "marian presso Norton punto com."

Occorre usare molta cura nel creare un account di posta per un bambino. Scegli un nome che non consenta agli estranei di trovarlo. Digli di non usare combinazioni tra nome e cognome e neppure nomi o indirizzi suggestivi, quali "sexylexy" o "selvaggio", anche se sembra "figo" farlo. Accertati che usi password efficaci e che non le riveli a nessun altro oltre ai genitori. Devi conoscere le password degli account di tuo figlio per poter tenere sotto controllo la sua attività. Guarda a chi manda mail e da chi ne riceve. Conosci tutti? E fai sapere a tuo figlio che, se lo fai, è per proteggerlo e non perché non ti fidi di lui.

Messaggistica istantanea

La messaggistica istantanea (MI) non è una funzione nuova ma è diventata più ostica ai genitori semplicemente perché è contenuta nelle social network e pertanto è meno facile da monitorare. Forse non riuscirai a tenerne traccia, ma dovresti comunque prendere in considerazione alcuni servizi, quali Norton Online Family o quelli offerti dal tuo gestore di telefonia mobile.

RACCOMANDAZIONI IMPORTANTI

- Insegna a tuo figlio a non cliccare sui link contenuti nelle e-mail ricevute, dal momento che possono dirigerlo verso siti contraffatti. Inoltre non deve mai accettare un link né scaricare un file attraverso la messaggistica istantanea.
- Disabilita la funzione anteprima nell'e-mail per evitare l'esecuzione di eventuali codici maligni contenuti nel messaggio.
- I bambini non devono rispondere a e-mail o messaggi istantanei inattesi provenienti da persone che non conoscono.
- Non devono rendere pubblico il loro profilo di messaggistica istantanea o social network.
- Imposta le preferenze dei messaggi per controllare l'accesso di estranei.
- I bambini non devono consentire ai siti di mostrare quando sono connessi o di visualizzare la loro ID o i loro dati personali sulle pagine che visitano.
- Quando non usano la MI o quando modificano la pagina di social network servono sempre disconnettersi per proteggere la propria privacy.

Sicurezza dei telefoni mobili

Una volta promosso alla scuola secondaria, sicuramente tuo figlio ti chiederà (o pretenderà) un cellulare o uno smartphone. Dalla recente ricerca Ofcom Digital Literacy (aprile 2011) è emerso che il 65% dei bambini di 10 anni hanno già un proprio cellulare e la percentuale sale al 90% per i ragazzini tra i 12 e i 15 anni. Inoltre non è del tutto inconsueto che bambini di soli 6-9 anni ne abbiano uno, spesso dismesso da un fratello o da un genitore. La gamma di tipologie di telefoni e di servizi è così vasta che vale la pena d'informarsi bene prima di scegliere. Il solo fatto che tuo figlio dodicenne voglia un telefono non significa però che debba avere accesso illimitato a messaggi e rete.

Una volta ottenuto un cellulare, tuo figlio dovrà imparare come inviare i messaggi di testo. Lo studio americano Pew ha rilevato che il 54% dei teenager inviano messaggi di testo ogni giorno. La metà degli adolescenti maschi inviano 50 o più messaggi al giorno, mentre la media per le ragazze è di oltre 100 messaggi di testo al giorno. Lo studio di Ofcom in Inghilterra mostra un quadro leggermente diverso: le ragazze (12-15 anni) inviano in media 140 messaggi alla settimana. I bambini e gli adolescenti tra gli 8 e i 17 anni hanno largamente abbandonato l'e-mail come mezzo di comunicazione in favore degli sms e della messaggistica incorporata nella social network preferita. L'unico caso in cui un bambino usa il cellulare per telefonare è per chiamare i genitori. Alcuni usano ancora la messaggistica istantanea e la videochat del computer, ma anche questi servizi fanno sempre più solo parte della social network preferita e non sono tanto visibili come attività separata.

Se il cellulare di tuo figlio consente l'accesso a Internet, valuta l'eventualità di renderlo più sicuro. Puoi bloccare l'aggiunta di software spia o l'uso della funzione GPS (global positioning system) per individuare la sua posizione fisica, ma anche impostare le funzioni di blocco e cancellazione a distanza. Norton offre prodotti per la sicurezza degli smartphone, come Norton Mobile Security, disponibili nel sito **www.norton.com**.

RACCOMANDAZIONI IMPORTANTI:

- Imposta una password sul telefono/dispositivo per impedire l'accesso indesiderato.
- Installa un software di sicurezza per proteggere il telefono e i dati in caso di perdita o furto.
- Carica il dispositivo durante la notte in cucina per evitare l'invio di sms notturni o lo scatto di foto inappropriate con la fotocamera del cellulare.
- Informati sui servizi offerti dal gestore, come filtri di Rete, limiti di tempo, blocco di numeri e altri controlli parentali.

Sicurezza dei dispositivi mobili

Oltre al cellulare, i nostri figli hanno sempre in tasca potenti computer, quali ad esempio molti dispositivi di gioco dotati di web browser o tablet, come l'Apple® iPadTM. Le funzioni offerte da questi dispositivi sono impressionanti, ma è comunque necessario tenere in considerazione le minacce e i rischi per la sicurezza online, anche con strumenti che si usano soprattutto per leggere e giocare.

Imposta una password per tutti i dispositivi mobili per evitare che qualcuno vi installi spyware o acquisti applicazioni senza autorizzazione. Imposta filtri e controlli parentali, o sull'apparecchio o utilizzando la rete WiFi di casa. Installa un software di sicurezza per rilevare l'eventuale presenza di spyware o bloccare l'accesso non autorizzato. I router offrono vari modi per controllare l'uso della rete di casa da parte di questi dispositivi. Imposta limiti di tempo, filtra i siti per categorie e nega l'accesso agli utenti non autorizzati regolando i parametri del router.

Una tendenza che probabilmente si diffonderà prossimamente e da tenere in considerazione è la possibilità di fare acquisti utilizzando il dispositivo mobile. Una nuova tecnologia detta "near field communications" (comunicazioni di prossimità) permette di utilizzare cellulari e dispositivi mobili per fare acquisti inviando segnali di autorizzazione. Sono già disponibili applicazioni per un'ampia gamma di provider, che consentono di acquistare caffè, effettuare pagamenti individuali o svolgere attività di online banking, il tutto con un dispositivo mobile. Possiamo stare certi che i criminali informatici scopriranno presto come sfruttare

questo fenomeno, quindi fai attenzione quando effettui pagamenti mobili e tieni sotto stretto controllo i tuoi account. Ricorda inoltre che se passi a tuo figlio il tuo dispositivo mobile dotato di questo tipo di funzioni, lo metti in condizione di usare il tuo account senza autorizzazione.

Blog

Un blog è un giornale o un diario online. Puoi leggere il mio su **www.norton.com/askmarian**. Alcuni blog sono monotematici, dedicati a un argomento particolare. Spesso gli adolescenti hanno blog che assomigliano più che altro al tradizionale diario segreto, salvo che sono aperti a tutti su Internet attraverso il sito del ragazzo o un sito di social network, il che è come pubblicare il diario online perché tutto il mondo lo veda. Tuo figlio deve decidere qual è l'obiettivo del suo blog prima di realizzarlo. Di solito i motori di ricerca rilevano le informazioni pubblicate, il che vanifica i tuoi sforzi per proteggere la privacy. La privacy risulta compromessa anche quando nel blog pubblichi foto o link a siti privati.

Inoltre il blog risulta visibile ad alcuni soggetti, quali potenziali datori di lavoro o funzionari incaricati delle ammissioni nelle scuole, e questa esposizione può influire anche su altri aspetti della tua vita. Ad esempio, persone sottoposte a colloqui di assunzione sono state rifiutate a causa delle voci contenute nei blog personali o in quelli di amici e parenti che li menzionavano. Fai una ricerca online su di te e sui tuoi familiari. Se hai obiezioni su elementi pubblicati da altri, puoi e devi richiederne la cancellazione. Se si rifiutano, li puoi denunciare all'host del sito. Se l'elemento è offensivo o illegale, puoi anche rivolgerti alle autorità.

Foto digitali e privacy

Molti bambini hanno un telefono cellulare dotato di fotocamera e a volte anche una fotocamera tutta loro. Spiega a tuo figlio che è necessario proteggere le foto in rete dagli estranei, ma anche dagli amici che le potrebbero utilizzare in maniera inadeguata. Puoi tenere traccia dell'invio di foto digitali dal telefono (controlla la guida online o cartacea). Accertati che tuo figlio ti mostri le foto che ha sul telefono, affinché tu possa consigliarlo in merito a possibili rischi o a quanto non è corretto condividere. Se usi siti di condivisione foto, non permettere ad altri di usare le tue foto, in particolare quelle contenenti persone. In alcuni casi le foto contenute nei siti di condivisione sono state utilizzate a scopo pubblicitario senza

il consenso dell'interessato.

Molti telefoni cellulari e fotocamere digitali contrassegnano le foto con i dati del luogo in cui sono state scattate. Così facendo indichi dove ti trovavi quando la foto è stata scattata. Può essere un modo pratico per creare una mappa fotografica di una passeggiata in campagna o di un'escursione a una cascata lontana, ma non è una buona idea rendere pubblica la tua posizione per default in ogni immagine. Controlla i parametri della fotocamera o del telefono e disattiva la funzione di contrassegno delle immagini. E se tuo figlio usa un servizio di geolocalizzazione attraverso i social media o indica la sua posizione attraverso la rete sociale, spiegagli in quali problemi di privacy può incorrere.

RACCOMANDAZIONI IMPORTANTI:

- Disattiva i tag di geolocalizzazione sulle foto scattate con la fotocamera o il cellulare.
- Non rendere pubblici gli album di foto private.
- Chiedi ai visitatori di un sito di condivisione foto di utilizzare una password.
- Effettua il back-up delle foto con un apposito software perché guasti del computer, tagli di corrente, incendi o catastrofi naturali possono facilmente cancellare le foto e altri file dal computer.
- Usa solo servizi fotografici online che offrono una protezione della sicurezza.
- Quando un servizio fotografico online ti offre la possibilità d'inviare e-mail, proteggi la privacy dei tuoi amici inviando loro piuttosto un link al sito.

Acquisti online

Internet è il paradiso dello shopping, soprattutto per i teenager dotati di carta di credito o carta regalo prepagata (o di accesso alla tua). Vi sono tuttavia alcune regole che devono seguire per fare acquisti in sicurezza. Inizia la sessione di shopping online accertandoti che il software di sicurezza sia attivo e aggiornato. Acquista solo in siti noti e di buona reputazione, in quanto l'uso di un sito sconosciuto può essere pericoloso. Un modo per aumentare la sicurezza è verificare che ogni pagina in cui inserisci dati personali, come indirizzo o numero di carta di credito, sia codificata. Puoi capirlo in base all'indirizzo Web, che inizia con https. Un altro elemento da cercare è l'icona del lucchetto in basso nel riquadro del browser, che indica che il sito che stai visitando usa una codifica per

proteggere le tue comunicazioni.

Fare shopping in siti di buona reputazione è solo il primo passo per un'esperienza in rete sicura. Non cliccare sui link contenuti nelle e-mail per arrivare a un negozio o a una vendita preferita, ma digita l'indirizzo nella finestra del browser. In tal modo eviterai di subire attacchi di phishing, che ti trasferiscono a una versione contraffatta del sito del tuo negozio preferito. I phisher possono rubare password, login, dati della carta di credito e molto altro.

Controlla più spesso possibile - almeno una volta al mese - gli estratti conto della carta di credito. È il miglior modo per sapere chi usa la carta e per individuare i problemi prima che siano troppo difficili da risolvere. La società che emette la carta di credito offre una protezione del consumatore e ti aiuterà gestire eventuali addebiti contestati o non autorizzati. Non usare le carte di debito online. Le carte di credito offrono livelli supplementari di protezione, tra cui la possibilità di contestare addebiti dubbi, mentre con una carta di debito il denaro può essere prelevato da un conto bancario senza che nessuno se ne accorga fino all'emissione dell'estratto conto mensile. E talvolta ci vuole molto tempo per recuperarlo.

Operazioni bancarie e pagamento bollette online e mobili
Sempre più persone hanno dimestichezza con l'online banking. L'accredito diretto dello stipendio in banca è una buona misura di sicurezza, in quanto impedisce che qualcuno rubi l'assegno dalla tua casella di posta e velocizza l'accesso ai fondi. È anche una fonte di risparmio per il datore di lavoro. Alcuni siti offrono anche la possibilità di pagare le imposte online.

La tendenza più recente nel settore bancario è il mobile banking. Si tratta di numerose applicazioni per i dispositivi Apple e Android proposte dai principali istituti finanziari, che permettono di depositare un assegno con la stessa facilità con cui si scatta e s'invia una foto con il cellulare. Naturalmente i primi ad adottare questa tecnologia sono stati i più giovani, ma con la pratica sono certa che sempre più persone proveranno a usarla.

I criminali informatici sono pronti per approfittare di questi strumenti. Abbiamo già subito un'ondata di malware, come il Trojan Zeus che ha sottratto le credenziali

dell'online banking e rubato milioni di dollari dalle vittime. Alcuni programmi di malware si rivolgono ai gestori di piccole imprese ed enti di beneficenza, estraendo i dati dai siti per inviare messaggi di phishing mirati.

Presta attenzione alle attività di banking online come a quelle relative alle carte di credito. Controlla regolarmente le operazioni sull'estratto conto. Verifica che le bollette siano pagate puntualmente e per l'importo corretto. Proteggi il tuo computer come fai per internet in generale per evitare che ti rubino password o dati bancari e non accedere ai tuoi conti da computer pubblici, chioschi o connessioni wireless poco sicure. Digita sempre l'indirizzo Web della tua banca nel Web browser; non cliccare mai su un link contenuto in un'e-mail. Quando hai finito disconnettiti dall'account. Non salvare i dati di accesso al conto nel browser. Oggi molte banche offrono lettori di carte da utilizzare per le operazioni online. Per stare al sicuro online quando effettui attività di online banking la cosa migliore è utilizzare il lettore, e se non lo hai ancora ricevuto contatta la tua banca.

Gioco online e segnali di dipendenza
MMORPG. Che cos'è? È l'abbreviazione di "massive multiplayer online role-playing games", ovvero giochi di ruolo online con più giocatori, sempre più diffusi e potenzialmente in grado di creare dipendenza. A volte sono molto coinvolgenti e per alcuni adolescenti, soprattutto maschi, sono una fonte potente di distrazione dalla vita reale. Stabilisci insieme a tuo figlio la quantità di tempo da trascorrere in questi siti, se debba ricevere denaro da spendere per iscriversi o per acquistare accessori per il gioco (nel mondo reale, come nei siti di aste online o all'interno del gioco) e ogni altro aspetto tu ritenga opportuno.

Ecco alcuni sintomi fisici e psicologici di dipendenza:
- Incapacità d'interrompere l'attività.
- Tendenza a trascurare familiari e amici.
- Menzogne a datori di lavoro e familiari sulle attività.
- Problemi con la scuola o il lavoro.
- Sindrome del tunnel carpale.
- Secchezza oculare.
- Scarsa igiene personale.
- Disturbi del sonno o alterazioni del ritmo sonno-veglia.

Una parola conclusiva

Internet è una risorsa meravigliosa, dotata di elementi che spesso la fanno sembrare una vera e propria città. Offre istruzione, divertimento, notizie dal mondo e migliora la nostra vita grazie all'accesso a servizi incredibili, quali chat, e-mail, shopping online e molto altro. Se sei consapevole dei rischi e dei pericoli della rete e utilizzi un software di sicurezza aggiornato, puoi aiutare tuo figlio a navigare in questa stupefacente città cibernetica con un'autonomia sempre maggiore. Informati continuamente sulle nuove tecnologie e i problemi legati alla rete e fai sì che il tuo comportamento online serva da modello di ruolo per tuo figlio operando per primo in maniera sicura. Grazie!

Consigli utili per proteggere la tua famiglia in rete

- Installa un software di sicurezza su tutti i computer
- Non aprire e-mail sospette e non cliccare su link sconosciuti
- Ove possibile tieni in vista il computer e i cellulari
- Evita di utilizzare software di condivisione file
- Usa computer pubblici o reti WiFi con cautela
- Effettua il backup del tuo computer – vai su Internet con NortonTM Online Backup
- Fissa regole per l'uso di Internet
- Impara a usare le social network – iscriviti e imposta i parametri di privacy e sicurezza
- Aiuta i tuoi figli a proteggere i loro dati personali
- Crea password complesse ed esclusive e mantienile segrete
- Installa software di controllo parentale e controlla spesso la cronologia di Internet sul computer
- Stai con i tuoi figli quando sono connessi e fai loro regolarmente "Il Discorso"
- Insegna ai tuoi figli a informare un genitore, un insegnante o un adulto di fiducia se si sentono a disagio per qualcosa che hanno visto su un computer.

Marian Merritt

Marian Merritt

Marian è Responsabile della Sicurezza Online di Norton presso Symantec Corporation e fornisce informazioni sui problemi tecnologici che affliggono le famiglie. Marian traduce le questioni tecniche in un linguaggio facilmente comprensibile al pubblico e incontra periodicamente insegnanti, genitori e bambini per dare alla Società un'idea di ciò che succede oggi nel mondo di Internet e fornire a famiglie e scuole le informazioni necessarie per imparare a utilizzare questa tecnologia in maniera intelligente e sicura.

In passato, Marian ha svolto numerosi incarichi nell'ambito della gestione dei prodotti di consumo in Symantec. Risiede a Los Angeles, California, con suo marito e i suoi tre figli.

- Se vuoi ricevere altro materiale illustrativo e didattico
- Se sei vittima della criminalità informatica
- Se vuoi avere informazioni aggiornate sull'evoluzione delle minacce in rete

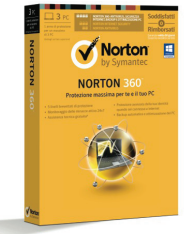
visita **www.norton.com/familyresource**.

Puoi leggere il blog di Marian su **www.norton.com/askmarian** e le puoi porre domande scrivendole all'indirizzo **marian@norton.com**.

Prodotti per la sicurezza Norton

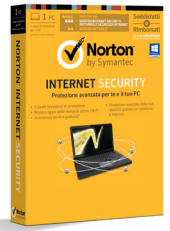
Norton 360™

Norton 360 offre a te, al tuo computer e ai tuoi file una protezione completa e facile da usare contro ogni minaccia. PC Tuneup sincronizza il computer e il back-up automatico previene la perdita di foto digitali e di altri file importanti.



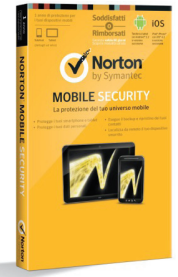
Norton™ Internet Security

Naviga, acquista, accedi ai social network online e fai online banking senza preoccuparti di virus e criminalità informatica. Norton Internet Security offre una protezione leggera e veloce che blocca le minacce e protegge la tua identità senza rallentare il PC.



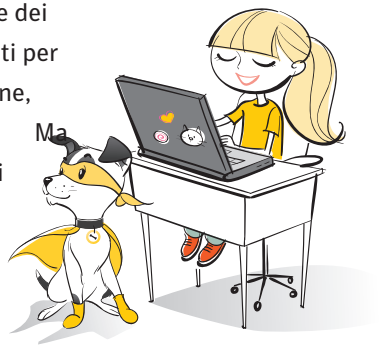
Norton™ Mobile Security

La tua vita è archiviata nel tuo telefono. Tieni al sicuro entrambi con Norton Mobile Security. La sua tripla protezione dal furto ti permette di disabilitare il telefono, cancellare i dati personali e persino ottenere le coordinate GPS del telefono in caso di perdita o furto, il tutto a distanza. Si scarica e si installa sul telefono con pochi click.



Norton™ Online Family

Un modo intelligente per garantire la sicurezza in rete dei tuoi figli. Norton Online Family ti fornisce gli strumenti per gestire le visite ai siti, quanto tempo trascorrono online, con chi parlano e quali informazioni condividono. Ma soprattutto ti aiuta ad aprire un dialogo positivo con i tuoi figli sulle buone abitudini in rete.



Norton Family Premier è la versione a pagamento di Norton Online Family. In più puoi bloccare o consentire i siti Web e i messaggi di testo e controllare le app installate attraverso lo smartphone Android dei tuoi figli. Ti permette inoltre di monitorare i video guardati sul Web dai tuoi figli e ricevere via e-mail i report sulle loro attività online settimanali o mensili.

Norton 360TM Multi-Device

Norton 360 Multi-Device fornisce in un'unica soluzione protezione efficace per tre dispositivi a tua scelta tra PC, Mac, Smartphone e Tablet Android, iPhone e iPad. Ti protegge dai virus e durante lo shopping online, localizza il tuo Android, iPhone e iPad e ti permette di archiviare i tuoi dati in modo semplice.

Guida alla Sicurezza Online per le Famiglie

di **Marian Merritt**
Introduzione di **Ida Setti**