

Vivi Internet, al meglio.



# Guida per le famiglie

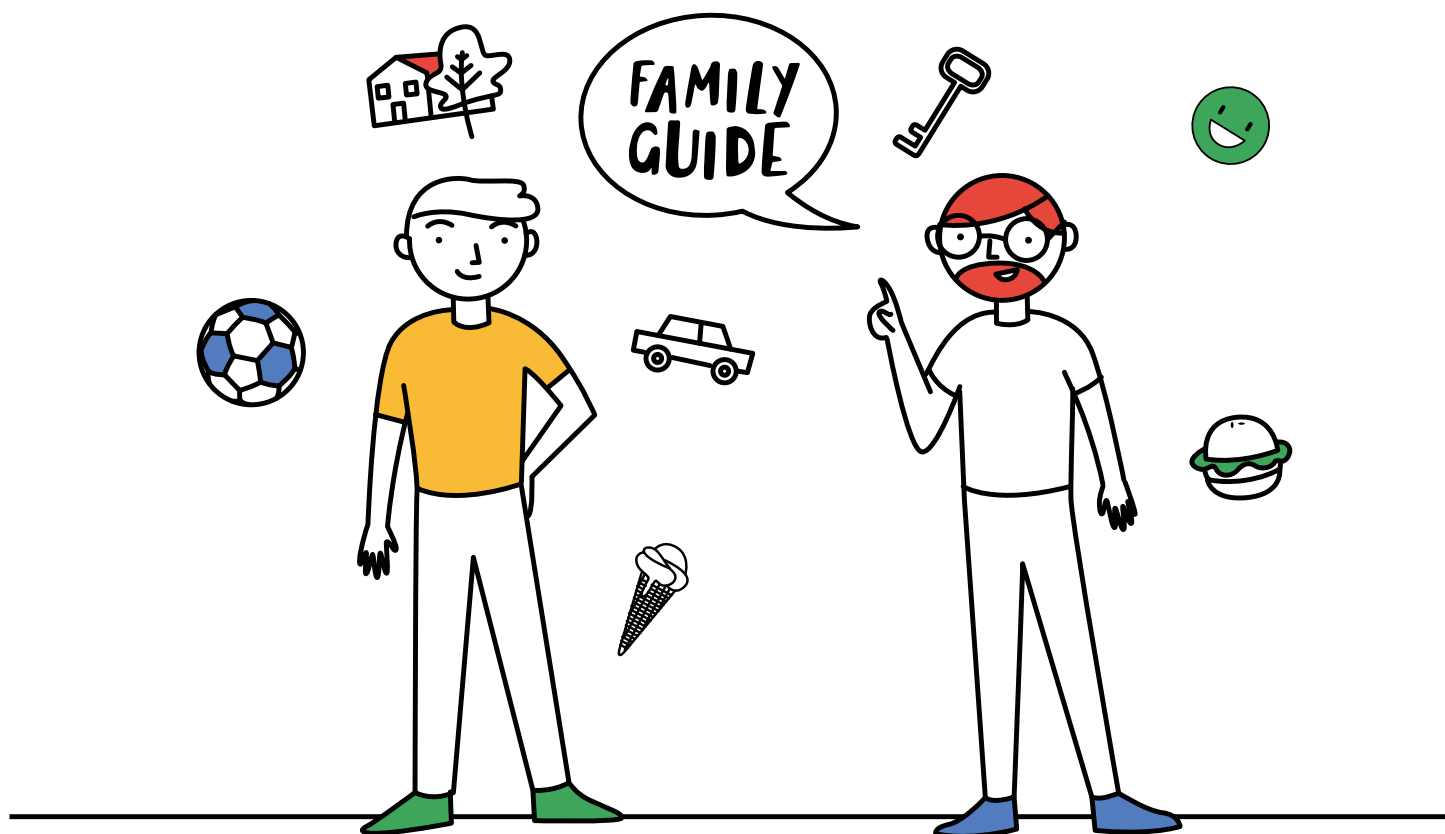
Utilizza la tecnologia con buon senso

Impara a distinguere il vero dal falso

Custodisci le tue informazioni personali

Diffondi la gentilezza

Nel dubbio, parlane



# Vivi Internet, al meglio.▲

Gentile genitore o tutore,

Vivi Internet, al meglio ha l'obiettivo di aiutare i più giovani a vivere il Web responsabilmente, attraverso semplici strumenti per apprendere i principi base dell'educazione digitale.

Il progetto, che si pone in linea di continuità con le iniziative avviate negli anni scorsi da Google con Altroconsumo per formare le persone all'utilizzo del Web in sicurezza, si propone di promuovere la cittadinanza digitale tra i giovani attraverso un percorso formativo che si rivolge ai ragazzi, alle famiglie e agli educatori. Vivi Internet, al meglio mette al centro cinque tematiche di assoluta pertinenza: reputazione online e benessere digitale, phishing e truffe, privacy e sicurezza, molestie e bullismo online, segnalazione di contenuti inappropriati.

Oggi, sicurezza e cittadinanza digitale sono due componenti fondamentali dell'insegnamento in aula, ma la famiglia sarà sempre alla base dell'apprendimento per i ragazzi e avere sane abitudini online non fa eccezione. La tecnologia si muove rapidamente e rimanere al passo con i tempi può rappresentare una sfida.

Abbiamo creato questa guida per aiutare le famiglie a introdurre e mettere in pratica più facilmente buone abitudini digitali nella vita di tutti i giorni.

Questa guida, ricca di informazioni utili, aiuterà te e i tuoi figli a discutere, imparare e riflettere insieme sulle cinque aree che vi faranno vivere Internet, al meglio:

**Utilizza la tecnologia con buon senso**

**Impara a distinguere il vero dal falso**

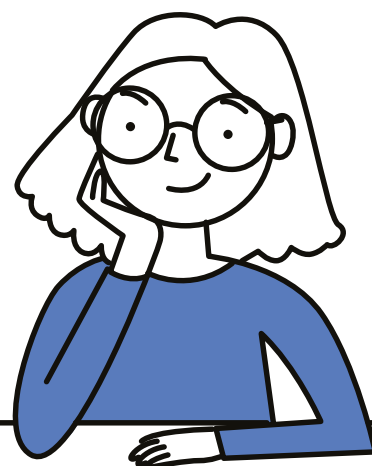
**Custodisci le tue informazioni personali**

**Diffondi la gentilezza**

**Nel dubbio, parlane**

Questa guida è stata creata come una risorsa indipendente per aiutare la tua famiglia a imparare cosa siano la sicurezza e la cittadinanza digitale. Oltre alle principali raccomandazioni rivolte ai genitori per ognuna delle cinque lezioni, troverai il lessico e le attività che ti aiuteranno a gettare solide fondamenta per un utilizzo di Internet sicuro e di successo.

Divertiti a esplorare Vivi Internet, al meglio!





**Utilizza la tecnologia  
con buon senso**

pag 01



**Impara a distinguere  
il vero dal falso**

pag 05



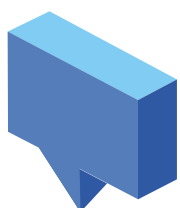
**Custodisci le tue  
informazioni personali**

pag 09



**Diffondi la gentilezza**

pag 13



**Nel dubbio, parlane**

pag 19

# Utilizza la tecnologia con buon senso

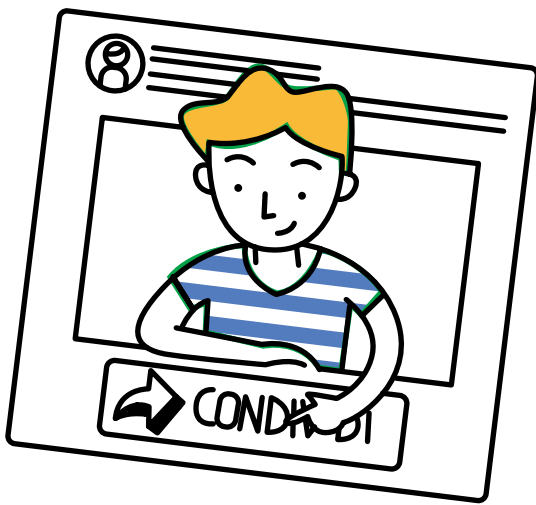
Gli insegnanti e i genitori sanno che alcuni errori commessi sui dispositivi digitali e su Internet in giovane età potrebbero comportare danni alla reputazione o avere conseguenze permanenti sulla tua vita. È fondamentale far comprendere ai propri figli che un uso equilibrato e intelligente dei dispositivi, dei social e più in generale di Internet può rappresentare una opportunità di apprendimento e di vero e proprio benessere digitale, con effetti positivi anche sulle relazioni personali e sul percorso di studio.

È necessario quindi rendere i ragazzi più consapevoli sui temi della reputazione online e del benessere digitale.



L'età adolescenziale, per sua natura, è un periodo della vita in cui prevalgono gli **istinti**, le azioni fatte di getto, **poco ragionate**. E questa propensione si ripercuote inevitabilmente sulle interazioni online degli adolescenti. Prima che si imbattano in situazioni spiacevoli per la loro reputazione, vediamo qualche **consiglio utile**.

## Quali sono i rischi



### Reputazione online

Quando si parla di reputazione online, i rischi non sono pochi, soprattutto quando c'è di mezzo la credibilità sociale.

L'insieme di foto, video, informazioni che rendono riconoscibili gli utenti online viene definita ombra digitale.

La qualità o meno di quest'ombra digitale definisce la felicità presente e futura di tutti, adolescenti compresi.

Purtroppo, i ragazzi condividono foto, messaggi e video il cui contenuto spesso è molto riservato. Ad esempio:

- Pensano che mandare al proprio partner foto intime rimanga una faccenda tra loro, ma non è così. Chi riceve questo contenuto è come se fosse in possesso di una potentissima arma di ricatto.
- Pensano che postare un commento molto offensivo sulla pagina di un conoscente non avrà conseguenze, ma ne avrà. Oggi un contenuto negativo è trattato alla stregua di una diffamazione, con tutte le implicazioni penali connesse.
- Pensano che condividere con qualcuno un video di cui potrebbero vergognarsi non sia una cattiva idea. Invece, anche in questo caso, l'effetto boomerang può presentarsi in qualunque momento.

### Benessere digitale

In quanto nativi digitali, i giovani spesso possono non rendersi conto dell'impatto che un utilizzo eccessivo della tecnologia può avere sulla loro vita, il loro rendimento scolastico e i loro rapporti interpersonali.

## Come si può agire

Da genitore, quello che puoi fare è invitare i tuoi figli a una **riflessione** molto semplice, a partire da alcune domande: Mostreresti questo contenuto dal vivo? Se non lo faresti di persona, perché lo dovresti fare online? E più in generale, sei sicuro che la tecnologia non ti distraiga troppo da ciò che per te conta veramente?

## Reputazione online

Parla coi tuoi figli del concetto di reputazione online, e di come, anche sul Web, si debbano applicare alcuni principi base della vita offline:

- Tutto ciò che riguarda la famiglia e gli amici è riservato.
- Tutto ciò che riguarda la propria vita sentimentale è riservato.

Queste regole si applicano ovviamente anche agli altri, di cui è importante rispettare i limiti.

È quindi bene affrontare questi temi coi tuoi figli, facendo presente i seguenti punti:

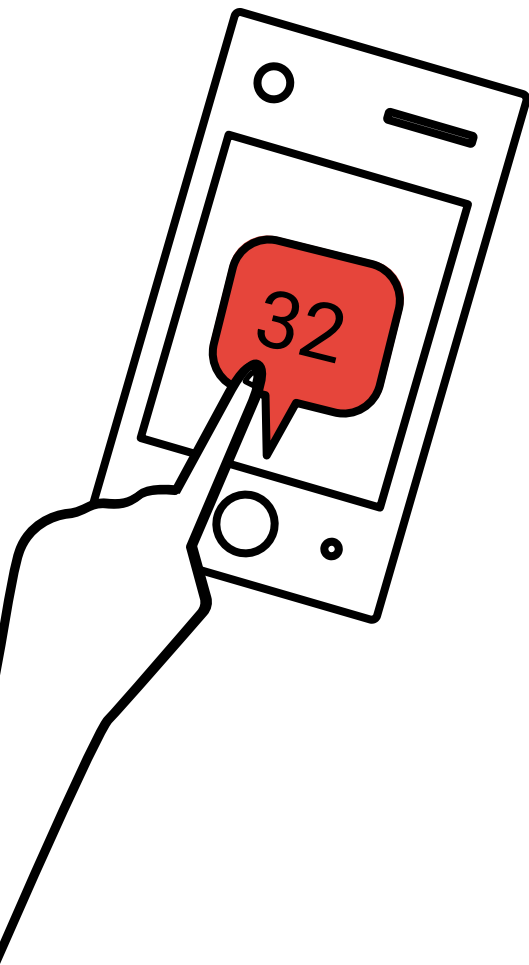
- Con una semplice ricerca online puoi renderti conto in prima persona di quante informazioni si trovino sulle persone e come sia facile farsi un'idea (spesso errata) di quella persona.
- Peraltro, nessuno potrà assicurarti che quei dati siano stati ottenuti in maniera legittima. Prima di comunicare su qualunque sito contenuti personali mettiti nei panni di chi ti vede: cosa penserebbero di te se giudicassero solo ciò che vedono?

## Benessere digitale

In generale, è utile anche educare i ragazzi all'utilizzo consapevole della tecnologia, evitando di adottare un approccio rigido, bensì dialogando con loro sul modo migliore di utilizzare i dispositivi. Parla coi tuoi figli del concetto di "Benessere Digitale", spiegando loro alcune buone prassi per raggiungere un rapporto equilibrato della tecnologia.

Ecco alcuni consigli:

- Chiedi loro se le attività che svolgono sui dispositivi sono appropriate per lo sviluppo, se migliorano l'umore e se sono educative.
- Rifletti con loro sul ruolo che la tecnologia ha nella loro vita, invitandoli a seguire alcune buone pratiche per raggiungere un rapporto equilibrato della tecnologia. Ecco alcuni esempi i piccoli consigli:
  - disattivare le notifiche sul tuo telefono
  - ricaricare lo smartphone lontano dal letto
  - scegliere la modalità aereo quando sei a tavola o in compagnia.
- Invita i tuoi figli a trovare il giusto equilibrio tra tempo speso sul Web e all'aria aperta: chiedi loro di riflettere sul come utilizzano i dispositivi, invitandoli a fare in modo che non diventino per loro un qualcosa che li allontana da ciò che li circonda.



## Attività

**Per i genitori:** sai come aiutare i tuoi figli a vivere Internet, al meglio?

Fai [questo test](#) per scoprire se per te il Web non ha segreti o se, invece, potresti imparare cose nuove per aiutare i tuoi figli a navigare le complessità del mondo online.

**Per i ragazzi:** il Web è casa tua. Per imparare ad abitarlo responsabilmente guarda [questo video](#), insieme agli altri inclusi nel programma Vivi Internet, al meglio. Ti sarà più semplice riflettere sulle possibili conseguenze delle tue azioni in rete.

## Lessico

### Privacy online

Un termine generico usato di solito per definire la capacità di controllare quali dati condividi su di te online e chi può vederli e condividerli.

### Impronta digitale (o presenza digitale)

L'impronta digitale riguarda tutti i dati su di te che compaiono online. Può trattarsi di fotografie, audio, video e testi fino ai "mi piace" e ai commenti che pubblichi sui profili dei tuoi amici. Ciò che pubblichi online lascia una traccia proprio come le dita lasciano impronte su una superficie quando appoggi la mano.

### Benessere Digitale

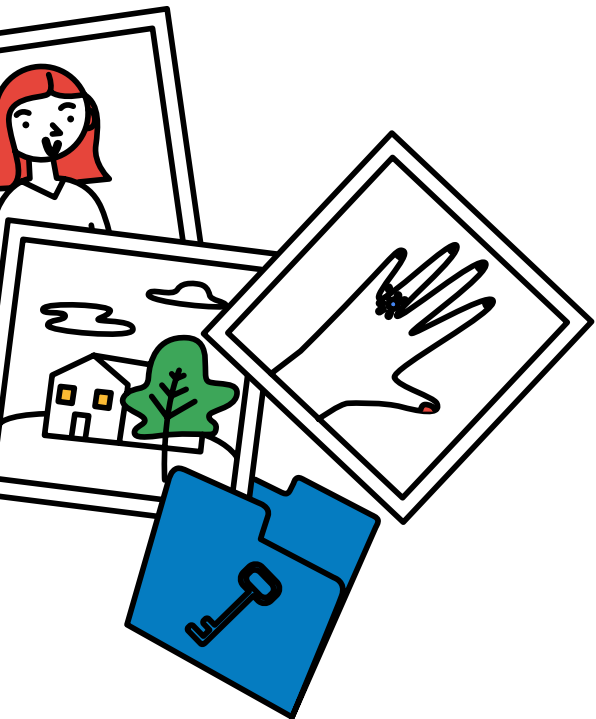
Quello stato di soddisfazione e comfort che si sviluppa in relazione al modo in cui la tecnologia fa parte della propria vita, permettendo di instaurare un rapporto bilanciato con la tecnologia.

### Reputazione

Idee, opinioni, impressioni o convinzioni che le persone hanno su di te: qualcosa di cui non hai certezza ma che di norma vorresti siano buone o positive.

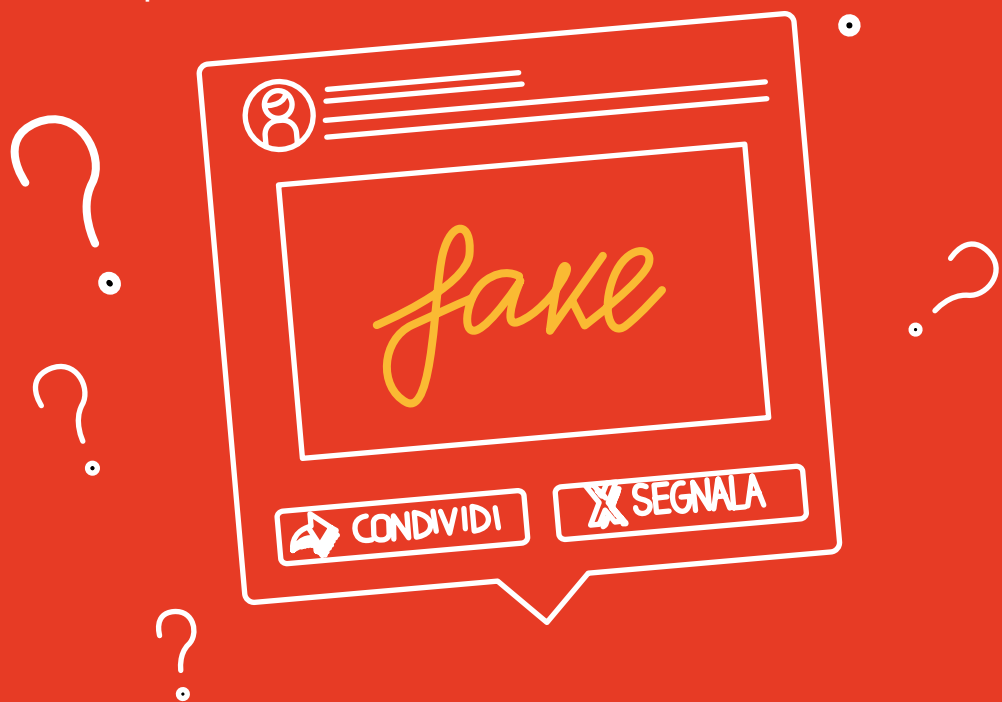
### Informazioni personali

Sono informazioni che identificano una persona precisa, come il nome, l'indirizzo, il numero di telefono, il codice fiscale, l'indirizzo e-mail ecc. Questi dati sono definiti informazioni personali o sensibili. Pensaci bene prima di condividere online questo genere di informazioni.



# Impara a distinguere il vero dal falso

Uno dei rischi più frequenti che i ragazzi corrono online è quello di essere truffati. Molti messaggi sul Web si spacciano per buoni, quando altro non sono che tentativi di rubare informazioni o danneggiare i dispositivi.





Hai mai sentito parlare di **phishing**? È una parola che ricorda il verbo inglese “to fish”, pescare. In effetti il campo semantico è molto simile: cadere in una frode online è come abboccare a un’esca. In questo caso il “pescatore” è qualcuno che cerca di accedere ai tuoi dati, come password, codici bancari o messaggi, **tramite l’inganno**.

Di solito si tratta di email che arrivano nella tua casella in cui ti invitano a fare clic su un link, inserire dati personali o rispondere a una richiesta di contatto. In tutti i casi spesso il mittente si presenta sotto le vesti affidabili di un link noto, in cui riconosci parole familiari (magari il nome della tua banca, del tuo posto di lavoro, di un locale che frequenti). Peccato che, una volta fatto clic su quel link, sarai indirizzato a un **sito dannoso** per il tuo dispositivo oppure darai accesso inconsapevolmente a dati riservati.

È così che accadono truffe e **furti di identità digitali**. Se questo può accadere a chiunque, ancora di più potrebbe accadere ai tuoi figli, che spesso navigano in mezzo a stimoli molto diversi e la cui capacità di giudizio è poco allenata.

Come fare quindi a capire che si tratta di **un’esca** e non di un sito o di un **messaggio affidabile**?

## Rudimenti di sicurezza per ragazzi che navigano



Partiamo da una buona notizia: alcuni tentativi di phishing sono facilmente riconoscibili.

La chiave di tutto risiede nell’URL del sito che apri, ovvero l’indirizzo alfanumerico che appare nella barra di ricerca.

Infatti:

- Se inizia con **https://** preceduto da un lucchetto verde significa che è un sito sicuro.
- Assicurati che l’URL combaci con ciò che stavi cercando.
- Se compaiono delle finestre pop-up, cioè finestre automatiche che non hai aperto tu, è probabile che il sito non sia affidabile.
- Se ricevi nella tua posta messaggi da mittenti sconosciuti il cui contenuto è privo di senso o non indirizzati esplicitamente a te, vuol dire che qualcuno sta provando a forzare i tuoi sistemi di sicurezza.
- Ricorda che molte volte l’istinto può aiutarti. Se un messaggio richiede informazioni personali può darsi che stia tentando di avere indizi sulla tua persona per indovinare le tue password.

## Come si può agire

Per i tuoi figli è fondamentale prendere la buona abitudine di cambiare spesso la password dei loro account e di usare password complesse. Una buona password è fatta di caratteri alfanumerici con punteggiatura e lettere maiuscole.

È bene avvisare i propri contatti se si è rimasti vittime di una frode e, imparata la lezione, segnalare il sito dannoso come spam.

## Attività

**Per i genitori:** sai come aiutare i tuoi figli a vivere Internet, al meglio?

Fai [questo test](#) per scoprire se per te il Web non ha segreti o se, invece, potresti imparare cose nuove per aiutare i tuoi figli a navigare le complessità del mondo online.

**Per i ragazzi:** il Web è casa tua. Per imparare ad abitarlo responsabilmente guarda [questo video](#), insieme agli altri inclusi nel programma Vivi Internet, al meglio. Ti sarà più semplice riflettere sulle possibili conseguenze delle tue azioni in rete.

### Motore di ricerca

È un programma che cerca e identifica le informazioni in un database che corrispondono alla query dell'utente.

### Web crawler

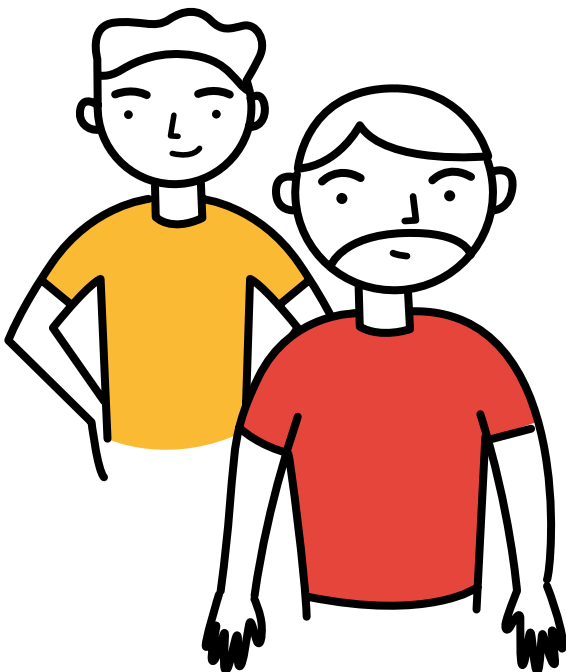
Chiamato anche "bot", è un programma eseguito all'interno del software di un motore di ricerca che esegue una "scansione" di Internet per organizzare o "indicizzare" il contenuto dei siti e dei database che visita per poter rispondere alla query che hai inserito nella casella di ricerca.

### Assistente virtuale

Come il Web crawler, gli assistenti virtuali recuperano le informazioni dai database di ricerca, dalle informazioni utente e da altri siti Web per rendere la vita un po' più facile rendendo automatica la risposta alle domande, l'esecuzione di comandi (come dare indicazioni stradali verso la nuova casa del tuo amico) o di semplici compiti come la riproduzione di una canzone.

### Risultati di ricerca

Elenco di siti Web e altre risorse visualizzati nella pagina del motore di ricerca in risposta a una ricerca.



## Lessico



### Safe Search

È una funzionalità che i genitori possono attivare o disattivare in qualsiasi momento per filtrare i contenuti che ritengono non appropriati in modo che non compaiano tra i risultati della ricerca.

### Informazioni errate

Informazioni false, fuorvianti o imprecise.

### Disinformazione

Informazioni errate (vedi sopra) utilizzate per fuorviare o ingannare volutamente le persone, ad esempio la propaganda di un avversario politico o di un altro governo.

### Verificabile

Qualcosa che si può dimostrare essere vero o corretto.

### Ingannevole

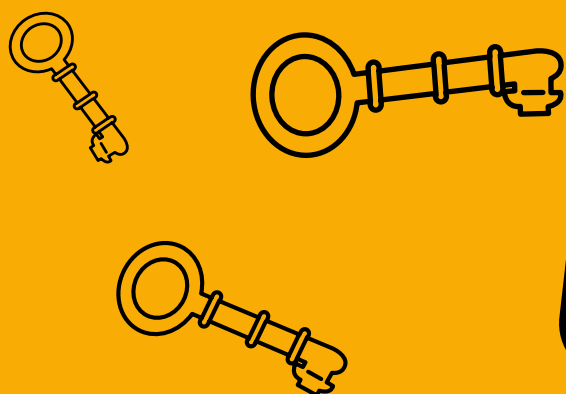
Falso; azione o messaggio progettato per ingannare, imbrogliare o fuorviare qualcuno.

### Manipolazione

Persona o gruppo di persone che controllano o influenzano un'altra persona o una situazione in modo sleale, disonesto o intimidatorio. Possono essere considerate una forma di manipolazione anche informazioni, immagini o dati modificati o presentati fuori contesto per farti credere qualcosa di non veritiero.

# Custodisci le tue informazioni personali

In una casa la cassaforte ha uno scopo ben preciso: custodire cose preziose. Quando le cose preziose sono le tue, le chiavi di quella cassaforte sono in tuo possesso. Anche sul Web hai cose preziose, molto preziose da custodire. Quindi andiamo a vedere come proteggere ciò che protegge. Le nostre chiavi, le nostre password.



Un utente medio del Web visita abitualmente almeno **4 o 5 diversi siti** su cui è necessario registrarsi con un login e una password.

Questo richiederebbe l'utilizzo di una chiave di accesso specifica per ciascun account, cosa che comporta memoria e organizzazione. Purtroppo, le indagini sulle abitudini dei nostri ragazzi ci restituiscono uno scenario molto diverso: moltissimi adolescenti usano le stesse password per più account, un po' per **pigrizia** e un po' per **inconsapevolezza**.

Infatti, i rischi che si corrono sono gli stessi di chi usa, per ipotesi, la stessa chiave per aprire la casa, la macchina e la cassaforte. Cosa succederebbe se perdesse quell'unica chiave?

I ragazzi possono mettere a repentaglio la sicurezza di dati molto sensibili e non solo i loro. Come **aiutarli**? Un tasto su cui far leva può essere la loro creatività.

## Come si può agire

Cominciamo col capire come si crea una password efficace. Sapevi che, nel 2017, le due password più utilizzate dalle persone sono state "123456" e "password"? Una password protegge la nostra sicurezza personale, i dispositivi, le identità, la reputazione e le relazioni; una password debole può quindi rendere più facile ai malintenzionati l'accesso alle nostre informazioni. Una delle cose fondamentali da insegnare ai nostri figli è come si crea una password forte.

Deve essere difficile da indovinare sia per un conoscente sia per un hacker; questo significa che:

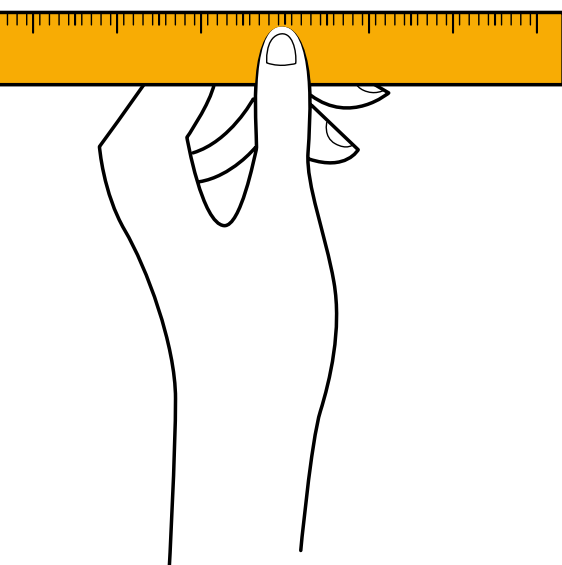
- Deve essere facile da ricordare senza che vengano utilizzate informazioni su di te, come città, anno di nascita, squadra del cuore, soprannomi.
- Più è lunga meglio è: usa quindi almeno otto caratteri. Esiste sicuramente una frase, un'espressione o una citazione che solo tu conosci. Usala.
- Puoi aiutarti con i numeri, ad esempio sostituendo la lettera "e" con il numero "3" e viceversa.
- Deve essere facile da ricordare senza che vengano utilizzate informazioni personali come la data di nascita o il nome dell'animale domestico.
- Puoi so\$t1tu!rE l3 £e++er& c0n s!mB°l1 & n^m3ri ç@me Qu1, con un doppio vantaggio: la password è facile da ricordare, ma è difficile da decifrare per un programma.

FEBBRAIO93

MAMMA

ANDREA91

STELLA101295



- Devi utilizzare una combinazione di lettere maiuscole, minuscole, simboli e numeri. Utilizza sempre il blocco schermo sui tuoi dispositivi.

- Stabilisci un tempo entro il quale aggiornare di nuovo le password: cambiale almeno due volte all'anno.

- Per ogni account crea un'associazione mentale a qualcosa che solo tu conosci e da lì crea una password.

- Potrai prendere in considerazione l'utilizzo di un gestore delle password. Si tratta di un'app o di uno strumento che tiene traccia delle tue password in caso te ne dimentichi alcune: molti browser oggi hanno una funzionalità di sicurezza che può farlo al posto tuo.

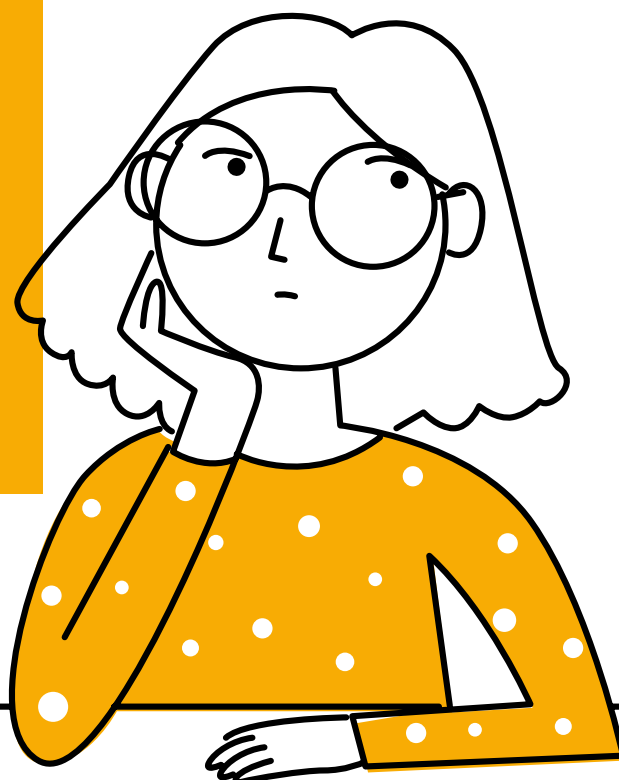
- Dovrai scambiarle: non utilizzare la stessa password su siti e dispositivi diversi. Puoi, però, creare diverse varianti della stessa password per account diversi.



Se ti risulta difficile tenerne a mente molte puoi sempre aiutarti salvandole sul dispositivo che usi nelle aree dedicate e protette. Scriverle su un foglietto da portare con sé non è una buona idea perché può finire nelle mani di chiunque. Il metodo migliore per assicurare una protezione quasi totale è la cosiddetta autenticazione a due fattori: un account che, oltre a chiederti la password di accesso, chiede anche l'inserimento di un codice che viene inviato in tempo reale al tuo telefono.

A meno che tu non abbia perso il telefono (e la memoria), è un metodo molto sicuro.

Le password sono la custodia di ciò a cui tieni. Per proteggere davvero quello che conta si può imparare anche la cura per la custodia stessa.



---

## Attività

**Per i genitori:** sai come aiutare i tuoi figli a vivere Internet, al meglio? Fai [questo test](#) per scoprire se per te il Web non ha segreti o se, invece, potresti imparare cose nuove per aiutare i tuoi figli a navigare le complessità del mondo online.

**Per i ragazzi:** il Web è casa tua. Per imparare ad abitarlo responsabilmente guarda [questo video](#), insieme agli altri inclusi nel programma Vivi Internet, al meglio. Ti sarà più semplice riflettere sulle possibili conseguenze delle tue azioni in rete.

---

---

## Lessico

### Sicurezza

La protezione dei dispositivi delle persone, del software e delle informazioni su di loro.

### Password o passcode

Combinazione segreta di lettere, numeri e simboli utilizzati per accedere a qualcosa. Può assumere forme diverse: ad esempio, puoi avere un codice di soli quattro numeri che utilizzi per bloccare il tuo telefono o tablet e una password più complessa per email, social media o conto bancario. In generale, dovresti rendere le tue password il più complesse possibile ed essere comunque in grado di ricordarle

### Verifica in due passaggi (chiamata anche verifica o autenticazione a due fattori)

Processo di sicurezza che richiede non solo password e nome utente, ma anche qualcosa che tu, e solo tu, fisicamente possiedi in modo da rendere più difficile a potenziali intrusi l'accesso o il furto di dati personali o dell'identità. Un esempio può essere un account che richiede l'inserimento di un codice a tempo inviato sul telefono o all'indirizzo email dopo l'inserimento della password.

### Crittografia

Processo che aiuta la protezione di informazioni come i messaggi che invii online codificando i dati, rendendone quindi difficile la decodifica.

### Complessità

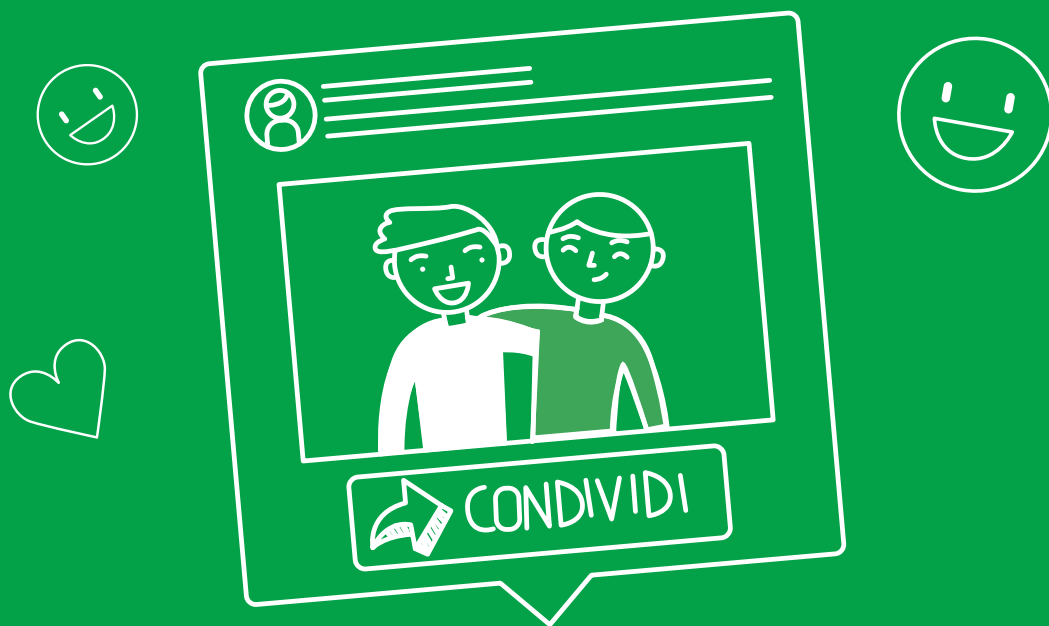
È l'obiettivo della creazione di una password sicura. Una password è considerata complessa quando contiene una combinazione di numeri, caratteri speciali come "\$" o "&" e sia lettere maiuscole che minuscole. La lunghezza, cioè il numero di caratteri, aumenta anch'essa la complessità.

### Hacker

Una persona che utilizza i computer per accedere senza autorizzazione ai dispositivi e ai dati di organizzazioni o persone.

# Diffondi la gentilezza

Il Web è come un altoparlante che amplifica qualunque messaggio venga trasmesso. Quello che i nostri ragazzi possono imparare è come immettere su Internet messaggi positivi, incoraggianti e costruttivi, perché ciascuno di loro sa già, senza bisogno di insegnamenti, che costruire è più bello che distruggere.

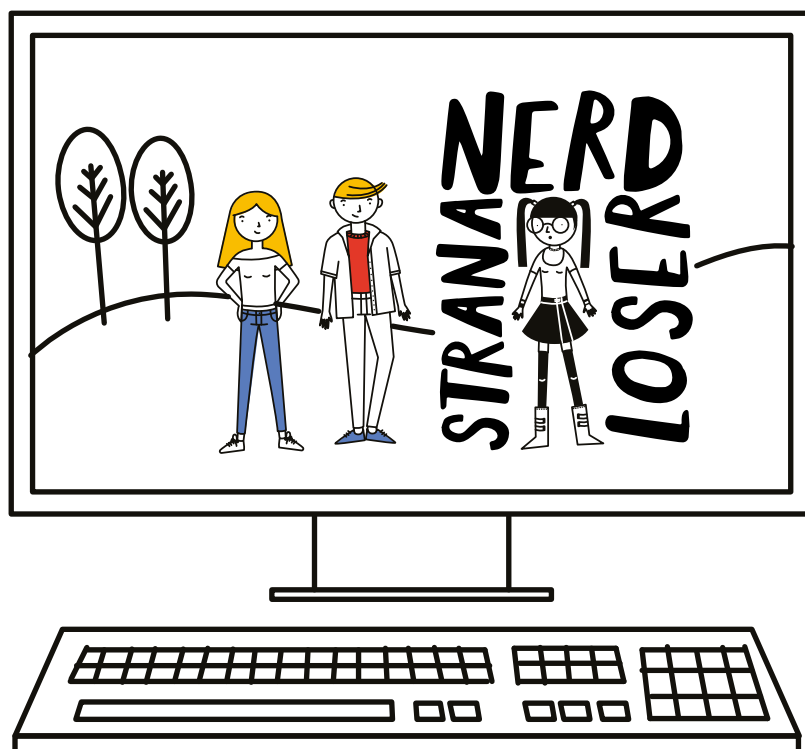




Internet ha dato agli adolescenti una possibilità che in realtà è un desiderio latente in ciascuno di loro, cioè agire senza conseguenze dirette, un po' come se si lanciasse un sasso in strada dalla propria camera senza che nessuno veda.

Questo ha reso possibile la proliferazione di messaggi offensivi, a volte molto lesivi, di ragazzi nei confronti di compagni più deboli, indifesi, emarginati dal gruppo. Tra loro c'è solo lo schermo di un dispositivo e tutto ciò che devono fare è dar sfogo al loro istinto di supremazia. Ecco cos'è il cyberbullismo. Ma dietro quello schermo ci sono persone, ragazzi che per colpa anche solo di un commento negativo vengono isolati, non accettati, derisi dai propri compagni. E spesso chi fa la voce più grossa sembra prevalere, nella vita reale come online.

In generale, online, le parole possono avere forti conseguenze.



Spesso, e purtroppo, vengono utilizzate per emarginare, ferire, etichettare e discriminare. Mentre navigano, agli adolescenti può capitare di trovarsi di fronte a frasi di odio e che incitano alla violenza: queste frasi possono essere devastanti, soprattutto quando si basano su caratteristiche etniche, politiche, religiose e di orientamento sessuale.

Queste frasi sono devastanti per tre motivi principali:

1. **Sono virali:** una volta messe online si propagano immediatamente, innescando una vera e propria "amplificazione dell'odio".
2. **Non se ne vanno:** sono difficili da eliminare, anche se chi le ha create successivamente cambia idea.
3. **Possono essere anonime** e questo viene usato come scudo a discapito degli altri. Inoltre, il filtro di uno schermo ci impedisce di osservare il loro effetto sugli altri e quindi di provare empatia.

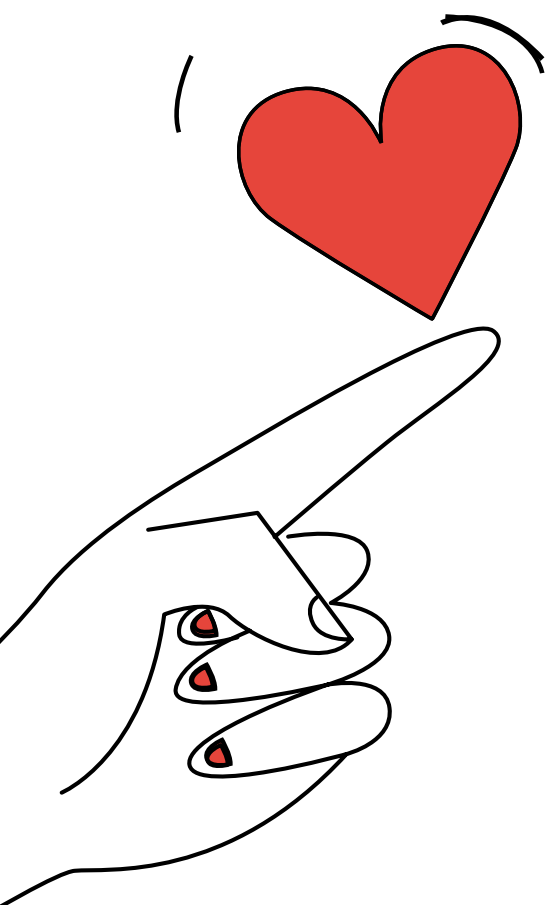
C'è da ricordarsi, quindi, che nonostante queste spiacevoli situazioni, Internet però può essere usato anche per **amplificare la gentilezza**: i ragazzi possono dare il meglio di sé, innescando comportamenti positivi, per contrastare e costruire un'alternativa agli atteggiamenti di prepotenza e di incitamento all'odio.

Insegnare loro a comportarsi con gentilezza ed empatia, e fornire strategie per scoraggiare e depotenziare i comportamenti negativi, è essenziale per aiutarli a costruire relazioni positive.

Il ruolo degli adulti è anche quello di supportarli nel **chiedere aiuto** e ad uscire dal silenzio che spesso circonda gli episodi di bullismo e di violenza.

---

## Come si può agire



---

Cosa fare? Cosa suggerire a tuo figlio? Posto che potrebbe trovarsi a essere tanto un bullo quanto una vittima o un testimone, come nella vita di tutti i giorni, la strada migliore è quella della gentilezza. Quella vera, fatta di prese di posizione nette, messaggi che sappiano rispondere con forza positiva a commenti negativi ed incitamento all'odio.

Quando qualcuno combina un pasticcio, cosa incredibilmente facile da fare online anche senza averne intenzione, i membri della famiglia sono i più inclini a capire, perdonare e aiutarsi a vicenda nell'imparare dai propri errori.

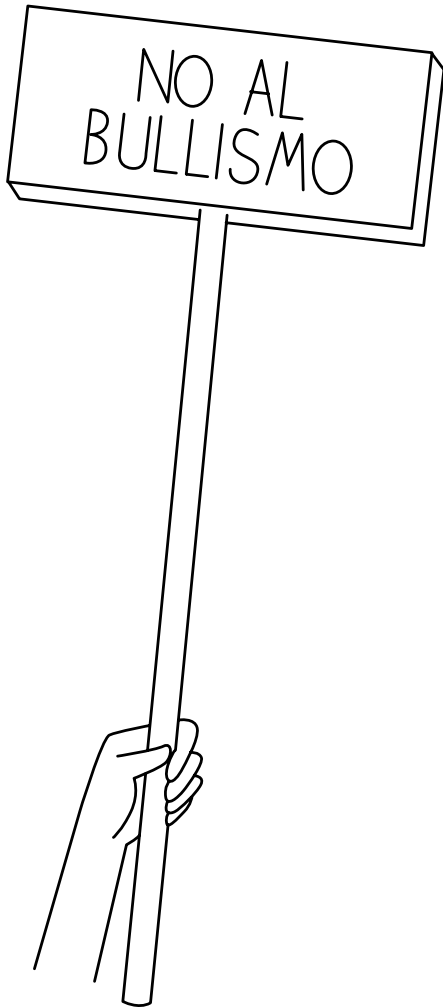
Non c'è quindi luogo migliore della famiglia dove iniziare a mettere in pratica il rispetto, la gentilezza e la positività online.

La famiglia può aiutare quando qualcuno si comporta in modo sgarbato, anche solo ascoltando.

Può anche fornire incoraggiamenti a diventare "upstander", cioè persone che sostengono e difendono le persone che sono l'obiettivo di comportamenti crudeli o dannosi.

Vediamo qualche esempio.

- Distinguiti dalla massa: se il coro è fatto di voci canzonatorie e negative, dai il buon esempio e canta fuori dal coro. Offri alla vittima il tuo sostegno, anche in privato.
- L'atteggiamento: se tu per primo sei amichevole e ben disposto innescherai più facilmente una catena positiva.
- Omertà uguale complicità: il vero problema è chi assiste senza intervenire e senza fare nulla, magari approvando il comportamento denigratorio. Prendi posizione e, se ti criticheranno, non temere di perdere consenso. Meglio non averlo da certe persone.



- Segnala a chi di dovere: se assisti a un comportamento spiacevole puoi sempre usare gli strumenti di segnalazione online per bloccare o inibire il bullo.
- Può capitare a chiunque: se anche tu diventi vittima di bullismo, non pensare che capiti solo a te. Chi non trova altro modo di esprimersi se non attraverso l'aggressività non può giudicarti.
- Sii il primo a dare il buon esempio: valuta se possiedi tutte le informazioni, prima di esprimere un giudizio negativo rispetto a fatti, persone o gruppi di persone.
- Se sei vittima di commenti negativi su Internet, rispondi all'odio in rete con una prospettiva costruttiva e con un atteggiamento positivo e aperto all'ascolto.

Alla fine, quello che più conta è trattare gli altri come vorresti che trattassero te. Un atto di gentilezza che hai ricevuto sicuramente ti ha fatto sentire bene, quindi replicarlo a tua volta è il modo migliore per contribuire a rendere Internet un posto più vivibile, più sano e più bello.

## Attività

**Per i genitori:** sai come aiutare i tuoi figli a vivere Internet, al meglio? Fai [questo test](#) per scoprire se per te il Web non ha segreti o se, invece, potresti imparare cose nuove per aiutare i tuoi figli a navigare le complessità del mondo online.

**Per i ragazzi:** il Web è casa tua. Per imparare ad abitarlo responsabilmente guarda [questo video](#), insieme agli altri inclusi nel programma Vivi Internet, al meglio. Ti sarà più semplice riflettere sulle possibili conseguenze delle tue azioni in rete.

## Lessico

### Bullismo

Comportamento deliberatamente cattivo, di solito protratto nel tempo. La persona che ne è bersaglio ha spesso grande difficoltà a difendere sé stessa.

### Cyberbullismo

Bullismo che si verifica online o tramite dispositivi digitali.

Il cyberbullismo comprende l'invio, la pubblicazione o la condivisione di contenuti negativi, dannosi, falsi o cattivi e la condivisione di informazioni personali e private su qualcuno che creano imbarazzo o umiliazione.

### Molestia

Rispetto al bullismo è un termine più generico. Le molestie possono avvenire sia online che nella vita reale e possono prendere diverse forme. Una molestia può essere l'atto di importunare, infastidire, intimidire, tormentare ecc. qualcuno.

### Conflitto

Discussione o disaccordo che non necessariamente si protrae nel tempo.

### Aggressore

La persona che mette in atto le molestie o il bullismo, viene chiamata anche "bullo".

### Bersaglio

La persona che viene bullizzata, molestata o tormentata.

### Spettatore

Testimone della molestia o del bullismo che riconosce la situazione ma non interviene, sia per scelta che per paura di ritorsioni.

### Upstander

Testimone di molestia o bullismo che sostiene la persona fatta bersaglio in privato o pubblicamente, talvolta cercando di fermare e/o denunciare l'episodio a cui ha assistito.

### Bloccare

Porre fine a ogni interazione online con un'altra persona, impedendole di accedere al proprio profilo, di inviare messaggi, di vedere i propri post ecc., senza informarla. È un modo efficace di fermare il contatto online con un bullo tramite un canale specifico, ma può non essere sufficiente a porre fine alla molestia stessa; i bulli possono pubblicare contenuti sui bambini anche se il loro bersaglio li sta ignorando.

### Disattivare delle notifiche

Meno definitivo dell'atto di bloccare qualcuno, disattivare le notifiche è un modo per smettere di vedere i post, i commenti ecc. di un'altra persona sul proprio feed social media quando la comunicazione diventa fastidiosa. La persona non viene informata della disattivazione delle notifiche mentre le proprie notifiche continueranno a essere visualizzate. Se qualcuno continua comunque a bullizzarti, è meglio bloccarlo del tutto.



**Trollare**

Publicare o commentare online in modo deliberatamente crudele, offensivo o provocatorio.

**Segnalare un abuso**

Utilizzare gli strumenti o i sistemi online di un servizio di social media per segnalare molestie, bullismo, minacce o altri contenuti dannosi che in genere ne violano i termini di servizio o le norme della community.

# Nel dubbio, parlane

Nonostante tutta la prudenza possibile, su Internet può accadere sempre che i ragazzi si trovino di fronte a contenuti inappropriati e discutibili. Chi può aiutarli?



È importante che gli adolescenti capiscano di **non** essere da **soli** quando vedono online contenuti o comportamenti che li mettono a disagio, soprattutto se sono dannosi per loro o per qualcuno a cui tengono.

Non dovrebbero mai esitare a chiedere aiuto a te o a un altro membro della famiglia di cui si fidano. Per loro è anche utile sapere che esistono diversi modi per **essere coraggiosi e agire**, come discutere di qualcosa offline e utilizzare gli strumenti di segnalazione online.

I genitori hanno un ruolo fondamentale e difficile allo stesso tempo. I figli hanno bisogno di contare su una figura presente, ma non invasiva. Gli incontri che possono fare online sono molti e possono essere al punto tale da necessitare un confronto serio con qualcuno di più grande.

Se dovesse accadere, è bene che il genitore sia pronto ad ascoltare senza giudicare (almeno in una prima fase) e magari avendo qualche conoscenza del problema e delle sue **soluzioni**. A volte il panico può portare i ragazzi a cercare di rimediare con soluzioni ben peggiori del problema che vogliono risolvere: serve una **mente fredda e preparata** per evitare che commettano leggerezze.

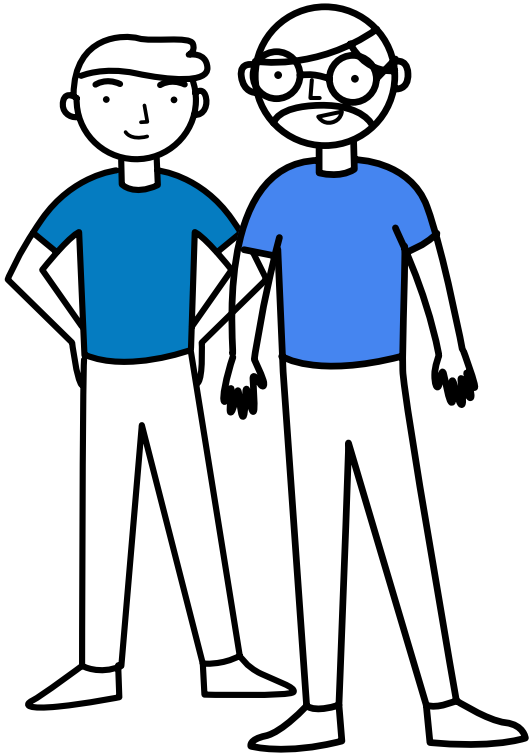
## È successo...



Vediamo alcune delle **situazioni più frequenti** che accadono online e che mettono in difficoltà i nostri ragazzi.

- Qualcuno minaccia i loro dati, con un virus o con una mail sospetta.
- Non sanno distinguere tra una truffa online ben camuffata e un'occasione da cogliere.
- Vengono interpellati da un altro utente su argomenti scomodi, riservati o imbarazzanti.
- Si rendono conto di aver condiviso contenuti che non avrebbero dovuto condividere.
- Temono di essere stati ricattati o che il loro account sia stato violato.

## Come si può agire



Come nella vita reale, il dialogo con i figli si **costruisce** a poco a poco, serve fiducia reciproca e soprattutto serve essere credibili ai loro occhi.

Se queste condizioni già esistono, allora sarà più facile innescare quell'**empatia necessaria** per affrontare il problema. Innanzi tutto, non drammatizzare la situazione. Per quanto grande sia il problema, **si può affrontare**. Un virus che blocca un account o un tentativo di truffa si possono risolvere facilmente cambiando le password e contattando la polizia postale.

Se invece tuo figlio è rimasto vittima di un comportamento lesivo, fagli subito sentire il tuo appoggio: deve capire che quello che ha visto o letto non è la verità, ma solo l'opinione di qualcuno disinteressato a lui. Se si rende conto di aver condiviso contenuti inappropriati, privilegia prima la **ricerca di una soluzione**: su Internet nulla è reversibile, ma si può sempre rimediare. Errare è umano, **ammettere di aver fatto un errore** è cosa buona.

## Attività

**Per i genitori:** sai come aiutare i tuoi figli a vivere Internet, al meglio?

Fai [questo test](#) per scoprire se per te il Web non ha segreti o se, invece, potresti imparare cose nuove per aiutare i tuoi figli a navigare le complessità del mondo online.

**Per i ragazzi:** il Web è casa tua.

Per imparare ad abitarlo responsabilmente guarda [questo video](#), insieme agli altri inclusi nel programma Vivi Internet, al meglio. Ti sarà più semplice riflettere sulle possibili conseguenze delle tue azioni in rete.

## Lessico

### Fiducia

Forte convinzione che qualcosa o qualcuno sia affidabile o sincero.

### Segnalazione di un abuso

In questa guida utilizziamo questo termine per riferirci alla segnalazione di problemi su app e servizi social media, molti dei quali hanno strumenti o sistemi appositi a questo scopo.