

Tecnologia - Diventare giovani content creator in sicurezza: i consigli di Kaspersky per i genitori

Roma - 01 set 2025 (Prima Notizia 24) Una guida fornisce consigli essenziali per aiutare a proteggere i bambini, affrontando le principali regole di sicurezza informatica sia per il mondo

online che offline.

Oltre il 30% dei bambini della Generazione Alpha sogna di diventare social media creator, e circa il 32% dei ragazzi tra i 12 e i 15 anni indica lo "YouTuber" come professione ideale. Per molti, i content creator rappresentano veri e propri modelli di riferimento, e il desiderio di emergere online si manifesta spesso già prima dell'adolescenza. In questo contesto, il coinvolgimento dei genitori non è solo utile, ma fondamentale. Quando i genitori scelgono di assumere un ruolo attivo, imparando come funzionano le piattaforme, impostando insieme ai figli le opzioni di privacy e sicurezza, e discutendo apertamente delle regole, il percorso digitale si trasforma in un'esperienza condivisa: i rischi diventano occasioni di apprendimento e i ragazzi possono esprimere la propria creatività in modo più sicuro.

1. Sii curioso, non critico. Il tuo interesse creerà una rete di sicurezza per i tuoi figli. Se un bambino dice di voler diventare YouTuber, è normale che i genitori si preoccupino. Ma la risposta più costruttiva non è vietarlo, bensì aprire un dialogo. Chiedere perché desidera aprire un profilo, quali contenuti vorrebbe condividere e scoprire insieme gli ultimi trend online, ad esempio attraverso il report Kaspersky, aiuta a entrare nel suo mondo. Questo atteggiamento ha due grandi vantaggi: da un lato dimostra attenzione autentica per i suoi interessi, creando fiducia; dall'altro permette di affrontare in modo naturale temi cruciali come la privacy, i limiti dei contenuti e la gestione del tempo online. Per rendere queste conversazioni più semplici e coinvolgenti, è utile partire da risorse adatte all'età. Un esempio è "L'Alfabeto della Cybersecurity" di Kaspersky, un libro gratuito che aiuta i bambini a familiarizzare con le basi della sicurezza digitale in modo divertente e intuitivo. Grazie a un linguaggio chiaro e illustrazioni colorate, introduce i concetti fondamentali della sicurezza online e mostra come riconoscere le truffe, proteggere i propri dati e navigare con maggiore consapevolezza, senza rinunciare alla creatività.

2. Configurare gli account insieme. Invece di consegnare un telefono e lasciare che i propri figli imparino da soli, è importante prendersi il tempo necessario per configurare gli account insieme. Che si tratti di YouTube, TikTok, Instagram o un'altra piattaforma, sedetevi con loro e seguite i passaggi fianco a fianco: ? Scegliete impostazioni di privacy adeguate (chi può vedere i post, commentare o inviare messaggi) ? Disattivate l'impostazione di geolocalizzazione predefinita ? Utilizzate una password forte e unica ? Abilitate l'autenticazione a due fattori (2FA) per una protezione aggiuntiva. Questo non solo riduce il rischio di hacking o esposizione, ma insegna anche a vostro figlio buone abitudini di sicurezza digitale fin dall'inizio.

1. Insegnate cosa non

condividere. Quando i bambini pubblicano contenuti online, spesso vogliono condividere tutto: dove sono, cosa fanno e con chi sono. Parte del crescere online, però, significa imparare che non tutte le informazioni devono essere rese pubbliche. È quindi importante aiutare i propri figli a capire la differenza tra creare e consumare contenuti divertenti ed essere esposto a materiali o attività potenzialmente pericolosi o dannosi. Questo significa non condividere l'indirizzo di casa, il nome della scuola, gli orari, i programmi delle vacanze o i luoghi frequentati regolarmente. Questi dettagli possono involontariamente renderli più facili da rintracciare, soprattutto se abbinati a foto, tag di posizione e timestamp.

2. Cercate regolarmente il loro profilo su Google. Una volta che vostro figlio inizia a pubblicare post con un nome utente, è importante monitorarne la visibilità online. Un modo semplice è cercare regolarmente il suo nickname su Google e sui social media per capire cosa appare. Ci sono foto personali, tag di posizione o commenti che rivelano più di quanto dovrebbero? Qualcuno ha copiato i suoi contenuti o ha cercato rubargli l'identità?

3. Avvertili delle collaborazioni truffa o delle offerte sospette. Con l'aumentare della visibilità, i giovani creator possono ricevere messaggi da presunti brand che offrono prodotti, sponsorizzazioni o collaborazioni. Per un bambino può sembrare un sogno, ma spesso si tratta di truffe. Insegnate ai vostri figli a diffidare da offerte improvvise, che arrivano tramite DM o e-mail, e che includono link a siti di phishing creati per rubare dati, password o persino informazioni bancarie. Alcuni truffatori chiedono anche "spese di spedizione" anticipate per regali inesistenti, o inducono a installare app dannose. Aiutarli a individuare i segnali di allarme, come: grammatica scorretta o tono urgente ("agisci subito!"), richieste di informazioni personali o password, link sospetti o siti web poco chiari, account non verificati che fingono di essere brand reali. Per i bambini più piccoli, è meglio che i genitori gestiscano tutte le interazioni: lettura dei DM, la valutazione delle offerte dei brand e la risposta alle richieste di collaborazione. Discutete insieme quali tipi di brand sono appropriati con cui lavorare e spiegate perché alcune offerte potrebbero non essere così sicure come sembrano.

4. Parlare con sconosciuti online. Costruire una community online significa attrarre non solo fan, ma anche persone con comportamenti inappropriati o manipolatori. Purtroppo, l'adescamento online è una minaccia reale, soprattutto per i giovani creator, aperti e fiduciosi che condividono dettagli della loro vita. È importante spiegare che non tutti quelli che sembrano simpatici online hanno buone intenzioni. Gli adescatori spesso si comportano come "amici solidali": lodano i contenuti, offrono aiuto o fingono di avere interessi simili. Con il tempo, potrebbero chiedere dettagli personali, foto private o cercare di spostare le conversazioni su piattaforme meno sicure (come chat private, videochiamate o messaggistica crittografata). I genitori devono insegnare ai figli a riconoscere i segnali di allarme:

- Messaggi frequenti e troppo personali da sconosciuti?
- Insistenza sulla segretezza ("non dirlo ai tuoi genitori")?
- Pressioni per condividere informazioni o immagini private?
- Manipolazione emotiva: sensi di colpa, lusinghe o minacce.

Ma soprattutto, devono assicurarsi che sappiano che possono rivolgersi a loro senza timore di essere puniti. "Quando un bambino vuole diventare un influencer, sta esprimendo la propria identità e creatività. Come adulti, il nostro ruolo è quello di sostenere questa ambizione, assicurandoci al contempo che comprenda i rischi digitali che derivano dalla visibilità. Strumenti come Kaspersky Safe Kids aiutano i genitori a essere coinvolti senza essere invadenti, offrendo informazioni

sulle attività online dei propri figli, gestendo il tempo trascorso davanti allo schermo e avvisandoli dei potenziali pericoli. Con il giusto supporto e un dialogo aperto, possiamo aiutare i giovani creator a far sentire la propria voce senza compromettere la loro sicurezza”, ha spiegato Anna Larkina, Privacy Expert di Kaspersky.

(Prima Notizia 24) Lunedì 01 Settembre 2025