La tutela dei propri figli è un dovere che molti genitori dimenticano

La sicurezza e la tutela dei minori in Rete sono fondamentali e sono compiti da ascrivere ai genitori e agli adulti che si occupano di loro: queste persone, spesso, sembrano ignorare i rischi legati alla diffusione in Internet dei propri dati personali (anche nel loro caso).

Smartphone, tablet e console di gioco hanno amplificato ancor di più questi pericoli: si tratta di dispositivi dotati anche di fotocamere che possono scattare foto e registrare video che, se condivisi in Rete, possono creare dei danni alla reputazione degli stessi adolescenti o essere utilizzati per altri scopi.

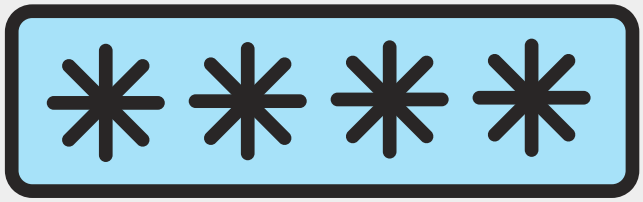
La protezione e la tutela dei bambini e degli adolescenti passa proprio dalla vita digitale che non può essere esclusa a prescindere dalle loro vite: i genitori devono capire che il mondo virtuale in cui trascorrono parecchie ore quotidianamente i propri figli è una parte integrante della loro esistenza e devono trovare un modo per renderlo più sicuro. È importante prestare attenzione soprattutto ai più piccoli: i bambini, infatti, potrebbero inconsapevolmente rivelare dettagli personali come il loro indirizzo di casa o il numero di telefono della madre, informazioni che facilitano il compito degli hacker per rubare la loro identità (o quella dei genitori).

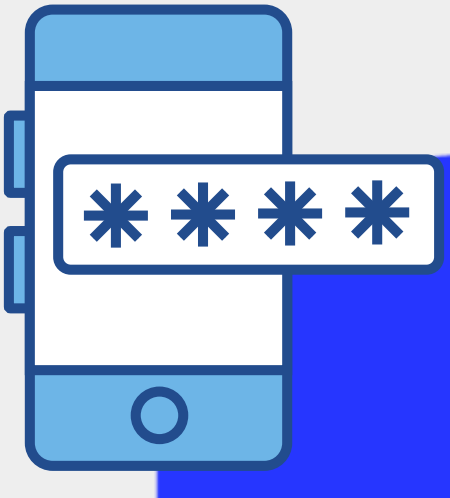
È importante spiegare ai più piccoli come mantenere private le loro informazioni personali: se l'identità di un bambino viene rubata, potrebbero passare degli anni prima di accorgersene. E, in molti casi, potrebbe portare l'adolescente a essere vittima in futuro di qualche forma di ricatto o di cyberbullismo. Spesso a condannare i propri figli sono anche i comportamenti poco responsabili degli stessi genitori che si divertono a condividere in modo compulsivo e scriteriato ogni momento della propria quotidianità, dando origine al fenomeno dello sharenting. Per qualche “mi piace” in più o visualizzazione, madri e padri si divertono a pubblicare di tutto e di più dei propri pargoli. Questo fenomeno produce una serie di pericolosi effetti collaterali: dal “furto d’identità” fino al cyberbullismo o al revenge porn.

Come capire se c'è stato un furto d'identità?

Come si può capire se l'identità del proprio figlio è stata rubata? Per esempio, se si ricevono e-mail da qualche azienda o organizzazione che non si conosce; se vengono addebitate/segnalate spese o acquisti per servizi o prodotti che non sono mai stati ordinati; se non è possibile più accedere ai social network o agli account che solitamente utilizza; se si ricevono messaggi in chat o sul proprio smartphone da perfetti sconosciuti e altro ancora. Gli hacker hanno diverse tecniche per rubare i dati: dal phishing fino ai trojan o malware e altri tipi di virus.

Per proteggere i dati personali dei propri figli non basta attivare un semplice parental control o un antivirus: bisogna modificare le impostazioni delle privacy di ogni account utilizzato (in primis, quelli dei profili social) ed è importante utilizzare delle password sicure. Per esempio, usare sempre la stessa combinazione di parole, lettere e simboli per tutti gli account e servizi che si utilizzano non è mai una buona idea: è importante insegnare ai propri figli a crearne diverse e non scontate. Assolutamente da evitare le combinazioni di numeri in sequenza o le date di nascita; proibiti anche i nomi reali o quelli dei propri animali domestici. Una volta creata la password è importante spiegare ai propri figli di non condividerla con nessuno (al di fuori della cerchia famigliare), mentre è fondamentale sensibilizzarli sull'importanza di cambiarla ogni tot di tempo.





Come proteggere i dispositivi

Con tutte le app per il parental control attivate, antivirus aggiornati e password a prova di hacker, non è mai facile proteggere i propri figli da ogni possibile pericolo che si cela in Rete. Come nel caso del cyberbullismo, anche in questo caso è importante sensibilizzare i propri figli attraverso il dialogo. È importante aiutarli a distinguere quello che è potenzialmente pericoloso da quello che non lo è. Sulle amicizie online è sempre meglio procedere con molta attenzione, mentre devono sempre avvisare gli adulti/genitori nel caso di qualche comportamento inopportuno.

Oltre a dotare il PC, smartphone, tablet e qualsiasi altro dispositivo che utilizzano con antivirus e aggiornamenti di sistema/app, è importante spiegare loro che alcuni programmi e siti mettono a disposizione del materiale o dei contenuti di un certo tipo solo per un motivo: rubare le credenziali del malcapitato. Spesso, dietro a video, file musicali o materiale pirata si possono celarsi pericolosi virus, malware o spyware.

È importante spiegare ai i figli che prima di scaricare un file è sempre necessario sempre verificarne la provenienza, mentre non è mai opportuno rivelare in Rete la propria identità o quella dei familiari. La stessa cosa vale per i social network: per usarli è infatti necessario fornire informazioni personali.

Oltre a settare perfettamente le “impostazioni della privacy” relative agli account, per controllare quello che fanno i propri figli sulle piattaforme social ci sono dei programmi che permettono di filtrare i contenuti che visualizzano: MinorMonitor e KidLogger sono una soluzione ottimale.