



unicef



GUIDA PER I GENITORI

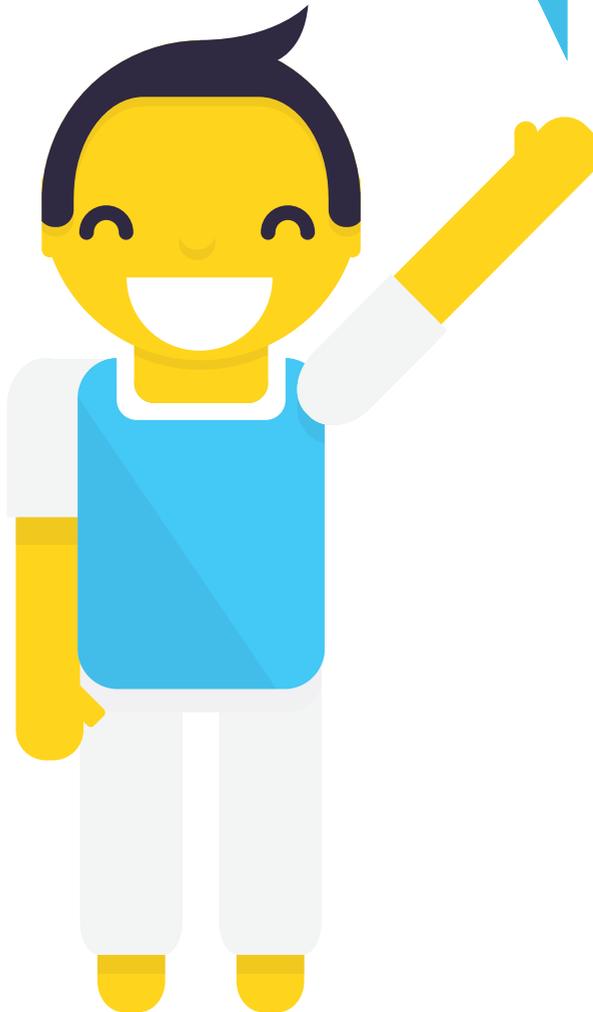
COME

# Parlare ai bambini di Internet





DIGI  
**CyberSAFE™**  
 in partnership with Cybersecurity Malaysia



©Telenor Group

È necessaria l'autorizzazione per la riproduzione di qualsiasi parte di questa pubblicazione. L'autorizzazione sarà concessa gratuitamente a fini educativi o ad organizzazioni senza scopo di lucro. Per richiedere autorizzazione e per altre informazioni sulla pubblicazione, si prega di contattare: [info@unicef.it](mailto:info@unicef.it). Tutte le verifiche per le informazioni in essa contenute sono state realizzate da Digi e UNICEF Malaysia.

I contenuti relativi alla situazione in Italia e gli adattamenti apportati rispetto all'originale sono stati realizzati dal Comitato Italiano per l'UNICEF.

[www.digi.com.my](http://www.digi.com.my); [www.unicef.my](http://www.unicef.my);  
[www.unicef.it](http://www.unicef.it)

Il Comitato Italiano per l'UNICEF ringrazia i succitati partner per aver concesso ai fini della traduzione e dell'adattamento in italiano, sia il progetto grafico che parte dei contenuti di questa pubblicazione.

I Edizione 2015  
 II Edizione 2018  
 III Edizione 2021

1

Capitolo uno

## Introduzione a Internet

2

Capitolo due

## Perché dovremmo parlare ai nostri figli di Internet

3

Capitolo tre

## Cosa dovremmo dire ai bambini?

4

Capitolo quattro

## Figli dell'era digitale Raccomandazioni

## Prefazione

Non è mai stato così facile per i bulli, gli autori di reati sessuali, i trafficanti e coloro che arrecano danni ai bambini contattare le potenziali vittime in tutto il mondo, condividere le immagini del loro abuso e incoraggiarsi l'un l'altro a commettere ulteriori reati. La connettività digitale ha reso i bambini più avvicinabili attraverso i profili dei social media non protetti e i forum dei giochi on-line. Ciò consente ai criminali di restare anonimi - riducendo il rischio di essere identificati e perseguiti - ampliare le loro reti, aumentare i profitti e perseguire più vittime alla volta. È in gioco anche la privacy dei bambini. La maggior parte dei minorenni - e dei genitori - ha una consapevolezza molto limitata, a volte nulla, della quantità di dati personali che

inserisce in Internet, e, ancora meno, dell'utilizzo che altri potrebbero farne.

Nessun bambino è al sicuro dai pericoli online, ma i più vulnerabili corrono il rischio di subire gravi danni.

Questa guida è per tutti i genitori che hanno domande su Internet, sull'uso e sulle misure di sicurezza quando i loro bambini sono online. Dove e in quale modo i nostri figli trascorrono il loro tempo online? Come li proteggiamo dai predatori? Dal cyberbullismo e dai contenuti dannosi e inappropriati? Quali altri rischi si trovano ad affrontare? Quali risorse sono disponibili? Come parliamo ai nostri figli di Internet?



unicef



telenor  
group

CAPITOLO UNO

## Introduzione a Internet

Che ci crediate o no, un tempo ci affidavamo a posta, radio, televisione, pubblicazioni cartacee ed enciclopedie per connetterci con il mondo e cercare informazioni. Per connetterci gli uni con gli altri, potremmo contare solo sulle cerchie chiuse - amici, parenti e la comunità locale che ci circonda -. Poi è nata Internet e siamo diventati una comunità locale interconnessa che ha aperto una finestra sul mondo. Le nostre vite non sono state più le stesse.

Alcuni paesi hanno avuto accesso a Internet da più di 20 anni e, da molti di noi oggi, il web viene considerato un amico. Mettendo in rete l'intero pianeta, Internet è una grande risorsa per creare contatti tra le persone in ogni parte del mondo.

Possiamo usarlo per diverse attività come studiare, stare in contatto con gli amici, colmare le lacune tra generazioni, imparare a cucinare, vendere oggetti fatti a mano, guardare programmi di intrattenimento o ottenere indicazioni quando ci siamo persi.

Internet ci consente di cercare opportunità di lavoro, di trovare istruzioni su come portare a termine un progetto, gestire i nostri soldi, fare acquisti in altri paesi, fare ricerche per i compiti di scuola, pubblicare i propri pensieri su giornali online o "blog", imparare tutto quello che non avremmo mai immaginato potessimo fare. Internet ha reso il mondo un posto più piccolo che può essere raggiunto con il tocco di un mouse.



## Come usare Internet – la strada giusta

1

### Usare Internet per imparare e ricercare informazioni

Oggi possiamo usare Internet per cercare informazioni di qualunque genere. Usando i motori di ricerca come Google o Bing, possiamo digitare una parola o una frase e le pagine di informazione indicizzate su quell'argomento appaiono subito sul nostro schermo. Attraverso video didattici su siti web come YouTube, possiamo imparare come cucinare una nuova ricetta o come piegare un aeroplano di carta. Siamo in grado di trovare rapidamente le informazioni, ottenere avvisi meteo, prezzi di alimenti, informazioni storiche, guardare live-webcam in tutto il mondo e foto di luoghi che sogniamo.

2

### Usare Internet per connetterci a qualcuno

Tramite email, social media, chat, forum online e altro oggi siamo più collegati che mai con il resto del mondo. In Bangladesh e Myanmar le aule mobili collegano insegnanti qualificati con le comunità rurali e l'uso della chat video può mettere in contatto medici qualificati con pazienti che vivono in villaggi remoti. In poche parole, Internet è uno strumento straordinario che permette il dialogo tra persone che altrimenti non potrebbero.

3

### Usare Internet per intrattenere

TV, radio, giochi e Internet una volta erano entità separate mentre oggi Internet ha avuto il merito di racchiuderle tutte al suo interno. L'intrattenimento su Internet è disponibile su YouTube, in streaming, attraverso Windows Media Player e iTunes o consolle come AppleTV, Xbox e PlayStation.

4

### Usare Internet per creare opportunità

L'utilizzo di siti come LinkedIn, Amazon, Blogger e molti altri possono creare potenziali opportunità di lavoro, shopping e possibilità di vendita online, nonché l'opportunità di pubblicare articoli con la propria voce.

In questo modo, oggi possiamo non solo ricercare informazioni attraverso un click del mouse, ma anche condividere i nostri pensieri con il resto del mondo. Tutto questo grazie a Internet.

## Perché dovremmo parlare ai nostri figli di Internet?

### *Perché la conoscenza è potere*

In un mondo in continuo cambiamento, sappiamo che i nostri figli stanno crescendo più velocemente che mai. In questa epoca possiamo aiutarli ad evitare le insidie tenendoci al passo del boom esplosivo che ha avuto Internet. Imparando noi stessi quali sono i modi migliori per parlarne con i nostri bambini, possiamo proteggerli da alcuni dei rischi causati dalla interconnessione: i pericoli di un uso improprio della rete.

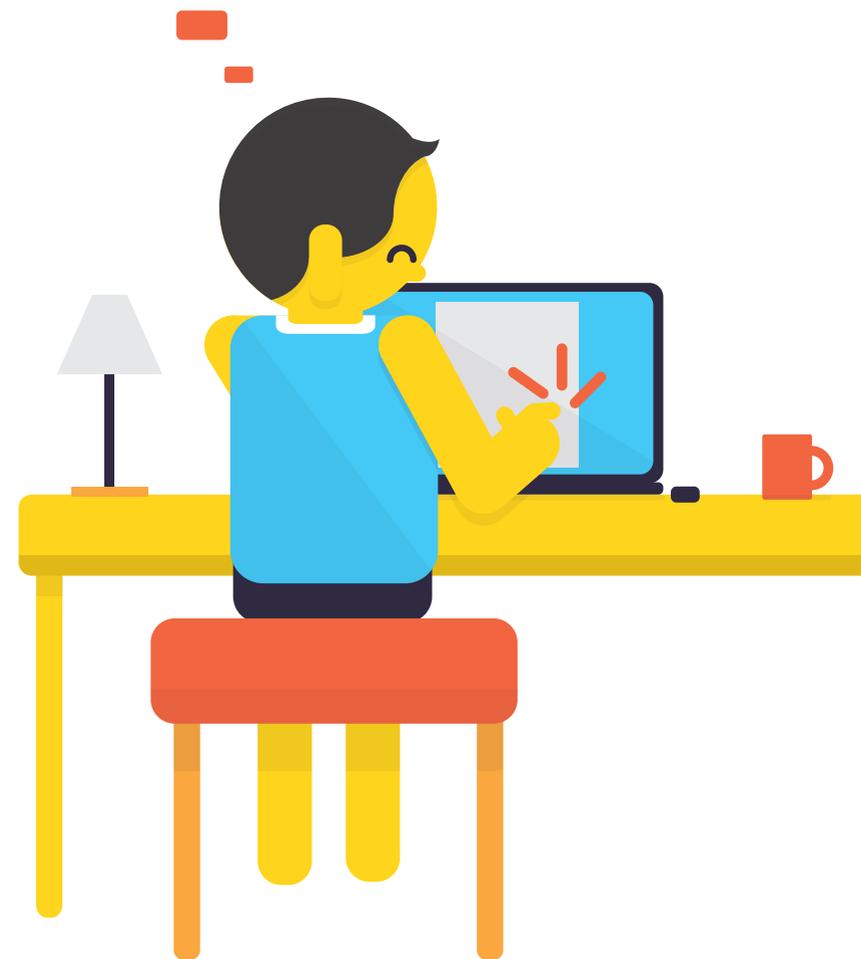
### *Evitare contatti con gli sconosciuti*

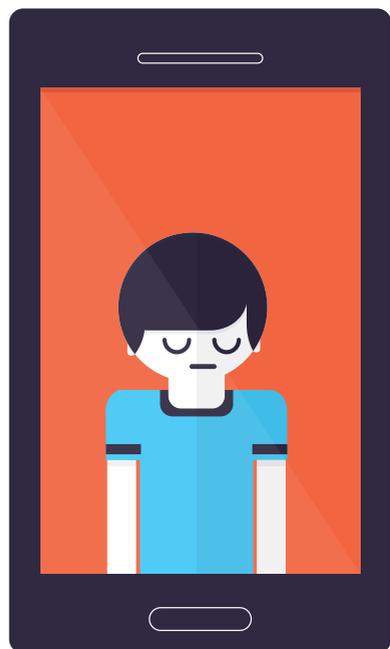
Entrare in contatto con gli sconosciuti attraverso i social media a volte può essere rischioso per i nostri figli soprattutto se si connettono con le persone sbagliate. Poiché non esiste un modo per verificare se il profilo di una persona corrisponde a quello che dice di essere, possiamo giudicare con i nostri figli quando una interazione diventa pericolosa per evitare di cadere nelle mani dei predatori online. Il modo migliore per tenere la situazione sotto controllo è essere sempre aggiornati su quali sono tutti i social media utilizzati dai propri figli. Tenuto conto delle indicazioni di legge (che in Italia fissano a 14 anni l'età minima per l'accesso autonomo ai social network e alle app) spetta

al genitore decidere quale sia l'età giusta che il figlio deve avere per possedere una pagina sui social e, dal quel momento, deve sempre essere aggiornato di quali sono i suoi amici "online". Se questi contatti non sono parenti, o non provengono dalla scuola frequentata dai figli, o da famiglie che conosce nella sua comunità, allora meritano un approfondimento.

### *La verità: ogni volta che qualcosa viene pubblicato online è difficile eliminarlo*

Sebbene ci possa sembrare facile eliminare un post online solo perché risulta invisibile, l'informazione pubblicata è stata caricata in Internet e quindi risulterà online per sempre. Se pubblichi una foto online, in un momento di euforia durante una festa, non troverai un pulsante "annulla" o "cancella" da premere. L'immagine o il testo pubblicato possono diventare pericolosi se alterati o veicolati su siti inappropriati, quindi è molto importante pensare prima di pubblicare. Alcuni sondaggi sull'atteggiamento che hanno bambini e adolescenti con Internet, hanno dimostrato che la maggioranza non è interessata alla violazione della propria privacy o dell'anonimato della persona con cui interagisce.





## Cyberbullismo: le leggi per contrastarlo

### Il contesto

La conoscenza, la prevenzione ed il contrasto dei fenomeni del bullismo e cyberbullismo fanno parte del lavoro che l'UNICEF svolge da sempre sia a livello globale che attraverso azioni mirate nei singoli paesi. I numeri ci fanno capire quanto sia importante fin da subito costruire sempre più efficienti strategie in grado di arginare il fenomeno: le statistiche più recenti delle Nazioni Unite mostrano come nel mondo uno studente su tre tra i 13 e i 15 anni abbia vissuto esperienze di bullismo di vario genere.

Secondo l'UNESCO, gli episodi di violenza a scuola e il bullismo sono fenomeni globali che affliggono un numero significativo di bambini e adolescenti: si stima che nel mondo 246 milioni di questi sperimentino ogni anno qualche forma di violenza a scuola o episodi di bullismo. Anche il cyberbullismo è in sensibile aumento: la maggior parte dei dati disponibili riguarda indagini condotte nei Paesi industrializzati dove una percentuale tra il 5% e il 20% della popolazione minorile ha vissuto sulla propria pelle tale pratica



dannosa, con importanti conseguenze psicofisiche che vanno ad incidere profondamente sulla loro vita.

L'aumento del cyberbullismo riflette la rapida espansione dell'accesso di bambini e ragazzi ad Internet: nel 2017 circa il 70% della popolazione mondiale tra i 15 e i 24 anni risultava connessa ad Internet e dai dati provenienti da 7 Paesi europei, la percentuale di bambini e adolescenti tra gli 11 e i 16 anni esposti a cyberbullismo è aumentata tra il 2010 e il 2014 passando dal 7% al 12%. L'ultima indagine diffusa dall'ISTAT su bullismo e cyberbullismo in Italia ha evidenziati numeri preoccupanti: poco più del 50% degli 11-17enni partecipanti all'indagine ha subito qualche episodio offensivo, non rispettoso e/o violento da parte di altri ragazzi o ragazze nei 12 mesi precedenti al sondaggio e sempre nello stesso arco di tempo il 63,3% dei ragazzi e adolescenti ha dichiarato di essere stato testimone di comportamenti vessatori di alcuni ragazzi verso altri. Anche se non esistono dati aggiornati, è opportuno ritenere che l'aumento dell'attività online da parte di bambini e ragazzi durante la pandemia COVID-19 li stia esponendo maggiormente ai rischi della rete.

### La normativa italiana

Il Comitato Italiano per l'UNICEF ha, fin da subito, espresso grande soddisfazione per l'approvazione della legge n.71 del 2017 - la prima ad introdurre la parola cyberbullismo in un ordinamento europeo - condividendo in particolare l'approccio incentrato sulla prevenzione, la formazione e la sensibilizzazione, gli unici strumenti che riteniamo siano realmente in grado di contrastare il fenomeno in modo efficace. Detto ciò, è opportuno evidenziare le principali criticità che ad avviso dell'UNICEF la normativa presenta, oltre ai ritardi sul fronte attuativo, auspicando che questa possa essere perfezionata attraverso la discussione parlamentare in corso.

- La definizione: estendere il campo di applicazione delle misure contemplate dalla legge anche alla prevenzione e al contrasto del bullismo, prevedendo una definizione di quest'ultimo in linea con gli standard internazionali di riferimento ed integrando la definizione di cyberbullismo con il requisito dello squilibrio di potere/forze alla base del comportamento vessatorio;

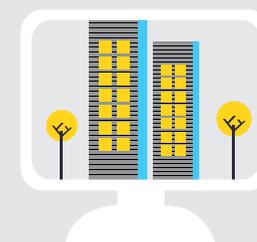
## Fatti e cifre

- Piano d'azione integrato: prevedere che il Tavolo tecnico per la prevenzione e il contrasto del cyberbullismo così come previsto dall'art.3 della normativa estenda il proprio mandato alle fattispecie di bullismo e si riunisca con cadenza periodica al fine di provvedere in tempi celeri alla redazione e approvazione del Piano di azione integrato per il contrasto e la prevenzione del cyberbullismo (e del bullismo) e del sistema di raccolta dati finalizzato al monitoraggio di entrambi i fenomeni (ex art.3, comma 3, L.71/2017) avvalendosi anche della collaborazione e dell'esperienza maturata dall'ISTAT;
- Linee di orientamento: Aggiornare biennialmente le Linee di orientamento per la prevenzione e il contrasto del cyberbullismo nella Scuola dell'ottobre 2017, così come previsto dall'art. 4, L.71/2017;
- Ruolo dei genitori: valorizzare il ruolo dei genitori e responsabilizzare questi ultimi in relazione alle azioni di carattere educativo da attivarsi in ambito di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo: il protagonismo educativo che attualmente la legge riconosce alla scuola non deve infatti comportare il totale esonero delle famiglie da queste funzioni;
- Consapevolezza digitale: investire nell'alfabetizzazione e nella consapevolezza digitale sia dei minorenni sia degli adulti di riferimento;
- Età minima per la presentazione dell'istanza di oscuramento: una criticità potrebbe rilevarsi nell'età minima richiesta ai fini della presentazione dell'istanza di oscuramento, che l'articolo 2 concede ai maggiori di 14 anni. In questo modo, essendo il fenomeno esteso anche ai ragazzi con meno di 14 anni, questi possono trovarsi, in caso di inerzia dei genitori, privi di strumenti di tutela diretta;
- Misure riparative e ammonimento: mantenere la matrice preventivo-educativa della L.71/2017, evitando strategie di contrasto caratterizzate dall'impiego di strumenti repressivi di carattere penale, ma prevedendo casomai misure di carattere riparativo o incentrate sullo svolgimento di attività sociali. Prevedere a questo proposito che la procedura di ammonimento ex art.7 L.71/2017 sia estesa anche alle fattispecie di bullismo;
- Fondi: prevedere l'aumento dei fondi stanziati dalla L.71/2017, che sin dalla sua iniziale discussione parlamentare sono stati più volte ritenuti insufficienti.

In Italia le ragazze sono più di frequente vittime di cyberbullismo: **7,1%** rispetto al **4,6%** dei ragazzi

Nel corso della propria carriera scolastica si è trovato a gestire il **65%** di casi di bullismo tradizionale e il **52%** di cyberbullismo

Le prepotenze più comuni consistono in offese con brutti soprannomi, parolacce o insulti (**12,1%**), derisione per l'aspetto fisico e/o il modo di parlare (**6,3%**), diffamazione (**5,1%**) esclusione per le proprie opinioni (**4,7%**) aggressioni con spintoni, botte, calci e pugni (**3,8%**).



## Frode delle vendite online e furto delle identità

*Istintivamente sappiamo quando qualcosa ci sembra troppo bella per essere vera, ma a volte abbiamo bisogno di un piccolo aiuto per averne la conferma. I venditori sono formati per essere efficaci nelle vendite ma a volte, non è chiaro se acquistare online sia soddisfacente o meno. Dobbiamo insegnare a noi stessi e ai nostri figli ad individuare attività potenzialmente fraudolente può aiutarci a salvarci dai furti e da spese inutili.*

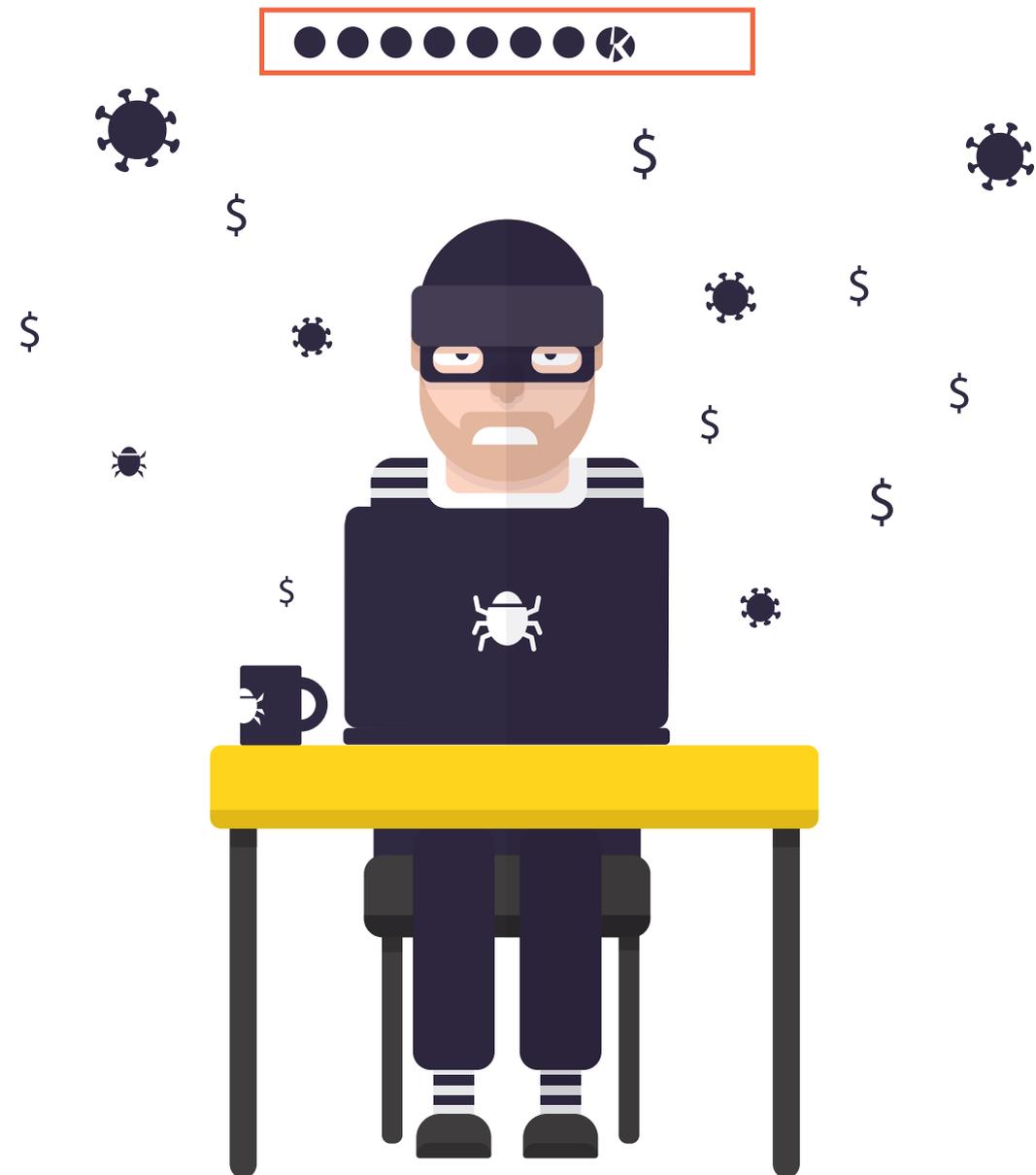
*Se chiediamo dove e quando vengono condivise le nostre informazioni personali – foto, numeri di carta di credito e conto bancario e indirizzi – possiamo evitare che altre persone usino i nostri dati in modo errato.*

### Attacchi virus e minacce malware

Se ci interfacciamo con il vasto mondo di Internet, ci apriamo anche agli hacker e ai malware che possono infettare i nostri computer, dispositivi e file importanti. I programmi antivirus di solito sembrano essere link inoffensivi. Imparare come evitare questi attacchi aiuterà a mantenere sani e funzionanti i nostri pc e dispositivi elettronici.

### Contenuti inappropriati all'età

Sappiamo che i nostri bambini sono curiosi ed è quello che li rende così straordinari. Ma bisogna tenere presente che i contenuti online possono essere non regolamentati: per esempio, i contenuti per adulti possono essere facilmente trovati dai più piccoli e quindi diventa importante educare i nostri figli su cosa va bene su cosa va bene e su cosa invece deve essere assolutamente evitato.



## Quali sono le app più popolari che i genitori dovrebbero conoscere?



### Facebook

Considerato il più famoso social media, la diffusione globale di Facebook consente ai suoi utenti di condividere post, immagini, note e persino acquistare alcuni articoli online. È un ottimo modo per tenere i rapporti con gli amici e la famiglia e il fatto di poter stare in contatto con persone che vivono in ogni parte del mondo, rende questa app gratificante. Nonostante i minori debbano avere almeno 13 anni per aprire un account di Facebook, molti bambini anche più piccoli ne posseggono già uno. Oltre a essere consapevoli delle attività dei loro figli su FB, i genitori dovrebbero parlare con loro dei rischi e dell'importanza delle impostazioni sulla privacy, segnalando anche richieste di amicizia indesiderate.



### Twitter

Twitter è un microblog dove gli utenti, postano brevi messaggi – noti come tweet – che non sono più lunghi di 280 caratteri. Gli utenti possono anche seguire i tweet di altre persone. È molto popolare tra gli adolescenti che sono soliti twittare notizie sulle loro celebrità preferite o curiosità sulla propria vita personale. I genitori dovrebbero essere consapevoli che, anche se i tweet possono essere mantenuti privati, molti adolescenti hanno account pubblici e quindi considerano i tweet pubblici la normalità. Bisogna parlare con loro di ciò che pubblicano facendo loro capire come velocemente può diffondersi un post. Gli aggiornamenti vengono visualizzati immediatamente e, anche se i tweet possono essere eliminati rapidamente, qualcuno nel frattempo potrebbe avere già letto e salvato il post. Quindi i bambini dovrebbero fare attenzione a come usare la giusta impostazione per garantire che il tweet possa essere visto solo dagli amici, anche se anche all'interno di una cerchia di amici, è possibile che sorgano dei problemi.



### Instagram

L'app che tutti usano potrebbe effettivamente promuovere, per i vostri figli, un mix tossico di narcisismo e insicurezza. La maggior parte delle foto pubblicate su Instagram sono autoscatti – selfie –, immagini dell'utente scattate da amici o da lui stesso. I "follower" dell'utente possono visualizzare, aggiungere "like" sulla foto o sul video o lasciare un commento. Quest'ultimo può diventare terribilmente esplicito e cattivo, dal momento che i ragazzi postano foto di se stessi in costume, biancheria intima o addirittura nudi. L'app rimane una delle più gettonate tra i giovani. Molti dei contenuti pubblicati hanno l'obiettivo di raccogliere molti "mi piace" e commenti positivi, utili a incrementare l'autostima degli utenti. Proprio per questo, l'app nasconde in sé numerosi pericoli tra cui: cyberbullismo, pedofilia, adescamento e condivisione impropria di contenuti personali.



### You Tube

YouTube non è solo il canale più conosciuto per guardare e condividere video ma anche il sito tra i più popolari di Internet. Voi e i vostri bambini potete trovare praticamente qualsiasi cosa su Youtube: dai video di formazione aziendale ai video sui gatti, alle esibizioni di pop star amatoriali. Per caricare un video devi avere almeno 13 anni, che è anche l'età richiesta per poter creare un account su Google, come previsto dalla legge sulla protezione della privacy online dei minorenni negli Stati Uniti. Le linee guida di YouTube proibiscono sesso, nudità, violenza, molestie, atti illeciti, incitamento all'odio, e altri contenuti inappropriati. Succede però che un video può tecnicamente soddisfare queste linee guida, pur essendo ancora provocatorio e non adatto ai minori. I genitori dovrebbero essere consapevoli che i figli possono visualizzare o pubblicare materiale non idoneo. Con la guida, YouTube può essere uno spazio per l'educazione e l'intrattenimento. YouTubeKids è un'app pensata appositamente per i bambini più piccoli.



## WhatsApp

WhatsApp è un'app di messaggistica istantanea molto utilizzata che consente agli utenti degli smartphone di scambiarsi messaggi grazie alla connessione Internet, senza incorrere in addebiti come invece avviene per gli SMS. Oltre ai messaggi di testo, gli utenti possono scambiarsi immagini, video e clip audio; possono anche effettuare telefonate. I messaggi possono avere un unico destinatario o possono essere inviati ad una chat di gruppo. WhatsApp è utile e divertente, ma essendo uno strumento di comunicazione, può essere utilizzato facilmente per lo scambio di contenuti inappropriati, e può esporre i giovani utenti a contatti indesiderati. Anche se WhatsApp afferma di non essere destinato ad utenti al di sotto dei 16 anni di età, i dati dicono che è molto popolare tra i giovani. Dopo esserti registrato, la app ti connette direttamente agli altri utenti WhatsApp della tua rubrica e ti incoraggia ad aggiungere nuovi amici.



## Snapchat

Questa app di messaggistica video e foto consente agli utenti di pubblicare contenuti che durano 10 secondi al massimo prima che vengano cancellati. A causa della natura temporanea di ogni snap, l'app è stata considerata un mezzo popolare per la pubblicazione di contenuti discutibili, incluso il sexting. Snapchat è molto popolare tra i giovani, molti dei quali lo usano solo per divertimento, ma i genitori dovrebbero in ogni caso informarli, del pericolo che corrono nel momento in cui pubblicano una foto. Erroneamente, molti utenti credono che le loro immagini non possano essere salvate o inviate in modo virale. Per questo motivo i genitori dovrebbero avvertire i propri figli che nulla scompare in modo definitivo da Internet. Per maggiori informazioni, i genitori possono consultare il Centro di Sicurezza di Snapchat o visitare il sito web.



## TikTok

TikTok, il cui nome evoca lo scandire del tempo, è senza dubbio il social del momento. L'app che conosciamo oggi, disponibile in 34 lingue e con oltre 1 miliardo di utenti attivi ha velocemente conquistato i teenager di tutto il mondo. Aprire un profilo è semplicissimo: basta avere 13 anni e iscriversi con un account Facebook, Twitter, Google, Instagram, o anche solo con un numero di telefono e una email valida. Una volta aperto il profilo, l'utente viene catapultato in un karaoke virtuale fatto di challenge, musiche, coreografie, filtri e filmati brevissimi, della durata massima di un minuto, che possono diventare dei veri e propri tormentoni. Sebbene sia una piattaforma essenziale e divertente TikTok presenta molti rischi potenziali per i teenager: dalla violazione della privacy, dalle insidie da parte di predatori sessuali all'elevata dipendenza da like e visualizzazioni.



## OnlyFans

OnlyFans è una piattaforma online, ideata nel 2016 per consentire ad artisti e creator di condividere a pagamento contenuti speciali e avere un contatto diretto con i propri fan. Gli artisti possono caricare foto, video e chattare con i fan su pagine personali; a loro volta, gli utenti possono accedere, pagando un abbonamento mensile, a contenuti esclusivi pensati appositamente per loro. OnlyFans non prevede alcun tipo di censura sui contenuti condivisi, ragione per cui la piattaforma, pur continuando a ospitare diverse categorie di artisti, è rapidamente diventata la "vetrina" prediletta di professionisti della pornografia in cerca di guadagni extra e di utenti comuni che pongono in vendita proprie immagini e video sessualmente espliciti. Sebbene l'accesso sia consentito solo dai 18 anni in poi, sono noti diversi casi di adolescenti che sono riusciti ad aggirare il limite, attratti dal mito di facili guadagni. Per loro sono massimi i rischi di rimanere vittime di sexting, cyberbullismo, pedopornografia e revenge porn.



## Twitch

Twitch è la nuova piattaforma di live-streaming che sta letteralmente spopolando fra i teenager, tanto da arrivare a oscurare parzialmente social più consolidati come Facebook e YouTube. La piattaforma, che conta oltre 15 milioni di account, nasce con lo scopo di permettere agli streamer di mostrare in tempo reale con i follower del proprio canale le proprie sessioni di gioco o altri contenuti di intrattenimento. La dimensione di community è rafforzata da strumenti come le chat e la moneta virtuale ("bit") con cui i follower possono sostenere i propri "creator" e ottenere gadget personalizzati. Per quanto sia possibile inserire filtri, bloccare e segnalare account, non è disponibile il tipico servizio di "parental control": data la natura imprevedibile dello streaming, non è raro incappare in situazioni in cui viene utilizzato un linguaggio per adulti. Per questo motivo e per la bassa soglia dell'età minima per accedere (13 anni) è consigliabile che i genitori vigilino sull'utilizzo che i figli fanno di questa app.



## Tinder

Tinder è un app di appuntamenti destinata agli adulti che offre la possibilità di incontri di coppia. In realtà viene spesso usato per incontri sessuali casuali. È possibile che i bambini accedano all'app e, così facendo, si trovino a visualizzare immagini del profilo più adatte ad un pubblico adulto. La funzionalità di geocalizzazione e di anonimato di Tinder potrebbe incentivare i predatori online a compiere molestie o fare stalking. A differenza di altre app che si basano su una rete di amici, Tinder si basa sull'idea di condividere il proprio profilo e le proprie immagini con estranei che potenzialmente potrebbero incontrare. I genitori dovrebbero avvertire i propri figli che questa app è pensata solo per gli adulti e i bambini che la sperimentano possono finire vittime di malintenzionati.



## Tellonym

Tellonym, creata nel 2016 da tre studenti tedeschi, è una app di messaggistica sempre più popolare tra gli adolescenti, che fornisce agli utenti la possibilità di chiedere e rispondere a domande in modo anonimo e non. La piattaforma, dall'accesso gratuito e con un'età minima di 17 anni, consente agli iscritti di inviare dei messaggi ("tell") e rispondere alle domande degli utenti condividendo pensieri su ogni tipo di argomento. Tellonym si propone come un aiuto per comprendere meglio se stessi e gli altri, grazie alla possibilità di porre domande che non si avrebbe il coraggio di fare senza la sicurezza garantita dall'anonimato. Come tutte le altre chat anonime, tuttavia, se utilizzata in modo poco responsabile può esporre bambini e adolescenti (nel 70% dei casi ragazze) a subire atteggiamenti aggressivi, con forte rischio di cyberbullismo e sexting. Per queste ragioni la app ha previsto diverse funzionalità di controllo parentale, con l'obiettivo di minimizzare il rischio per i giovanissimi.



## Giochi Online

Molti degli stessi pericoli che affrontano i giovani utenti dei social media - come i predatori on line, cyberbullismo, contenuti inappropriati e dipendenza da Internet - sono presenti anche nel mondo dei giochi online. I genitori dovrebbero essere consapevoli della natura dei giochi online per bambini, e che molti di questi hanno caratteristiche a sfondo sessuale e contenuto violento. Mentre molti film e altro intrattenimento contengono in modo simile un contenuto inappropriato, i giochi online hanno l'aggravante di essere giochi di ruolo che possono potenzialmente lasciare un maggiore impatto negativo sul comportamento dei bambini nel mondo reale. Rapporti online con altri giocatori possono causare altre criticità.

## Cosa dovremmo dire ai bambini?

*Oggi non è facile essere genitori, specie perché la rivoluzione dei social media non sembra esaurirsi. Per usare Internet e le sue app in modo responsabile, presentiamo alcuni suggerimenti per iniziare la conversazione con i bambini.*

### Iniziate la conversazione

Voi conoscete i vostri figli meglio di chiunque altro. Sedetevi con loro e commentate i vantaggi di Internet: dall'apprendimento ai social network, all'intrattenimento e alla creazione di opportunità. Insieme, scoprite i modi in cui Internet amplierà i loro orizzonti. Nella stessa conversazione, adottate un piano realistico per evitare l'uso improprio di Internet. Usate il linguaggio più adatto per avviare un dialogo aperto e sincero.

Se i vostri figli utilizzano già Internet, scoprite quali siti e app stanno utilizzando, come funzionano queste app e se hanno avuto problemi (come il contatto con estranei e cyberbullismo). Fate sapere ai vostri figli che se qualcuno li fa sentire a disagio o se qualcuno sta dicendo cose dannose o contro di loro online, possono confidarvelo senza timori. Dovrebbero sentirsi a proprio agio nel raccontarvi qualsiasi esperienza negativa online che stanno vivendo e sapere che troverete il modo di aiutarli.

### Familiarizzate con il galateo di Internet

Proprio come ci sono regole sociali all'interno delle nostre comunità, ci sono regole online di base che dovremmo seguire. La cosa più importante da chiedersi è - "dovrei davvero postare questo?", "qualcuno sarà ferito o offeso da questo post?". Prendendo 10 o 30 secondi per rivedere ciò che pubblichiamo online e le ripercussioni di questi post è parte della nostra responsabilità sociale.

Se un post non è qualcosa che condivideremo con la nostra famiglia, è probabilmente una buona idea non condividerlo anche online.

### Create regole e rendetevi conto che non potete monitorare le mosse dei vostri figli online in ogni momento

Create regole online generali per proteggere i vostri figli. Stabilite che i vostri figli richiedano la vostra autorizzazione prima di scaricare qualsiasi app sul proprio dispositivo mobile in modo che ne siate a conoscenza. Quando i vostri figli vogliono unirsi alle piattaforme sui social media, compilate insieme le impostazioni di sicurezza del profilo per scegliere quelle più idonee.



### Consigliate ai vostri figli di non condividere le password con nessuno

Questo include i migliori amici e fidanzati o fidanzate. Condividere le password potrebbe potenzialmente danneggiare l'identità online di vostro figlio, ed è meglio tenerle per uso personale.

### Impostate limiti di età sugli smartphone, laptop, tablet e desktop dei vostri figli

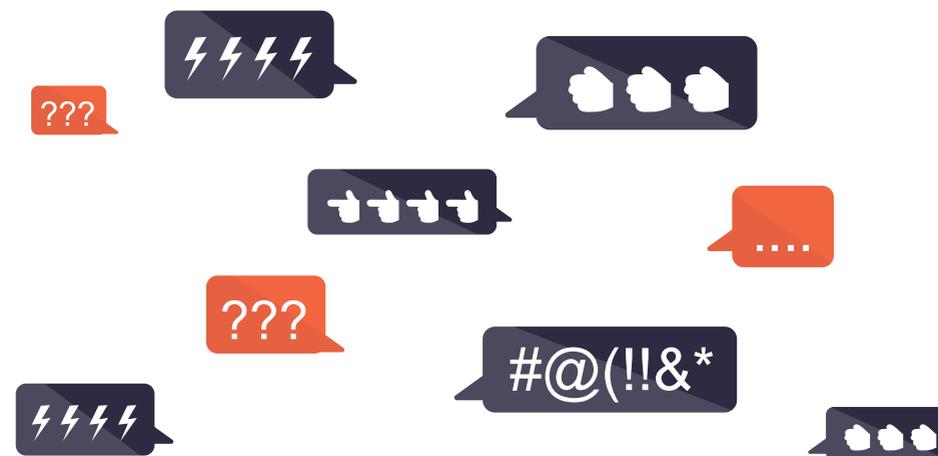
Come genitori, in genere potete impostare limiti di età sugli smartphone, laptop, tablet e desktop dei tuoi figli, disabilitando la possibilità di scaricare o acquistare determinate app e programmi. Con l'aggiornamento di software e hardware alla velocità della luce e con la tecnologia indossabile che si fa strada sulla scena, i genitori dovrebbero familiarizzare con i manuali utente per essere in grado di capire come funzionano, creando così un ambiente sicuro per i loro figli.

## Domande da fare ai vostri bambini sull'uso di Internet

Q1

### Uso tecnico generale

1. Qual è il tuo sito web preferito? Cosa fai su questo sito? hanno scritto su di te, che non è vero ma pensano che lo sia?
2. Su quali siti web navigano i tuoi amici?
3. Sei mai stato contattato da qualcuno in rete che non conosci? Se sì, che cosa voleva? Cosa hai fatto? Come hai risposto?
4. Come proteggi la tua sicurezza on line?
5. Ti preoccupi se le persone leggono ciò che altri
6. Hai mai parlato con qualcuno online che non è della tua scuola?



Q2

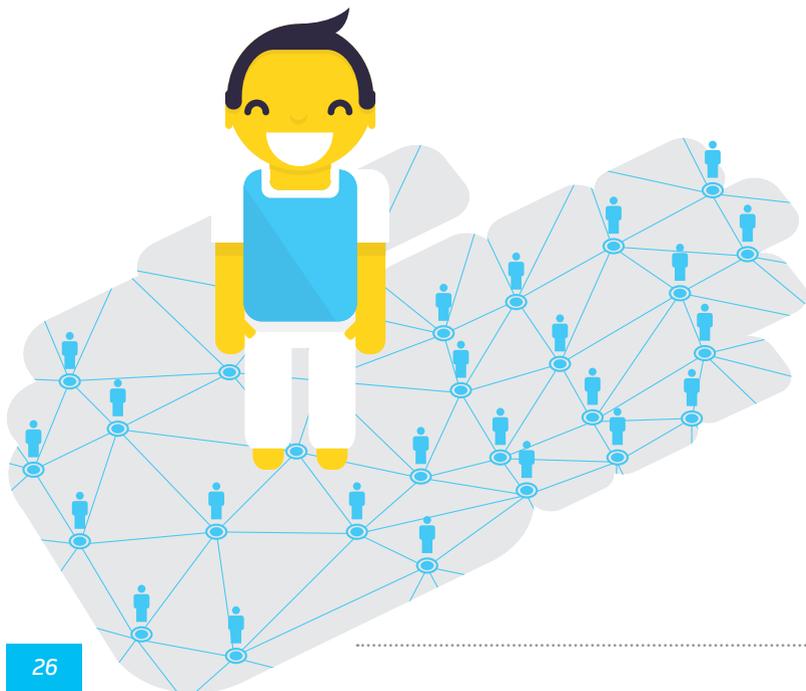
### Cyberbullismo

1. Hai mai discusso o pubblicato aggiornamenti dannosi sul tuo Instagram, Facebook, Twitter o altri social media o siti? Perché?
2. Hai mai dovuto eliminare un post o un commento sulla tua pagina che è stato scritto da qualcun altro?
3. Il cyberbullismo si verifica spesso? Se fossi vittima di cyberbullismo me lo confideresti?
4. Pensi che la tua scuola prenda il cyberbullismo sul serio?
5. Hai mai dovuto contattare un insegnante o qualcun altro a scuola a causa di una cyberminaccia? Se è così, hanno fatto qualcosa al riguardo e ti hanno aiutato?
6. La tua scuola ha un sistema per segnalare anonimamente bullismo e cyberbullismo?
7. Pensi che i tuoi amici ti avrebbero appoggiato se avessi confidato loro che stavi facendo del cyberbullismo?
8. Sei mai stato attaccato verbalmente durante giochi online?
9. Hai mai dovuto lasciare un gioco online perché qualcuno ti ha infastidito?
10. Ci sono stati pettegolezzi a scuola su di te basati su qualcosa detto online?
11. Hai mai scoperto chi ha messo in giro il pettegolezzo? Cosa hai fatto quando l'hai scoperto?
12. Hai mai bloccato qualcuno online perché ti sei sentito molestato? Così facendo, ha smesso?

## Q3

## Sexting

1. Hai mai inviato immagini attraverso messaggi? Ricevi immagini? Se sì, da chi?
2. I bambini a scuola scattano foto con i loro cellulari? Sai cosa ci fanno?
3. Hai mai usato Skype o FaceTime con gli amici?
4. Usi Snapchat? Mi spieghi come funziona? Pensi che le foto siano davvero completamente sparite?
5. Hai mai fatto fare o dire qualcosa a qualcuno di inappropriato su Skype o Snapchat?
6. Sai cos'è il sexting? Un adulto a scuola ti ha mai parlato di sexting?
7. Uno sconosciuto ti ha mai inviato messaggi espliciti? Come hai reagito a questi messaggi?
8. Un amico ti ha mai inviato testi o immagini esplicite o offensive?
9. Conosci le conseguenze che possono essere causate dall'invio di immagini inappropriate (leggi sulla pornografia infantile)?



## Q4

## Social media sicuro

1. Quale social media usi più di frequente? Quanti amici o follower hai?
2. Che tipo di persone incontri su Instagram e Facebook? Ti connetti con persone che conosci? O incontri persone casualmente?
3. Hai un sacco di amici o accetti le richieste di amicizia da parte di sconosciuti? Se sì, come le gestisci?
4. Usi Twitter? Per che cosa? Chi segui? E chi ti segue?
5. Sai come utilizzare le impostazioni sulla privacy di Instagram, Facebook e Twitter?
6. Hai impostato la privacy in modo che solo quelli che tu accetti come amici possono vedere ciò che pubblichi? Come sai chi può vedere le tue informazioni?
7. Che tipo di informazioni personali stai postando on line? Hai mai pubblicato il tuo nome completo? Età? Scuola? Numero di telefono? Posizione attuale?
8. Sei mai stato taggato in una foto in un modo che ti ha fatto arrabbiare?
9. Sai come modificare le tue impostazioni sulla privacy in modo che se qualcuno vuole taggarti in un post o foto, devi approvarlo?
10. Sai come eliminare il tag dalle immagini?
11. Ritieni che i social media vengano usati per sfogare le proprie frustrazioni? I tuoi amici si sfogano online? Le persone commentano? Che cosa dicono?
12. Che tipo di video guardi su YouTube? Pubblici mai video?
13. Hai mai segnalato video inappropriati visti su YouTube? O su qualsiasi altro sito web?
14. Qualcun altro conosce la tua password o passcode per qualsiasi sito o app di social media? Oppure per il tuo computer o il tuo cellulare?

## Come possiamo educarci regolarmente ad un uso sicuro di Internet?

La realtà è che con la velocità con cui Internet cambia è pressoché impossibile tenere traccia dell'utilizzo online che ne fanno i propri figli. Come possiamo, tuttavia, continuare a mantenere aperta la comunicazione con i nostri figli per garantire che si sentano sicuri nel condividere con noi anche situazioni ingiuste o pericolose? Per chi ha figli che utilizzano smartphone, ci sono app disponibili per monitorare la posizione dei bambini, come Life 360, disponibile gratuitamente su Android e iOS. TimeAway

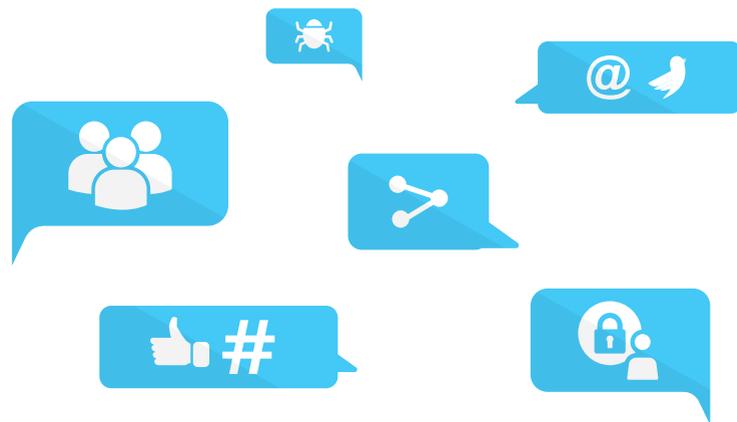
è uno strumento per Android gratuito che consente ai genitori di posizionare blocchi, impostare i limiti dell'app, tracciare la posizione del proprio figlio e pianificare il tempo di utilizzo dello smartphone. L'app gratuita MamaBear su Android e iOS aiuta i genitori a rintracciare l'attività sui social media dei figli, gestire l'app utilizzando e geo-localizzando il bambino. L'ultimo ma costoso monitoraggio di Internet è il software mSpy, disponibile per tutti i dispositivi e computer in tutto il mondo.

## Conclusioni



Per i milioni di utenti principianti e bambini piccoli, Internet apre le porte a fantastici contenitori di informazione e apprendimento ... ma anche ai rischi di furto, frode, bullismo, abuso e malware on line. Siamo tutti responsabili di assicurarci che i nostri bambini e ragazzi siano dotati non solo di mezzi per accedere a Internet, ma di giuste informazioni per rimanere protetti durante l'apprendimento e comunicare su Internet. Potrebbe sembrare piuttosto impegnativo per tutti noi perché i nostri figli oggi stanno quasi

sempre su Internet con i telefoni cellulari - molto più difficili da supervisionare e monitorare 24 ore su 24. La sicurezza dei nostri bambini pur essendo 'Online' sui loro telefoni è basata sul dialogo e sulla fiducia che siamo stati in grado di coltivare. Ecco come sviluppare le loro competenze e aumentare la loro resilienza nel mondo online. Sommando tutto questo abbiamo sintetizzato in questa guida alcune semplici regole.



### Limitate il tempo di esposizione dei vostri bambini online

Offrite ai vostri figli una quantità fissa di tempo online gratuito per chattare, giocare o accedere ai siti sociali, ma dopo, limitate il loro ricorso al computer o al cellulare per svolgere i compiti o altre attività. Continuate a parlare e ad imparare insieme ai vostri figli. Parlate e ponetevi reciprocamente domande sulla tecnologia. Comunicate apertamente e cercate di mantenere il tono positivo e fiducioso. È importante che i vostri bambini sappiano che possono parlare con voi – sia di argomenti positivi che negativi, come quando commettono un errore su Internet o visitano un sito che non dovrebbero.

È importante che non vengano puniti troppo duramente quando commettono un errore perché non rinuncino a confidarsi la volta successiva.

### Condividete le informazioni su Internet stando vicini

Invitateli a mostrarvi i loro siti web preferiti e altri servizi Internet e assicuratevi di avere informazioni per gli account che hanno online.

Non permettere ai vostri figli di condividere le loro password con nessun altro all'infuori di voi. Cercate di realizzare in una zona centrale nella vostra casa la postazione Internet per i bambini in modo da non perderli d'occhio mentre sono online.

Definite regole, criticate i contenuti e comunicate apertamente con i vostri figli. Tenere i bambini al sicuro significa impostare linee guida e avere criticità e discussioni non giudicanti sul comportamento in Internet. Se i vostri figli si sentono a proprio agio con queste conversazioni, saranno più propensi ad affrontare un problema online – come un bullo o un sito web inadatto o discutibile.

## Vocabolario Internet

### 0101 Algoritmo

Calcoli matematici basati su passi procedurali per elaborare i dati e produrre un ragionamento sistematico. Esempio: l'algoritmo di Facebook aiuta l'utente a scoprire contenuti per lui pertinenti in base al suo profilo e alla sua storia. Anche l'algoritmo di Facebook sa interpretare come a un utente piace "essere" su Facebook e mostra informazioni per lui rilevanti.

### App

Abbreviazione di 'software applicativo', l'app è un programma per computer utilizzato su dispositivi mobili come smartphone e tablet. Esempio: Google Maps è un'applicazione che utilizza il GPS (tecnologia di posizionamento globale) per aiutare gli utenti su ubicazioni e direzioni. Oggi esistono circa 6,5 milioni di app, e ciascun utente ne ha mediamente installati 80 sul proprio smartphone.

### Cyberbullismo

Se il tradizionale fenomeno del bullismo si consuma in ambienti definiti (tipicamente, la scuola) e si basa sulla capacità di un individuo o di un gruppo di predominare per lo più fisicamente sulle proprie vittime, il bullismo in Rete non conosce limiti: può svolgersi 24 h. al giorno, ovunque, e chiunque può essere potenzialmente vittima o persecutore, con i propri connotati oppure in forma anonima. Se nel bullismo il timore principale è il danno fisico, nel cyberbullismo è massimo lo stress emotivo, che può portare chi lo subisce ad avere l'impressione di non avere scampo. Per maggiori informazioni e suggerimenti su come contrastarlo visita il nostro sito alla pagina [www.unicef.it/cyberbullismo](http://www.unicef.it/cyberbullismo)

### Chatroom

Le chat (dal verbo inglese "to chat", chiacchierare) sono programmi a sé stanti oppure integrati all'interno di siti web, social network, giochi o servizi commerciali. Possono essere del tipo "one to one" (messaggistica istantanea tra due utenti) oppure "one to many" (chat di gruppo), anche se questa differenziazione è sempre più sfumata, con presenza di un moderatore o – più spesso – senza alcun controllo sui contenuti. Chat come WhatsApp, Messenger o Snapchat sono strumenti di uso quotidiano per gli adolescenti di tutto il pianeta: mentre contribuiscono alla libertà di espressione e alla costruzione dell'identità dei giovanissimi, possono al tempo stesso celare rischi per la loro privacy e per la sicurezza. È fondamentale che i genitori aiutino i ragazzi a un uso di consapevole di questi strumenti e al rispetto delle regole (v. "netiquette")



### **Blog**

Un aggregatore di testi e/o contenuti multimediali, contraddistinti per data, che trattano una tematica specifica e che di norma consentono agli utenti di interagire tramite commenti. I primi blog sono nati negli USA nel 1997 e si stima che oggi ne esistano ben 500 milioni. Quando i post di un blog sono costituiti da video siamo di fronte a un video-blog o "vlog".



### **Hacker**

Un utente di Internet che utilizza dati elettronici per ottenere accesso ai dati di altri utenti. Gli hacker possono spesso accedere a informazioni personali come il conto corrente bancario e profili utente per eseguire il furto di identità.



### **Predatore online**

Qualcuno che usa Internet per localizzare qualcuno altro in modo dannoso, specialmente qualcuno che si serve di Internet per attirare i bambini e metterli in pericolo.



### **Motore di ricerca**

Un programma che offre agli utenti la capacità di effettuare ricerche, in genere con parole chiave o lettere, e trovare informazioni in tutta la rete web.



### **Social media**

Applicazioni e siti web che consentono agli utenti di interagire fra loro a seguito della creazione di profili individuali (account), condividendo contenuti testuali o multimediali. I social media sono di gran lunga gli ambienti più frequentati dal web, con oltre 4 miliardi di utenti attivi e colossi come Facebook, WhatsApp, YouTube che hanno superato la soglia dei 2 miliardi di account ciascuno. L'ecosistema dei social network si va sempre più differenziando: se tra gli adulti predominano quelli incentrati sull'elemento testuale come Facebook, Twitter o Reddit, gli adolescenti prediligono piattaforme come Instagram, TikTok o Twitch, caratterizzate dal consumo rapido e continuo di contenuti multimediali.



### **Streaming**

Media, come un video, una canzone o una partita di calcio che si consuma online quando viene inviato al proprio computer o telefono cellulare in un flusso continuo di dati.



### **Virus e malware**

Sebbene sia uso comune definire "virus informatico" tutto ciò che danneggia un computer o un dispositivo mobile, questo termine dovrebbe applicarsi ai soli programmi (software) che si autoreplicano all'interno della macchina infettata, imitando il comportamento dei virus in un organismo vivente. I virus sono in realtà solo una parte della vastissima famiglia dei "malware" (dall'inglese "malicious software"), programmi che hanno la più ampia gamma di forme, strategie di diffusione e finalità. A seconda dei casi, i malware possono spiare l'attività compiuta dall'utente, carpire dati personali a scopo di truffa (phishing) o ricatto, prendere il controllo del computer per diffondere pubblicità indesiderata (spamming), infettare reti aziendali o condurre attacchi informatici mirati contro specifici siti o server. Il modo migliore per proteggere un dispositivo dai malware è installare e mantenere sempre aggiornato un programma antivirus, oltre ad applicare norme di buon senso come, ad esempio, non aprire allegati di email ricevute da sconosciuti. Per quanto sia nota la pericolosità di queste insidie, si stima che il 25% dei computer nel mondo non sia protetto da antivirus.



### **Netiquette**

Il codice di buon comportamento della Rete (il termine associa il francese "étiquette" all'inglese "net") è costituito da regole consuetudinarie e principi di buonsenso, finalizzati ad assicurare una convivenza pacifica e rispettosa tra gli utenti del web. Sebbene non abbia valore di legge, le sue norme sono considerate valide dall'assoluta maggioranza del popolo web e ricorrono spesso nei termini di uso dei singoli siti, app o social media. Apprendere e applicare la netiquette dovrebbe essere considerato un dovere etico di ogni utente della Rete, minorenni o adulti che sia.



### **Parental control**

La crescente esposizione di bambini e ragazzi a Internet, soprattutto tramite smartphone, ha reso indispensabile sviluppare una serie di software e servizi finalizzati a proteggere i soggetti più vulnerabili da contenuti violenti, pornografici o pericolosi. Oggi è possibile installare sui dispositivi dei propri figli dei "filtri genitoriali" (parental control) impedendo l'accesso diretto o tramite motori di ricerca a siti per adulti o con altre caratteristiche negative, di monitorare o limitare i tempi di utilizzo del dispositivo stesso e di vincolare l'installazione di nuove app all'autorizzazione esplicita di un genitore.



CAPITOLO QUATTRO

## Figli dell'era digitale Raccomandazioni

Più di 175.000 bambini vanno online per la prima volta ogni giorno - un bambino ogni mezzo secondo.

L'accesso digitale espone questi bambini a una ricchezza di benefici e opportunità, ma anche a una serie di rischi e danni, tra cui l'accesso a contenuti dannosi, sfruttamento e abuso sessuale, cyberbullismo e uso improprio delle loro informazioni private.

Mentre i governi e il settore privato hanno compiuto alcuni progressi nella formulazione di politiche e tentativi per eliminare i rischi online più eclatanti, è necessario compiere maggiori sforzi per comprendere e proteggere pienamente le vite online dei bambini.

In tutto il mondo 1 utente su 3 di Internet è un bambino, eppure, ancora troppo poco è stato fatto per proteggere i minorenni dai pericoli del mondo digitale, per salvaguardare le tracce di informazioni che le loro attività online creano e per aumentare il loro accesso a contenuti online sicuri e di qualità.

L'UNICEF chiede con forza e cooperazione ai governi, alla società civile, alle agenzie delle Nazioni Unite e alle altre organizzazioni internazionali e, soprattutto, al settore privato di mettere i bambini al centro della politica digitale ispirandosi alle seguenti raccomandazioni:

- 1. Fornire a tutti i bambini accesso a risorse online di qualità a prezzi contenuti.** Significa creare incentivi per incoraggiare le aziende di telecomunicazione e le imprese tecnologiche a ridurre i costi della connettività; tenere in considerazione le esigenze dei bambini non connessi nello sviluppo di piani infrastrutturali; investire in un maggior numero di hot spots pubblici e nella creazione di contenuti multimediali culturalmente e linguisticamente più adeguati; infine, affrontare tutte le barriere, incluse quelle culturali, che impediscono ai bambini, specialmente alle ragazze, di collegarsi online.
- 2. Proteggere i bambini dai rischi online.** Ciò implica un maggiore coordinamento a livello internazionale e nazionale e una profonda collaborazione tra i sistemi giudiziari e l'industria tecnologica, per vigilare sulla tecnologia digitale che permette e nasconde il traffico illecito di minorenni e la diffusione di materiale pedopornografico online.
- 3. Tutelare la privacy dei bambini online.** Questo significa sollecitare il settore privato e i governi a impegnarsi maggiormente per proteggere i dati dei minorenni da un uso improprio, rispettandone la crittografia; imporre l'applicazione di norme internazionali per la raccolta e l'utilizzo dei dati online sui bambini; e insegnare ai bambini come difendersi dalle minacce alla propria privacy.

- 4. Insegnare l'alfabetizzazione digitale per formare bambini consapevoli, impegnati e sicuri online.** Ciò significa sostenere una maggiore collaborazione tra governi e tecnologi per sviluppare piattaforme e curricula informatici dalla scuola primaria fino alla scuola superiore, promuovendo le librerie online e sostenendo le biblioteche pubbliche nell'insegnamento di competenze informatiche; investire nella formazione degli insegnanti nella tecnologia digitale; insegnare ai bambini a riconoscere e proteggersi da pericoli online; e rendere la cittadinanza digitale una componente fondamentale dell'alfabetizzazione digitale.
- 5. Promuovere migliori pratiche aziendali e standard etici per proteggere i bambini online.** Questo comporta uno sviluppo responsabile ed etico di prodotti e di attività di marketing che riducano i rischi per i bambini, nonché

un maggiore impegno per estendere l'accesso alla connettività e ai contenuti online. Il settore privato - in particolare le aziende di telecomunicazione e le imprese tecnologiche - ha una responsabilità specifica e una capacità unica di modellare l'impatto della tecnologia digitale sui bambini.

- 6. Porre i bambini al centro delle politiche digitali.** Questo vuol dire investire maggiormente nella raccolta di dati relativi all'accesso e alle attività dei minorenni online; sviluppare quadri normativi che riconoscano le diverse esigenze dei bambini; rafforzare il coordinamento e la condivisione delle conoscenze a livello globale per affrontare le sfide del mondo digitale; consolidare la collaborazione con le organizzazioni per la tutela dell'infanzia; e impegnarsi in maniera sistematica con i responsabili politici e i legislatori.



???



safe internet

