

Qual è il problema?

Imparare a proteggere i dati personali, creare password sicure ed essere cauti quando si scaricano programmi e file, è fondamentale per la sicurezza dei vostri bambini, così come per la sicurezza dei dati memorizzati sui dispositivi digitali che usano. In caso contrario, i bambini potrebbero esporre se stessi e l'intera famiglia a pericolose minacce come virus informatici, furto di dati e identità, e altre possibili truffe online.

Per comprendere i concetti relativi alla sicurezza digitale, è necessario conoscere alcuni concetti nuovi come phishing, malware, spyware, spam e junk. Tutto ciò si riferisce a piccoli programmi impostori collegati a software dall'apparenza rispettabile – per esempio, un gioco scaricabile che sembra molto divertente – che poi provocano danni più o meno gravi una volta installati sul computer o sullo smartphone.

Perché è importante?

Se non proteggete i vostri dati personali, vi esponete a molti rischi: danni ai dispositivi, furto di identità e perdite finanziarie. I vostri bambini possono non rendersi conto di mettere in pericolo i loro dati, perché non sempre vi sono segnali evidenti. Per esempio, un amico di vostro figlio potrebbe chiedere la password del computer di casa per giocare e poi accedere alla vostra posta elettronica. Oppure vostro figlio potrebbe utilizzare un programma di condivisione di file (file-sharing) e trasmettere un virus al vostro computer. Un ladro di dati, spacciandosi per una tipologia di persona che dia fiducia ai bambini, potrebbe chiedere ed ottenere dati personali come il numero di telefono di casa, l'indirizzo dell'abitazione, la data di nascita o il codice fiscale, il che espone l'intera famiglia al rischio di furto di identità. Proprio come nel mondo materiale, anche in rete i bambini devono imparare di chi possono fidarsi.

La voce del buon senso

- **Aiutate i vostri figli a padroneggiare la sottile arte della creazione di password:**
 - **NON usare la stessa password per diversi siti o servizi online.** Nel caso la password venisse scoperta su un sito, sarebbero a rischio anche tutti gli altri.
 - **NON usare password facili da indovinare**, come il proprio soprannome o il nome del proprio animale domestico.
 - **NON usare alcun dato personale nella propria password** (ad esempio la data di nascita). I ladri di identità potrebbero riuscire ad usare questi dati per fingere di essere loro.
 - **NON usare come password una parola presente sul dizionario.** I criminali informatici tentano di indovinare le password usando programmi automatici che provano ogni parola presente sui dizionari.
 - **USARE combinazioni di lettere, numeri e simboli.** In questo modo è molto più difficile indovinare le password, perché ci sono tantissime combinazioni possibili.
- **Insegnate ai vostri bambini a fare molta attenzione a tutto ciò che scaricano dalla rete.** Fategli capire che non devono mai scaricare copie gratuite di giochi o film normalmente disponibili solo a pagamento. Spesso questi file nascondono spyware e virus che faranno finire il computer in assistenza – e loro in castigo! Alla fine, si scopre che ciò che sembrava gratuito, ha spesso un costo, ad esempio la raccolta dei vostri dati.
- **Insegnate ai vostri bambini come identificare e gestire lo spam.** Insegnate loro che lo spam è costituito dai messaggi di posta elettronica indesiderata. Devono imparare a non aprire queste email, perché se lo fanno, ne riceveranno sempre di più. La strategia migliore è di non aprire alcun messaggio ricevuto da persone che non conoscono.

Dati personali e altri dati

* LO SAPEVI CHE...

Un sondaggio su un gruppo di bambini della tua età ha messo in evidenza che uno su tre ha condiviso online informazioni che non avrebbe diffuso in pubblico. Mannaggia!

Collega con una freccia le parole con la definizione corretta

Cittadino digitale	informazioni che non permettono di identificarti e/o localizzarti, come un tuo nickname, il tuo cibo preferito o altre informazioni generiche
Dati personali	membro di una comunità globale connessa grazie ad Internet
Altri dati	quando un ladro ruba i dati personali di una persona al fine di svolgere delle azioni a suo nome a sua insaputa
Furto di identità	informazioni che possono essere sfruttate per identificarti e/o localizzarti, come il cognome, l'indirizzo di casa, il numero di telefono, ecc.

* COSA NE PENSI?

Quale può essere una buona regola che i bambini possono seguire quando gli vengono richiesti dei dati personali?

* TI RICORDI?

Come puoi proteggerti dal furto di identità online?

1. Attività in famiglia

Prendi dei fogli di un piccolo blocco note oppure taglia un foglio di carta in strisce più piccole. Con un tuo genitore o un altro componente della famiglia, scrivi sui vari biglietti delle informazioni che riguardano voi, dei singoli famigliari o la vostra famiglia in generale (per esempio: "Amo i cani", "Frequento la classe della Maestra Martina", oppure "Viviamo in Via Roma, 123."). Quindi prendi due contenitori ed etichettane uno con la scritta "dati personali" e l'altro con "altri dati". Poi disponi i biglietti nel barattolo corretto per esercitarti a distinguere tra le due categorie.

2. Sfrutta la tecnologia

Chiedi a mamma o papà di mostrarti un sito web che richiede dati agli utenti. Osservate insieme i dati che gli utenti sono tenuti a compilare e cerca di identificare le domande che ti spingono a fornire dati personali o altri dati (per esempio potreste confrontare i dati richiesti per l'iscrizione a diversi social network).

3. La voce del buon senso...

I dati personali sono dati che possono essere utilizzati per identificarti, come il vostro indirizzo o il codice fiscale. Invece gli altri dati non possono essere sfruttati per identificarti, come la tua età o i tuoi cibi preferiti. Questi ultimi sono solitamente sicuri da condividere online; al contrario, può essere pericoloso condividere i propri dati personali su Internet.