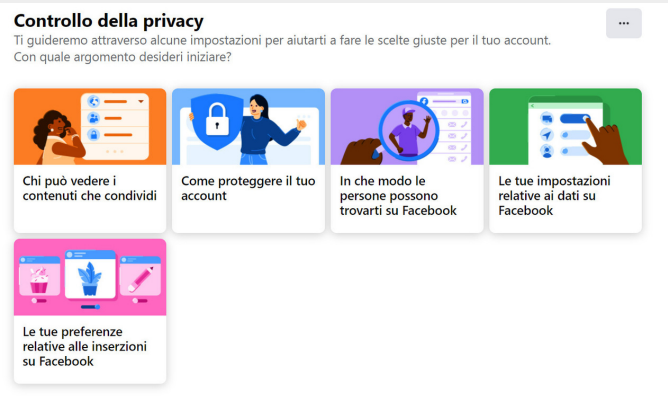
1 - Verifica le impostazioni della privacy

Le impostazioni della privacy cambiano molto spesso, solitamente introducendo nuove funzioni per garantirti una maggiore privacy: se non le cambi da tanto tempo, probabile che ti sia perso qualche novità. Ma cosa fanno queste opzioni? Fondamentalmente, limitano la visibilità del tuo profilo solo a chi vuoi tu. Se tuo figlio sta già utilizzando i social network, parlane con lui, cercando di spiegargli la differenza fra un post che tutti possono vedere e un altro che invece è limitato a soli amici. Meglio ancora, aiutalo a impostare queste opzioni al meglio, così da avere la certezza di farlo navigare in una “bolla” sicura.

Le opzioni naturalmente dipendono dal social network che utilizzi e Facebook è quello che ne offre di più: cliccando sul tuo avatar si aprirà un lungo menu delle opzioni. Scrollando verso il basso, troverai la sezione Impostazioni e Privacy. Vai su Impostazioni e poi Impostazioni del Profilo e infine Provacy del profilo per assicurarti che sia protetto al meglio. Fai tap su Verifica alcune impostazioni importanti e accederai a un menu molto semplice che ti chiarirà chi può vedere i tuoi post e le informazioni come e-mail e numero di telefono.



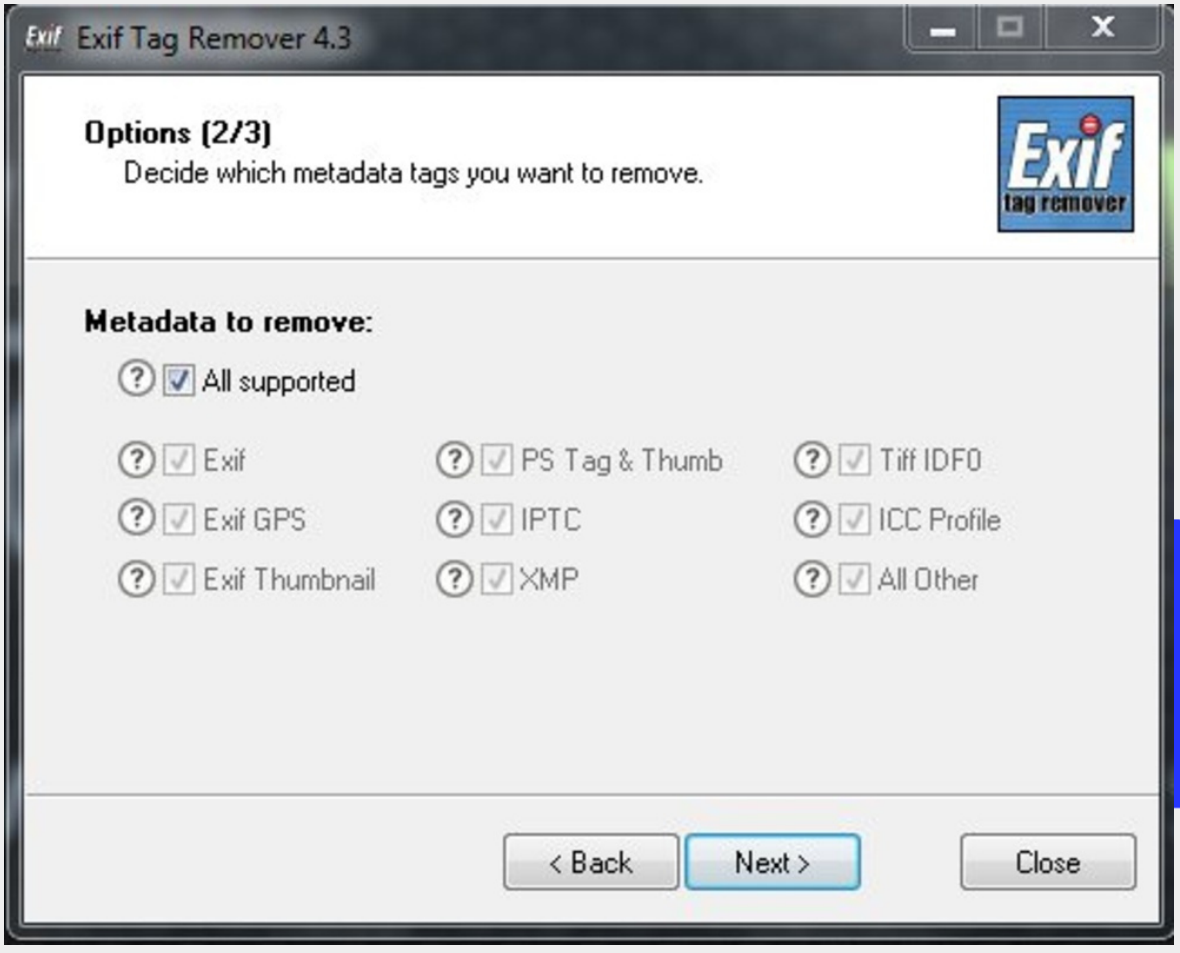
Si tratta di semplici procedure guidate che ti aiuteranno a verificare che i tuoi figli non condividano per errore contenuti a tutto Facebook, né mostrino informazioni sensibili come indirizzo, telefono o altro.

Non tutti i social network offrono tanta libertà. Instagram, per esempio, ha solo due opzioni: profili pubblico (tutti possono vedere quello che posti) o privato (solo le persone che hai accettato come amici le possono vedere). Snapchat, invece, è un po' più granulare in quanto a opzioni. TikTok sotto questo profilo è molto attento e, a seconda dell'età dell'utente, applica automaticamente alcune restrizioni: gli utenti con meno di 16 anni, per dire, avranno il profilo automaticamente impostato su Privato, non permette il download di video, impedisce di duettare con gli amici e consente solo agli amici di commentare. Dai 16 anni in su, invece, hai maggiore libertà di azione.

2 - Occhio alle foto: dicono più di quanto pensi

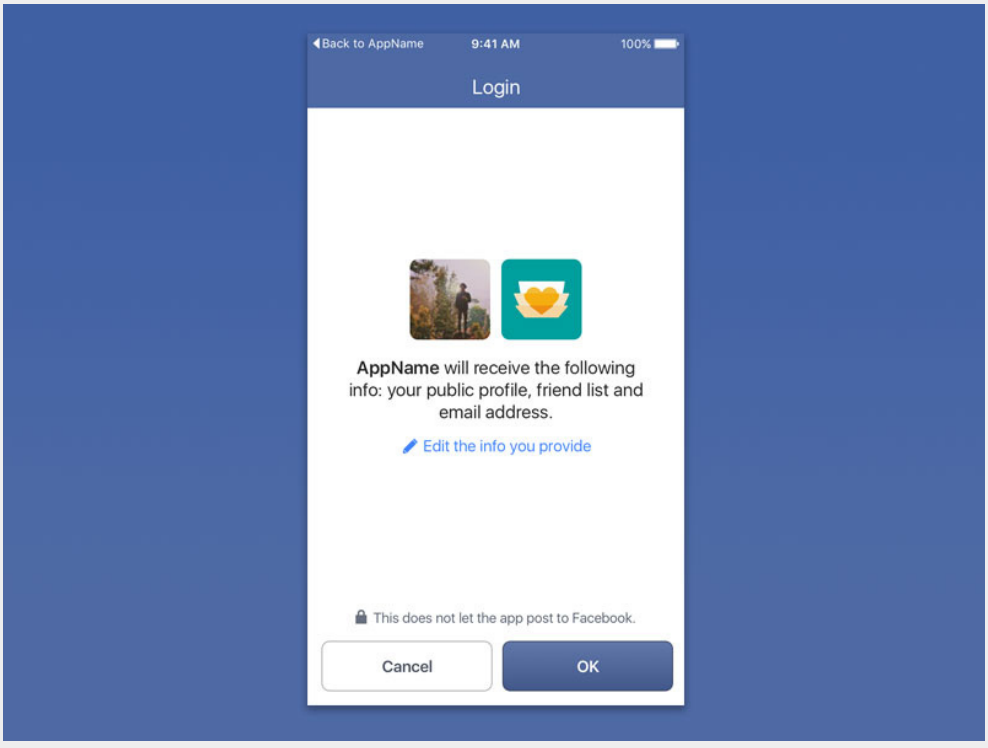
I tuoi figli sicuramente scatteranno una quantità impressionante di foto e selfie, che ovviamente condivideranno coi loro amici. Niente di male, magari lo fai anche tu. L'importante, però, è comprendere quali informazioni possono essere dedotte da queste immagini. Il problema non è il contenuto, che può essere innocente, ma i metadati, che possono dire un sacco di cose su quello scatto: dove è stato fatto, con quale macchina e – soprattutto – la posizione geografica.

Quando le carichi su Instagram o Facebook questi dati vengono automaticamente eliminati, ma questo non avviene se invii la foto via e-mail o la carichi su un blog. Prima di condividere qualsiasi foto, anche la più innocente, io ti consiglio di eliminare queste informazioni, chiamate in gergo Exif Tag. CI sono numerosi software che lo fanno in automatico e in maniera molto semplice: personalmente, ti consiglio Exif Tag Remover.



3 - Fai attenzione alle app collegate

I social network, Facebook in particolare, permettono di collegare differenti app all'account. In alcuni casi si tratta di servizi utili e ragionevolmente sicuri, ma talvolta si tratta di minacce più o meno gravi alla privacy. Un po' come i plugin per i browser, infatti, alcune di queste potrebbero essere più invasive di quanto credi. Questo non significa che ti rubino informazioni, ma sicuramente possono dare a terzi più dettagli di quanto vorresti.



Per questo motivo, ti consiglio di tenerti alla larga il più possibile, e di suggerirlo anche ai tuoi figli, dai vari test e quiz che ti chiedono di “collegare” l’account per essere completati. Vale la pena di rischiare, anche se poco, per sapere che eroe Marvel sei?

Considera che per un ragazzo (e non solo) questi test rappresentano un forte motivo di attrazione: spiegargli che possono rappresentare un potenziale problema (dire pericolo è esagerato, oggettivamente) richiederà probabilmente un po’ di pazienza, ma sarà un’occasione per ragionare insieme a lui sull’utilizzo della Rete e su come proteggersi al meglio.

4 - Usa una VPN, soprattutto se fuori casa

Quanto ti colleghi a un wi-fi, chi gestisce quello specifico router può vedere tutto quello che stai facendo online: i siti a cui ti colleghi, per esempio, e anche intercettare le tue password. Sino a che il router è quello di casa tua, sotto il tuo diretto controllo, puoi stare tranquillo, ma non si può dire lo stesso degli hotspot che trovi nei locali, negli aeroporti, nelle stazioni e via dicendo. Non ti sto dicendo che i proprietari del Mc Donald preferito dai tuoi figli intercettino i dati, anzi, tendo a escluderlo. Però per una persona con un briciolo di competenze informatiche ci vuole davvero poco per mettere in piedi un finto wi-fi, magari con lo stesso nome di quello del locale o dell'aeroporto, solo per intercettare i dati di qualche ignaro utente. Insomma, sino a che puoi, affidati alla connessione dati del tuo cellulare e non a hotspot sui quali non hai controllo.

Mi rendo conto che non sempre è possibile, soprattutto per i tuoi figli, che tendono a consumare GB come non ci fosse un domani. In questi casi, ti consiglio di investire qualche euro mensile in un servizio VPN: si tratta di siti particolari che cifrano tutto il traffico, in maniera end to end, cioè dal momento in cui i dati escono dal tuo dispositivo. Un eventuale spione potrà solo vedere che ti colleghi a un servizio VPN, niente altro. Le tue password, e non solo, saranno al sicuro.

Avrai anche un altro vantaggio: potrai guardare SkyGo e la programmazione italiana di Netflix e Amazon Prime anche se ti trovi all'estero. I servizi migliori? ProtonVPN, in Svizzera, è uno dei più blindati, ma vanno bene anche ExpressVPN, NordVPN e tanti altri.

5 - Non usare le app di tracciamento per i figli

Potresti essere tentato dall'utilizzare una delle tante app spia (legali, sia chiaro) da installare sullo smartphone di tuo figlio per seguire i suoi movimenti e vedere quello che fa, ma fidati, non è il caso. Per due motivi. Uno è che non hai alcuna garanzia che siano sicure. Certo, tu magari ti senti consolato da fatto che ti basta un tap sul cellulare per vedere dove si trova tuo figlio e attivare pure da remoto (a sua insaputa) camera e microfono. Se non hai voglia di leggerlo per intero o non sai l'inglese te lo riassumo molto velocemente: una di queste app, TeenSafe, teneva i dati dei suoi utenti – password incluse – non protetti su server facilmente accessibili.

TeenSafe®

Protecting Your Most Valuable Treasure

Chiunque, insomma, senza particolari competenze, poteva spiare questi bimbi, come se fosse uno dei loro genitori. Ed è solo uno dei tanti esempi. Evitale come la peste, credimi: pongono più rischi di quanto si creda, e offrono solo un falso senso di sicurezza. Capisco perfettamente che vuoi sempre essere a conoscenza degli spostamenti di tuo figlio, e probabilmente è uno dei motivi per cui gli hai concesso uno smartphone. Meglio affrontare la questione insieme a loro, senza spiarli di nascosto: chiedi loro di chiamarti a orari specifici, se ti senti più tranquillo, ma non usare MAI strumenti per spiare, che ti si ritorcerebbero contro.