



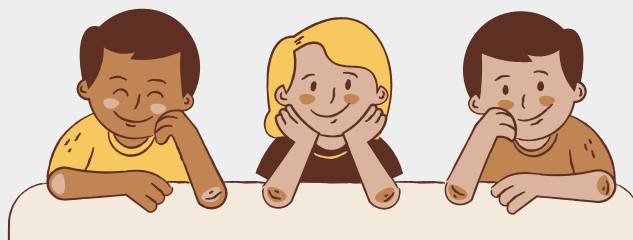
# Tutto quello che devi sapere per proteggerti dai furti di identità

Adolescenti, adulti e bambini quotidianamente usano i propri device per fruire contenuti di ogni tipo che si trovano in Rete. Online, infatti, è possibile trovare di tutto di più, anche quei contenuti che un genitore non vorrebbe mai che il proprio bambino o figlio visualizzasse. La diffusione globale dei social network ha stravolto il concetto stesso di privacy e ogni aspetto della propria vita quotidiana, ormai, viene condiviso attraverso immagini e video. Per questo motivo, adulti e genitori devono controllare regolarmente il comportamento della propria prole in Rete, cercando di capire quello che fanno, con chi hanno parlato e cosa hanno visto.





Dialogare e informare sono gli strumenti che hanno disposizione genitori e adulti, per rendere la loro esperienza in Rete più sicura e per proteggerli da tutti i rischi che si celano nel web. Per rendere la prevenzione efficace, è necessario utilizzare una serie di strumenti adatti e programmi specifici per filtrare i contenuti e monitorare quello che fanno i propri figli. Per fortuna, gli stessi giganti dell'IT offrono una serie di soluzioni per rendere più tranquilli mamme e papà: sono disponibili una serie di servizi (app e programmi) che permettono di inibire l'accesso a certi contenuti ai bambini o agli adolescenti, monitorando le attività che svolgono in Rete e limitando anche il tempo di utilizzo dei vari device.



L'uso di questi strumenti non preclude la strada della costruzione di un dialogo aperto e costruttivo con i propri figli, per educarli a tenere un atteggiamento consapevole e rispettoso in Rete.



## **Il furto d'identità è uno dei pericoli più grandi della Rete**

È importante informare i propri figli sui rischi che si possono correre quando si naviga online o si chatta con degli sconosciuti: il furto d'identità, per esempio, è un pericolo costante e, spesso, sottovalutato. L'identità online degli individui è costituita esclusivamente da informazioni che è facile scoprire e duplicare: dall'indirizzo di posta elettronica fino al profilo social e via dicendo. Il criminale/hacker di turno ruba le credenziali personali della vittima non solo per denaro ma anche per altri scopi.





Per esempio, ledere la reputazione di una persona (rivendendo i dati sul dark web o creando dei profili fake) o per compiere qualche reato (truffe, per esempio) utilizzando un'altra identità.

Purtroppo, tra social network e gli account che si usano quotidianamente per qualsiasi cosa (dalle e-mail fino ai servizi di streaming e via dicendo), per un hacker non è difficile recuperare le informazioni che cerca. Al criminale non importa chi sia effettivamente la vittima: gli interessano solo le sue credenziali. E usare quelle di un adolescente è un gioco da ragazzi. Infatti, in base ad alcuni studi condotti dal Telefono Azzurro e da DoxaKids, il 15% degli adolescenti intervistati ha ammesso di aver subito un furto d'identità su Internet, mentre un 30% ha dichiarato di essersi pentito del materiale che ha pubblicato online. Un 64%, invece, si dichiara molto preoccupato per quanto concerne l'utilizzo dei propri dati sensibili.



È interessante notare come un ragazzo su due ha ammesso di aspettarsi qualche consiglio in più (e anche qualche strumento per tutelarsi) da parte dei suoi stessi genitori o dagli adulti che si occupano di loro, soprattutto per affrontare un fenomeno in forte crescita come il cyberbullismo. Anche il sexting è un altro fenomeno in grande crescita e che sembra preoccupare ragazzi e ragazze: rispetto al passato sono cambiati i mezzi attraverso cui si comincia a esprimere la propria sessualità.





Con la tecnologia gli adolescenti si sentono più liberi di sperimentare e anche di mettersi in gioco: infatti, il 36% dei ragazzi e ragazze ha ammesso di conoscere coetanei che hanno inviato foto intime ad amici. La visione di siti pornografici da parte di bambini e adolescenti è in forte aumento: nello specifico si parla di un 46 % per i ragazzi e un 34 % per le ragazze.

