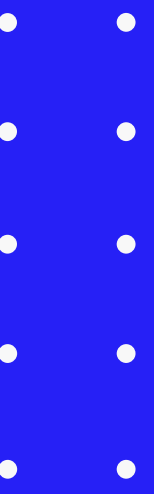


# Come proteggere i tuoi dati personali online

Tradotto dall'inglese  
dalla classe 4C SIA



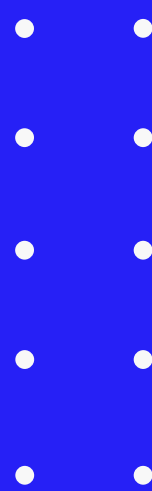
# 1



## + **Controlla le impostazioni del tuo profilo**

Su alcuni social i profili di minorenni sono automaticamente privati; questo significa che solo i tuoi amici possono vedere cosa ti piace, cosa posti e cosa condividi. Se il tuo profilo è già pubblico o lo imposti come pubblico, chiunque può vedere ciò che condividi o inviarti messaggi.

Rifletti sempre molto attentamente prima di disattivare le impostazioni di privacy: esistono per tenerti al sicuro.

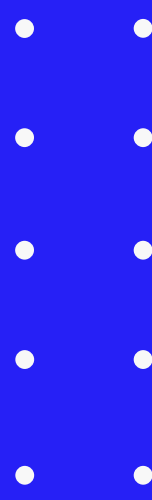


# 2

## + **Pensa prima di postare**

Che il tuo profilo sia pubblico o privato, ricorda che una volta postato qualcosa online può essere veramente difficile cancellarlo completamente da internet.

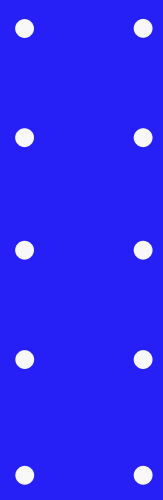
Quindi, prima di pubblicare, chiediti se è qualcosa che veramente vuoi che tutti vedano per anni.



# 3

## **+ Tratta i dati personali degli altri come se fossero i tuoi**

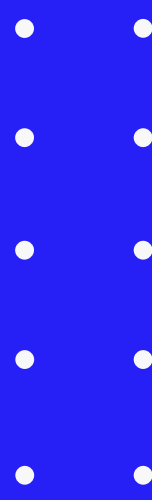
Ascolta i tuoi amici e familiari se ti chiedono di cancellare foto o video in cui appaiono, potresti volere lo stesso anche tu un giorno.



# 4

## + **Fai attenzione ai tag e ai check-in.**

Condividere la tua posizione online può essere rischioso, quindi disattiva la geolocalizzazione se non ne hai bisogno. Pensaci due volte prima di condividere la posizione o mostrare il luogo in cui ti trovi sul tuo profilo social.

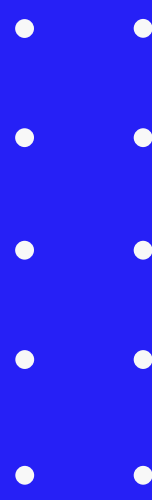


# 5



## **Non lasciarti influenzare**

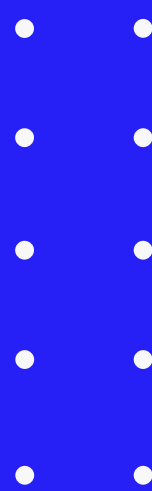
A volte, le applicazioni e le piattaforme cercano di spingerti a cedere più informazioni di quanto sia realmente necessario. Magari il bottone che vogliono farti cliccare è grande, luminoso e al centro dello schermo, mentre l'altra opzione è piccola e facile da non vedere. Fai attenzione a questi stratagemmi e scegli l'opzione con la quale ti senti più a tuo agio, non solo quella più facile da cliccare.



# 6

## + **Leggi i termini e le condizioni (al meglio che puoi)**

Le aziende dovrebbero informarti su ciò che fanno con i tuoi dati personali. Queste informazioni dovrebbero essere scritte chiaramente, così da poterle facilmente capire, e dovrebbero essere facili da trovare. Chiedi ai tuoi genitori o a un adulto fidato se non sei sicuro.



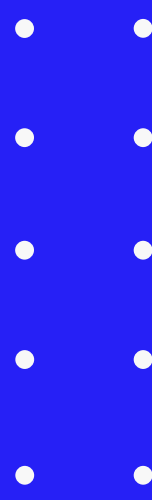
# 7

## + **Non limitarti a cliccare "accetta tutto"**

La prossima volta che vedi una notifica sulla privacy o un banner dei cookie, pensa se vuoi cambiare le impostazioni prima di cliccare su "accetta tutto". Cerca il pulsante che permette di rifiutare i cookie non necessari o non essenziali.

Altrimenti potresti accettare di condividere più informazioni di quelle che vorresti.

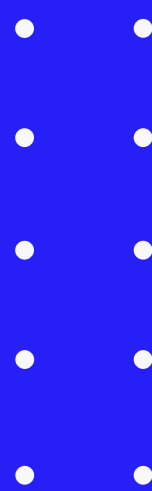




# 8

## + **Conosci il valore dei tuoi dati**

I servizi “gratuiti” non sono sempre gratuiti. Molti dei dati personali che condividiamo online sono usati per fare soldi, ad esempio con la pubblicità. Chiediti sempre “sto facendo la cosa giusta?”.

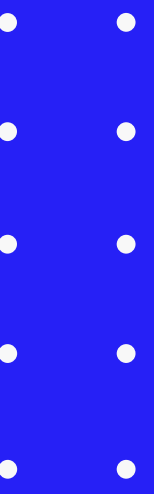


# 9

## + Ricorda: hai il controllo

Hai dei diritti in materia di dati personali. Le piattaforme online e le aziende devono ascoltarti se vuoi una copia dei tuoi dati o se vuoi eliminare i tuoi profili sui social media.

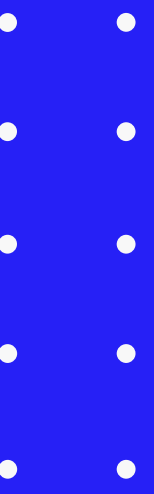
# 10



## + **Tieni i tuoi genitori al corrente**

Anche se controlli i tuoi dati personali, è sempre una buona idea informare i tuoi genitori e chiedere loro aiuto. Non devi mai mentire sulla tua età o fingere di essere il tuo genitore.

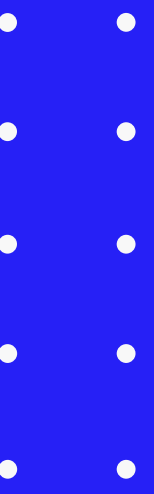
# 11



## + **Elimina quel che non serve più**

Non lasciare aperti account che non usi più. Possono essere hackerati ed essere utilizzati per entrare in altri tuoi account, soprattutto se hai delle password deboli.

# 12

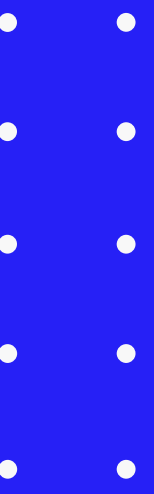


## + **Non usare la stessa password per tutto**

Renderesti facile il furto dei tuoi dati.

Non utilizzare mai la stessa password due volte e scegli le più insolite e originali possibile. Non basare la tua password su cose ovvie che qualcun altro potrebbe indovinare, come il nome del tuo animale o del tuo programma tv preferito. Usa un gestore di password se puoi.

# 13

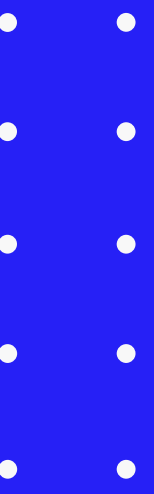


## + **Se ti sembra losco, non cliccare!**

Hai ricevuto un messaggio sospetto da uno sconosciuto o un amico? Potrebbe essere una truffa o qualcosa del genere.

Non aprirlo, non cliccare nessun link, e cancellalo immediatamente. Meglio prevenire che curare.

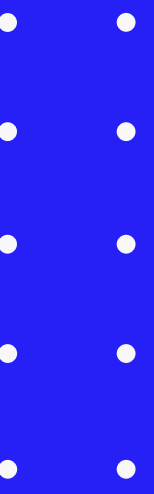
# 14



## + **Non utilizzare mai reti Wi-Fi non sicure**

Potrebbe sembrare semplice perché basta semplicemente cliccare e collegarti, ma reti non sicure potrebbero essere molto rischiose. Un hacker connesso alla stessa rete potrebbe usarla per rubarti i dati o anche controllare il tuo dispositivo!

# 15



## + **Mantieni aggiornati i tuoi dispositivi!**

Siamo sempre tentati di cliccare su “ricordamelo più tardi” quando ci viene chiesto di installare un aggiornamento.

Ma questi aggiornamenti contengono spesso protezioni contro gli ultimi virus e truffe.

Installa sempre i nuovi aggiornamenti il prima possibile.