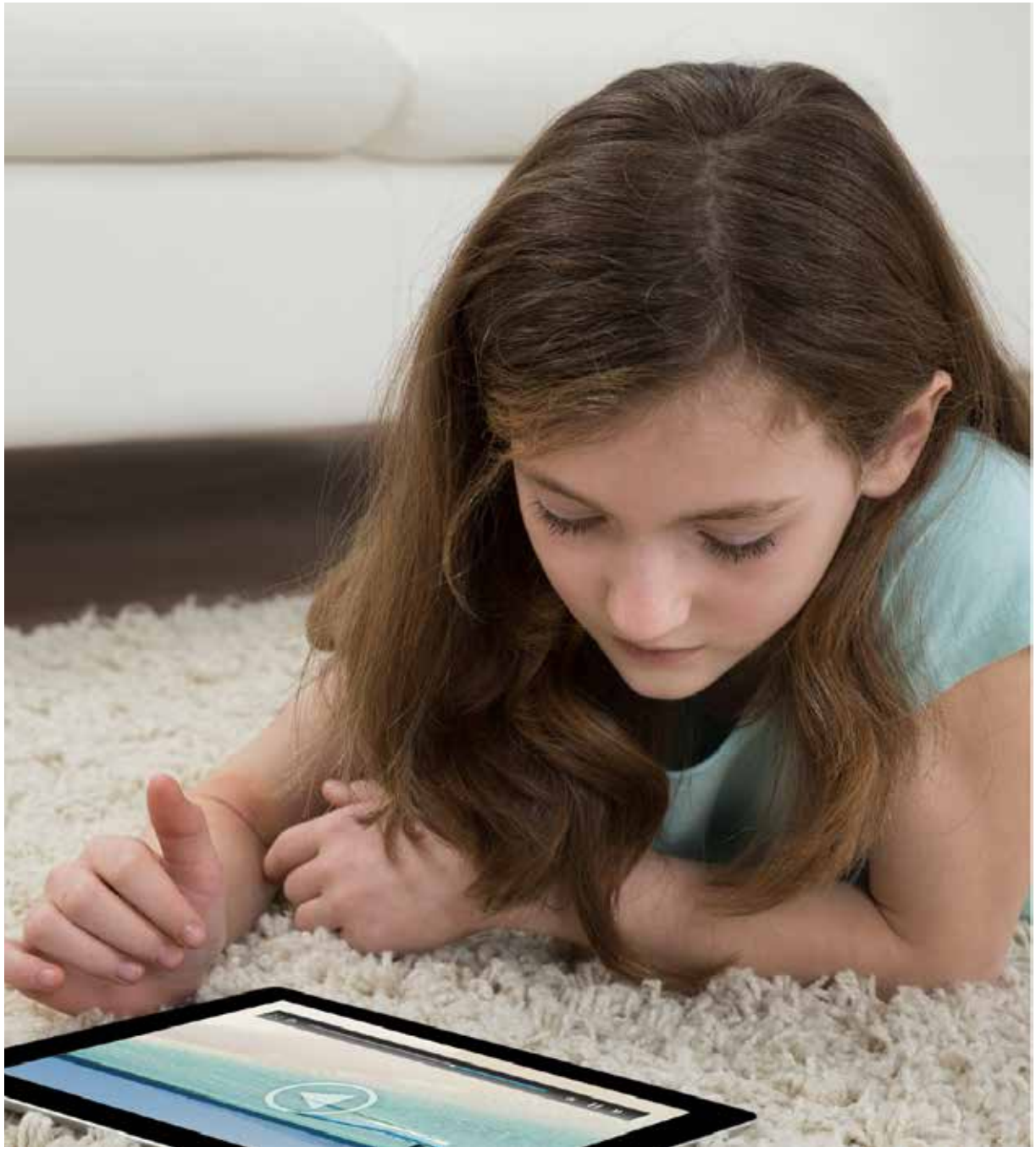
ENJOY SAFER TECHNOLOGY™

saferkidsonline

Internet più sicuro per i bambini - una guida per i genitori

Vite digitali

Molti di noi in ESET sono genitori come voi. Sentiamo l'esigenza di guidare i nostri figli nella vita e di proteggerli dal male, ma oggi questa responsabilità rappresenta una sfida enorme.
Con dispositivi mobili sempre più complessi, nuove piattaforme di comunicazione e un linguaggio online in rapida evoluzione, i genitori hanno molto da imparare per aiutare i loro figli.
Questa guida offre un aiuto e spiega cosa fare per far sì che i vostri figli possano usare internet in maniera sicura.



A chi spetta il compito di parlare con loro?

Non importa quanto questo possa mettervi a disagio, dovete essere voi.

I vostri figli incontreranno persone che avranno un ruolo molto importante nella loro vita, come parenti, amici e insegnanti. Eppure, nessuno di loro può sostituirsi al ruolo di genitore. Agli occhi di un bambino, siete voi che avete tutte le risposte e siete in grado di aiutarlo se non è sicuro di cosa fare dopo.

Quando si dovrebbe parlare con loro?

Ora!

Dal primo momento in cui un bambino mostra interesse per il vostro tablet, smartphone o computer, dovreste iniziare a spiegare come funzionano le cose. Ci sono molte regole che insegniamo ai bambini per tenerli al sicuro nel mondo reale. Ce ne sono altrettante per il mondo online. Mentre le minacce alla sicurezza si presentano in una forma diversa, il potenziale di danno è altrettanto reale.
Con l'aumentare dell'età, potrebbero presentarsi nuove problematiche e cambieranno di volta in volta anche le indicazioni più appropriati da fornire. Un consiglio gentile e amorevole in una di queste nuove situazioni potrebbe essere il passo decisivo, che spingerà il vostro bambino nella giusta direzione.

Educazione - una strada a doppio senso

Vi sentite come se i vostri figli "ne sappiano più di voi sulla tecnologia informatica"? Non siete i soli.

I bambini di oggi sono nativi digitali e sono moto abili nell'uso delle nuove tecnologie. Per molti adulti invece le competenze digitali vanno acquisite.
Tuttavia, sapere come accedere a Internet non significa saperlo usare in modo sicuro.

Non c'è bisogno che voi genitori sappiate più dei vostri figli su ciò che accade nel mondo virtuale. Ma dovrete avere la situazione sotto controllo nel caso in cui i vostri figli si imbattano in qualcosa di sconosciuto e abbiano bisogno di discuterne con qualcuno più esperto.

L'importante è rendere il bambino parte del dibattito: creare un ambiente in cui possano porre liberamente le domande e fornire il tempo necessario per assorbire nuove informazioni.

Cosa si deve fare quando il bambino raggiunge "quell'età"?

Affidati a ESET Parental Control

Qualunque sia l'età dei vostri figli, la tecnologia oggi a disposizione può fornirvi un aiuto. Gli strumenti ESET Parental Control permettono di bloccare siti o anche categorie di pagine che contengono materiale potenzialmente offensivo. È possibile impostare dei limiti di tempo per la navigazione in internet o per il gioco. Allo stesso tempo permettono a vostro figlio di chiedervi il permesso di visitare alcune pagine o di avere più tempo per giocare, se i suoi compiti sono finiti. Oltre agli strumenti di controllo, abbiamo alcuni consigli per le diverse fasce d'età che renderanno più sicure le attività online dei bambini.

FINO A 10 ANNI

1. Accompagnateli durante le loro prime esperienze sul web

Assicuratevi di esserci quando i vostri piccoli faranno i primi passi nel mondo digitale. Il primo contatto che un bambino ha con internet è una buona occasione per sedersi e guidarlo nella sua nuova avventura.

2. Impostare le condizioni per l'utilizzo di internet

Impostare le regole di base per l'utilizzo di Internet. Una buona pratica è quella di controllare il numero di ore trascorse online e stabilire gli orari in cui è consentito l'accesso al web.

3. Essere un buon esempio

I bambini di solito prendono come esempio il comportamento dei loro genitori, questa è valido sia on-line che nella vita reale. Se i membri della famiglia si comportano in modo positivo, è probabile che un bambino ne segua l'esempio.

DA 11 A 14 ANNI

1. Insegnare loro a non condividere informazioni che potrebbero identificarli

È importante far capire ai ragazzi che nel mondo virtuale non tutti sono amici e che alcune persone potrebbero anche volergli fare del male. Spiegare perché non è sicuro condividere informazioni quali: indirizzo, telefono, scuole o attività doposcuola che frequentano. Il bambino dovrebbe anche chiedervi l'autorizzazione prima di condividere immagini potenzialmente sensibili su internet.

2. Mantenere aperto il dialogo

Incoraggiate i vostri figli ad essere aperti con voi e chiedete liberamente cosa guarda su internet. Se viene utilizzato un computer desktop, cercate di installarlo in una stanza dove tutta la famiglia trascorre del tempo e dove può essere sotto la vostra supervisione, non nella sua camera da letto.

DA 15 A 18 ANNI

1. Nessun altro dovrebbe conoscere le loro password

Sappiamo che i teenager possono essere di difficile gestione, ma assicuratevi che capiscano e mettano in atto i comportamenti più idonei nell'utilizzo delle password. Rispettate la privacy dei vostri figli, ma allo stesso tempo assicuratevi che non diano mai una copia delle loro password a uno sconosciuto, o che non le "prendano in prestito" da qualcun altro, né di persona né su internet.

2. Segnalare immediatamente stalking e cyberbullismo

Ricordate il bullo della scuola? Il macho che rendeva la vita davvero difficile agli altri? Oggi, molti dei bulli sono passati alla tecnologia moderna e si nascondono dietro a Internet. Ciò che non è cambiato è il fatto che cercano di danneggiare psicologicamente gli altri. Pertanto, i ragazzi dovrebbero essere incoraggiati ad informare immediatamente i genitori se si imbattono in episodi di bullismo.

3. Le transazioni finanziarie online sono solo per adulti

L'acquisto di qualcosa su internet non dovrebbe essere un problema, a patto che sia fatto con attenzione. Finché i ragazzi non comprendono le misure precauzionali necessarie da adottare per l'invio di informazioni finanziarie personali, dovrebbero farlo solo sotto la supervisione dei genitori.

Quali sono le minacce principali sul web?

Malware

“Malware” è l'abbreviazione di malicious software, dall’inglese software maligno. Questo tipo di applicazione cerca di danneggiare un dispositivo in vari modi. Alcuni di essi cripteranno i file sul vostro computer, altri cercheranno di spiarvi o di scaricare altre applicazioni pericolose sul vostro dispositivo.
Nella maggior parte dei casi, l'infezione avviene a causa di "errori" commessi dagli utenti, dopo essere stati ingannati dall'aggressore. Utilizzare di soluzioni di sicurezza affidabili e adottare un comportamento accorto riduce il rischio di essere infettati da questo tipo di codice dannoso.

Spam

Avete già avuto a che fare con lo spam prima d'ora. Sono tutte quelle "mail spazzatura" non richieste che ogni giorno compaiono nella vostra casella di posta elettronica. Questi messaggi includono solitamente pubblicità che invitano a visitare determinate pagine con offerte "miracolose", che contengono per lo più contenuti potenzialmente dannosi.

Scam

Lo scam sono atti ingannevoli compiuti attraverso Internet. Inizialmente possono assumere molte forme, come lo spam e l'uso di tecniche di social engineering.
In quest'ultimo caso, gli aggressori si offrono di vendere qualcosa, di agire come vostri colleghi o addirittura di impersonare la vostra banca, mentre tutto ciò che vogliono è ottenere informazioni riservate. Anche i messaggi falsi che richiedono l’account di social network e la password sono un esempio molto frequente di scam.

Cyberbullismo

Questi ti pi di attacchi sono rivolti soprattutto ai bambini. La vittima è di solito minacciata e umiliata dai suoi coetanei nel cyberspazio ed è molto diffuso tra gli adolescenti. Può potenzialmente recare danni a chi ne è vittima, causando traumi emotivi. Il cyberbullismo viene messo in atto di vari contesti: sfruttando anche le funzioni di chat all'interno dei giochi per console.

Grooming

Il grooming avviene quando un adulto cerca di persuadere un bambino a praticare attività sessuali. L'adescatore cerca di creare un ambiente di fiducia e di costruire un legame emotivo. Spesso gli adulti fingono di essere bambini per stabilire una stretta relazione e poi cercano di organizzare un incontro di persona. Per un genitore è importante avere una buona visione d'insieme di chi sono le persone con cui il bambino interagisce online.

Sexting

Il sexting deriva dall'acronimo di Sex e Texting ed è una pratica ormai diffusa da tempo. Mentre la funzione SMS veniva utilizzata sui telefoni cellulari per lo scambio di messaggi di testo, lo sviluppo delle e-mail e di altri servizi di messaggistica ha permesso di inviare anche foto e video. È una pratica comune, poiché la maggior parte degli adolescenti e dei bambini hanno sempre con sé i loro dispositivi mobili.

Furto di Informazioni

Tutte le informazioni inviate via web, senza le necessarie precauzioni, possono essere intercettate da terzi. Queste informazioni possono essere utilizzate per scopi quali furto di identità o ricatto.

Suggerimenti finali

Utilizza strumenti di parental control

Possono essere implementati sia nei browser che nei software antivirus. È compreso nell'ultima Versione di ESET Smart Security o anche come applicazione separata ESET Parental Control per Android. Questi strumenti sono disponibili anche per le console di gioco.

Non lasciate che vostro figlio condivida informazioni riservate su Internet.

Le informazioni sensibili non devono mai essere richieste via e-mail o chat. Le banche non richiedono ma i dati del conto corrente o il PIN in questa maniera. È anche importante non dare informazioni così preziose ai vostri figli.

Non rispondere né eliminare i messaggi di stalking

Se vostro figlio è vittima di cyberbullismo, non deve reagire. Spiegare che l'obiettivo dello stalker è di provocare una reazione così da alimentare il suo desiderio di fare del male agli altri. Se questo tipo di situazione si ripete, avvisate le autorità competenti. Non cancellate i messaggi ricevuti in quanto potrebbero essere usati come prove.

Rimanete aggiornati

Al giorno d'oggi, negare a vostro figlio l'accesso alle tecnologie non è una soluzione. I dispositivi digitali sono parte della sua vita quotidiana e sono sempre più importanti per il loro sviluppo. Invece di porre delle restrizioni, aiutate i vostri bambini ad utilizzarle in modo sicuro e partecipate all'interazione tra loro e il dispositivo. Vale anche la pena di sottolineare che molti di questi rischi possono riguardare anche gli adulti, e molte delle precauzioni qui descritte dovrebbero essere messe in atto a qualsiasi età.
La sicurezza dei bambini è responsabilità di tutti e i consigli forniti in questa guida sono solo una base. Per saperne di più, visitate i nostri siti web e i social network:

eset.com/it/

www.welivesecurity.com

Diventa Fan www.facebook.com/eset

Seguici all'indirizzo https://twitter.com/ESET @ESET