ENJOY SAFER TECHNOLOGY™

saferkidsonline

Social Network Una guida per i genitori

Introduzione

Ricordate di un tempo in cui i bambini giocavano all'aperto e tornavano a casa solo quando avevano fame? Internet ha cambiato tutto. Al giorno d'oggi i giovani possono passare ore e ore sui social network.

Molti di noi, in ESET sono anche genitori, quindi comprendiamo le preoccupazioni che si hanno nel vedere il proprio figlio assorbito dal web. Ecco perché abbiamo realizzato questa guida. Qui troverete informazioni sulle possibili minacce in agguato sui social network e soluzioni che vi aiuteranno a mantenere protetta la vostra famiglia.

1. A cosa fare attenzione?

Malware

Malware è una combinazione dei termini inglesi maligno e software - o in altre parole codice dannoso. Virus, worm e trojan ne sono alcuni esempi. I truffatori utilizzano i social network per persuadere gli utenti a scaricare malware, spesso promettendo software o giochi piratati.

Phishing

Il termine "phishing" deriva da "pesca", in quanto viene utilizzata un'esca per catturare le vittime. Molti aggressori utilizzano questo metodo per rubare informazioni sensibili - come ad esempio le credenziali di accesso al profilo del social network dei giovani. Di solito avviene tramite e-mail collegata a una riproduzione del sito web dei social media. Può essere piuttosto difficile identificare una pagina falsa, poiché le differenze sono spesso minime e i bambini potrebbero inserire informazioni personali senza nemmeno accorgersi che qualcosa non va.

Furto d'identità

Assicuratevi che i vostri figli non pubblichino informazioni sensibili come l'indirizzo di casa e di scuola, il numero di cellulare, la data di compleanno o altri dati che potrebbero essere utilizzati per identificarli. Il furto di identità è una forma diffusa di criminalità informatica, in cui i criminali si appropriano delle informazioni personali degli utenti per utilizzarle per scopi dolosi.

Ci sono due modi principali in cui l'aggressore può ottenere questi dati sensibili:

Usando il social engineering, spesso fingendo di essere l'amico un amico di vostro figlio.

Oppure utilizzando le informazioni accessibili a tutti su un profilo di social network - è fondamentale utilizzare impostazioni di privacy appropriate.

Stalking e Abuso online

Non tutte le minacce ai vostri figli sui social network coinvolgono criminali informatici. Anche i loro coetanei possono essere un problema. Il bullismo non avviene solo nelle scuole: oggi avviene anche tramite internet e può essere dannoso come nella vita reale.

Un altro grave rischio è l'adescamento, soprattutto per quanto riguarda i bambini più piccoli. L'adescamento implica che un adulto cerchi di conquistare la fiducia di un bambino e di costruire un rapporto con lui per convincerlo a praticare attività sessuali. Questo include spesso il sexting, (messaggi con contenuti inappropriati che potrebbero essere inviati a o da vostro figlio).

2. Quali misure potete adottare per proteggere i vostri figli?

Tenendo conto delle potenziali minacce, l'uso dei social network potrebbe sembrare un'attività pericolosa. Tuttavia, proibire a vostro figlio di usarli non risolverà il problema. Troveranno il modo di ottenere comunque ciò che vogliono. Qui di seguito potete trovare suggerimenti che renderanno l'utilizzo dei social network più sicuro e forniranno una protezione adeguata per i vostri figli e la vostra famiglia.

Parlate

Il dialogo è uno dei fattori più importanti per mantenere i vostri figli al sicuro quando sono online - soprattutto quando si parla di social network. Mantenere una comunicazione aperta e onesta con i vostri figli è fondamentale se volete che si fidino del vostro giudizio e seguano i vostri consigli.

Un buon esempio è il cyberbullismo e la sua prevenzione. Fate capire a vostro figlio che se dovesse imbattersi in tali circostanze, anche se non lo riguardano direttamente, deve immediatamente avvertire qualcuno - voi, un insegnante o altri adulti responsabili.

Utilizza software di parental control

A seconda dell'età dei vostri figli, utilizzate un software di parental control. ESET Smart Security, consente di impostare un elenco di siti web bloccati e di limitare gli orari in cui vostro figlio può collegarsi al web.

Tuttavia, anche i bambini dovrebbero poter dire la loro. Proprio per questo ESET Parental Control per Android consente loro di chiedere il permesso di visitare siti web specifici o di avere tempo supplementare sui social network, magari se hanno finito le faccende di casa o i compiti prima del previsto.

Utilizzare una soluzione di sicurezza informatica affidabile

Poiché il malware è una delle minacce più diffuse nel cyberspazio, l'installazione di una soluzione di sicurezza con capacità di rilevamento proattivo sui dispositivi del bambino è essenziale per evitare le infezioni quando si utilizzano i social network.

Anche gli strumenti antispam e firewall possono ottimizzare la sicurezza del sistema di fronte a questi rischi. Inoltre, vostro figlio non dovrebbe mai utilizzare un account amministratore quando naviga sui social network. Impostate un profilo utente speciale per i vostri figli per ridurre al minimo l'impatto degli incidenti di sicurezza.

Utilizzare password forti e verifica a due fattori

I vostri figli sanno che aspetto ha una password sicura? Assicuratevi che non utilizzino opzioni facili da indovinare come "password" o "12345". Dovrebbe essere lunga almeno 10 caratteri, contenere caratteri maiuscoli e minuscoli, un numero e un simbolo speciale come # o @. Adattare una frase o un testo di una canzone può aiutare:

Nell vecchia fattoria diventa Nell@vecch1afatt0ria

Inoltre, ricordate loro di non condividere le loro password con nessuno, nemmeno con i loro migliori amici.

Se vi collegate a Facebook, Twitter o altri social network, assicuratevi che i vostri figli utilizzino la verifica a due fattori offerta nelle impostazioni di sicurezza. Ricevere un codice di accesso monouso sul proprio smartphone aggiunge un altro livello di sicurezza che è difficile da decifrare per gli aggressori.

Impostare un profilo "privato"

Le impostazioni predefinite per la privacy dei social network non garantiscono la sicurezza del bambino. È quindi consigliabile spendere un po' di tempo per impostarle correttamente e verificare quali informazioni potrebbero essere trapelate. Prendiamo Facebook come esempio:

Facebook

Utilizzare le impostazioni del profilo per garantire che nulla sia condiviso con tutti gli utenti. Preferibilmente, rendere disponibili le informazioni solo ad amici e familiari e, se possibile, solo a piccoli gruppi (come i parenti stretti o i migliori amici).

Limitare il pubblico che può vedere le immagini, gli stati e altri contenuti in cui il vostro figlio è stato taggato. Impedire alle applicazioni di accedere alle proprie informazioni personali o di pubblicare sulla propria bacheca.

Insegnate loro ad accettare solo richieste di amicizia da persone che conoscono personalmente. Chiarire che parlare con gli sconosciuti o contattarli su Internet può essere pericoloso come incontrarsi nel mondo reale.

Per informazioni dettagliate sull'utilizzo delle impostazioni di Facebook, si prega di leggere il nostro blog: http://blog.eset.com/2011/05/25/facebook-privacy

Twitter

Per Twitter vanno fatte considerazioni specifiche, come il limite di 280 caratteri, o l'uso frequente di URL abbreviati. Sono anche queste le differenze che dovreste affrontare quando spiegate a vostro figlio come stare al sicuro.

Oltre a seguire solo le persone che conoscono ed evitare collegamenti sospetti, dovrebbero anche controllare la legittimità di qualsiasi messaggio che potrebbero ricevere. I messaggi dannosi sono spesso identificati da altri utenti e le informazioni condivise, quindi una ricerca rapida utilizzando una parte del messaggio può spesso essere d'aiuto.

Inoltre, installate sul vostro computer o dispositivo un plug-in per un browser affidabile che consenta ai vostri figli di vedere il link originale da un breve indirizzo URL senza cliccarlo.

Altri social media

Ci sono molti siti di social media che soddisfano diversi interessi e fasce d'età. È importante controllare che i vostri figli utilizzino quelli più adatti a loro. Abbiamo video guide su Snapchat, Instagram e YouTube e abbiamo anche compilato un elenco di social network più appropriati per i bambini.

3. Conclusione

I social network possono essere una risorsa preziosa per gli utenti di Internet. Tuttavia, come dimostra questa guida, ci sono molte minacce alle quali i bambini possono essere esposti quando li usano. Non sottovalutate i criminali informatici o altri attori malintenzionati. È essenziale implementare le migliori pratiche e utilizzare strumenti di sicurezza affidabili per proteggere le persone importanti della vostra vita.

Aiutarli a impostare correttamente i loro profili sui social network e offrire consigli semplici ma utili potrebbe essere la cosa decisiva da fare per tenerli al sicuro.

10 consigli fondamentali

1. Insegnate ai vostri figli a riflettere prima di cliccare su link e pulsanti di download
2. Insegnate loro ad avvicinarsi alla comunicazione online con un sano senso di cautela
3. Impostate il loro account come privato
4. Insegnate loro a rifiutare le richieste di amicizia provenienti da sconosciuti
5. Mantenete aggiornati il sistema operativo e il software di sicurezza
6. Siate un buon modello di riferimento e tenete sotto controllo anche il tempo che voi passate online
7. Siate vigili su eventuali segnali che possano indicare che un bambino è vittima di cyberbullismo
8. Utilizzate un'applicazione di controllo parentale affidabile come ESET Parental Control
9. Incoraggiateli a usare password forti
10. Chiedete loro di riflettere prima di condividere informazioni personali, video o foto.