

QUELLO CHE DEVI SAPERE

sullo

SMARTPHONE



Stai al sicuro e sfrutta al meglio il potenziale digitale.

Benvenuti nella Guida all'uso consapevole dello smartphone o, come mi piace chiamarla, la patente digitale per ragazzi (e genitori) del ventunesimo secolo.

Prendete questo manuale per ciò che è davvero: un piccolo esperimento nato in casa, da una semplice domanda di una dodicenne piena di entusiasmo: "Papà, posso avere Internet sul telefono?". Il telefono lo aveva già, ma senza connessione: un po' come avere un'auto senza benzina. E io, da genitore (un po' ansioso e un po' nerd), non me la sentivo di "consegnare le chiavi" di un motore così potente senza essere sicuro che sapesse dove e come guidarlo.

Da qui è nata l'idea di questa guida: mettere nero su bianco tutto ciò che un adolescente dovrebbe sapere prima di usare uno smartphone in piena autonomia. Le regole, le attenzioni, le opportunità. Le ho proposto un patto: "Studia la guida, affronta il test finale e, se fai meno di tre errori, avrai tutto quello che ti serve davvero sul tuo telefono."

Il test (30 domande) serve a capire cosa c'è dietro ogni tocco, foto, messaggio o app che scarichiamo. E se si sbaglia? Nessun dramma: si ripassa e si riprova. Fa parte del percorso.

Ho scritto questa guida perché mi sono reso conto di una verità semplice: nessuno prepara davvero gli adolescenti (né tantomeno i genitori) a usare il telefono con consapevolezza. Gli viene dato in mano e basta. La scuola ne parla spesso in modo estemporaneo e sporadico, spesso lamentandosi, e i genitori si ritrovano divisi tra paura e permissività, senza strumenti pratici per accompagnare i figli.

Eppure lo smartphone è il principale strumento di comunicazione, informazione e identità delle nuove generazioni. Non possiamo lasciarli imparare solo "per tentativi ed errori".

L'ho scritta in pieno boom dell'intelligenza artificiale e, sì, è inevitabilmente imperfetta: qualche refuso, qualche paragrafo che un giorno riscriverò. Ma senza l'aiuto dell'AI ci avrei messo mesi, e mia figlia non avrebbe certo aspettato così a lungo per installare WhatsApp.

Questa guida non è perfetta, ma è sincera: nasce dalla mia esperienza personale, da oltre trent'anni immerso nella tecnologia, conoscendone rischi e opportunità, e cercando ogni giorno di viverci in equilibrio.

Per fare i quiz collegati a
www.quiz-patente-smartphone.it
o inquadra il codice QR.



Hardware: il corpo dello smartphone



Lo smartphone non è nato dal nulla: è il risultato di oltre un secolo di invenzioni e miglioramenti. Da primi esperimenti dell'italiano Antonio Meucci (1854) al primo telefono brevettato da Alexander Graham Bell (1876), al Motorola DynaTAC (1973) che trasmetteva solo la voce, grande come un mattone e pesante 2 kg, fino all'iPhone di Steve Jobs (2007), che ha reso il touch screen naturale e alla portata di tutti.

Oggi lo smartphone è diventato un vero coltellino svizzero digitale: telefono, fotocamera, orologio, torcia, agenda, lettore musicale, console per videogiochi e molto altro, tutto in un unico oggetto che porti in tasca.

Le parti del corpo dello smartphone

Schermo

Gli schermi di oggi sono touchscreen multi-touch, capaci di riconoscere più dita contemporaneamente. Ad esempio pizzicare lo schermo con due dita permette di ingrandire una foto (funzione introdotta per la prima volta con l'iPhone nel 2007)

Un tempo, invece, i cellulari non erano touch, avevano minuscoli display monocromatici, grandi quanto quelli di una calcolatrice.

Processore (CPU e GPU)

Il processore è il cervello dello smartphone: prende decisioni, calcola, gestisce i programmi.

Negli anni '90 serviva un computer da tavolo grande e rumoroso per fare quello che oggi fa un minuscolo chip nel tuo telefono.

Uno smartphone moderno contiene oltre 19 miliardi di transistor, immagina 19 miliardi di minuscoli interruttori che si accendono e spengono miliardi di volte al secondo!

Questi ad esempio, in un videogioco 3D, permettono di far muovere i personaggi in modo fluido: quelli sono i chip del GPU (scheda grafica) che lavora insieme a quelli del CPU.

Batteria

Le prime batterie erano enormi, si scaricavano in fretta e impiegavano ore a ricaricarsi. Oggi usiamo batterie agli ioni di litio, leggere e potenti e molto più veloci.

Esempio pratico: vai su Impostazioni > Batteria e guarda la lista delle app che consumano più energia. Scoprirai che i social e i giochi sono spesso i più “affamati” di energia!

Memoria

Negli anni '90 un cellulare poteva salvare solo 20 SMS. Ora puoi conservare centinaia di migliaia di documenti, foto, video e canzoni in un telefono che sta in tasca.

Negli anni 20 la media dei dispositivi aveva 5 GB, sufficienti per 1.000 canzoni. Oggi uno smartphone può arrivare a 1 TB circa 200.000 brani o centinaia di film.

Apri la Memoria del tuo telefono (Impostazioni > Memoria) e controlla quanta memoria è stata utilizzata e quanta ne rimane libera. L'ideale è avere sempre libera almeno 2 GB di memoria per non rallentare in telefono.

Fotocamere

Quando si parla di fotocamere, spesso senti la parola megapixel (MP). Un pixel è il puntino più piccolo che compone una foto sullo schermo. Un megapixel significa un milione di pixel.

Più megapixel ha una fotocamera, più dettagli può catturare. Ma attenzione: non conta solo il numero, anche il software, la grandezza e qualità del sensore fanno la differenza.

Esempio pratico: se fai una foto con una fotocamera da 2 MP e la ingrandisci, l'immagine diventa sgranata. Con una da 12 MP puoi ingrandire molto di più senza perdere qualità.

Sensori

Lo smartphone ha sensori invisibili ma potentissimi:

- **Microfono** > è il sensore che cattura i suoni: la tua voce quando telefoni, ma anche la musica e i rumori intorno a te.
- **Giroscopio e accelerometro** > capiscono se tieni il telefono in verticale o orizzontale.
- **GPS** > indica dove ti trovi sulla mappa grazie ai satelliti.
- **Sensore di prossimità** > spegne lo schermo quando avvicini il telefono all'orecchio.
- **Sensore di impronte digitali** > Permette di sbloccare il telefono con il tuo dito.

Ad esempio quando attivi il GPS e apri Google Maps e guardi la freccia blu che ti indica la direzione e che si muove girandoti, sta lavorando il giroscopio.

Da ricordare: alcune app possono chiedere l'accesso ai sensori anche quando non serve (es. giochi o torce).

Ad esempio il Microfono: se non controlli i permessi, rischi che il telefono ascolti più del dovuto.

Anche assistenti vocali come Siri, Google Assistant, Alexa si attivano con la voce: comodo, ma bisogna sapere che, anche se non registra le conversazioni, il microfono è sempre in ascolto per la parola di attivazione.

Consiglio pratico: vai su > Impostazioni > Privacy > Microfono e controlla quali app hanno accesso: togli il permesso a quelle che non usi.

Il microfono ti dà voce, ma ricorda: la tua voce è un dato personale, usalo con attenzione.

Tabella riassuntiva – L'hardware dello smartphone

Componente	Funzione	Unità di misura
Schermo	Mostra immagini, video e comandi	Pollici (") per la diagonale, pixel per risoluzione (es. Full HD 1920×1080)
Processore (CPU)	"Cervello" del telefono, esegue i calcoli	GHz (gigahertz) + numero di core
Scheda grafica (GPU)	Gestisce grafica e giochi 3D	Frequenza in MHz/GHz, unità di calcolo
Batteria	Fornisce energia al telefono	mAh (milliampere-ora)
Memoria RAM	Memoria veloce per le app in uso	GB (gigabyte)
Memoria interna (storage)	Conserva dati, foto, video e app	GB o TB
Fotocamera	Scatta foto e registra video	Megapixel (MP), apertura focale (f/)
Sensori (accelerometro, giroscopio, GPS, ecc.)	Rilevano movimento, posizione, luce, suoni	Dipende dal sensore (es. ° per giroscopio, metri per GPS, Hz per microfono)
Microfono	Cattura i suoni e la voce	Hz (frequenze sonore) e kHz (qualità registrazione)
Altoparlante	Riproduce suoni e musica	Hz (gamma di frequenze) e dB (volume)

Manutenzione – Come prendersi cura del telefono

Uno smartphone ben curato può durare anche **4-5 anni**, mentre trascurato rischia di rompersi in 2.

Schermo

Metti una pellicola protettiva

Pulisci con un panno in microfibra

Batteria

Non scendere sempre a 0%

Meglio ricariche brevi e frequenti (20–80%)

Attiva la modalità Risparmio energetico quando sei sotto il 20%.

Memoria e dati

Cancella foto doppie o inutili

Disinstalla app che non usi (di solito ne usi meno della metà!)

Fai il backup su cloud o PC

Custodia e cadute

Usa una cover protettiva

Evita di lasciarlo in tasca posteriore

Proteggilo da acqua e sabbia

Aggiornamenti sistema operativo e software

Servono per sicurezza e prestazioni del dispositivo

Esempio pratico: vai su Impostazioni → Aggiornamento software e verifica se hai l'ultima versione.

Consiglio finale:

Curare il tuo smartphone significa anche inquinare meno: meno rifiuti elettronici, più pianeta pulito

Tabella pratica – Cosa fare / Cosa evitare

Parte	✔ Cosa fare	✗ Cosa evitare
Schermo	Mettere una pellicola protettiva e pulirlo con panno in microfibra	Pulirlo con prodotti aggressivi o carta (graffiano)
Batteria	Fare ricariche tra il 20% e l'80%	Lasciare che scenda sempre a 0% o ricaricarla tutta la notte
Memoria	Eliminare foto doppie, app inutili e fare backup	Tenere tutto accumulato fino a riempire lo spazio
Custodia	Usare una cover e non lasciarlo in tasca dietro	Portarlo senza protezione o appoggiarlo in bilico
Aggiornamenti	Installare gli update di sistema e delle app	Ignorare gli aggiornamenti per mesi
Uso quotidiano	Tenerlo lontano da acqua, sabbia e sole diretto	Lasciarlo in auto al caldo o usarlo sotto la pioggia senza protezione

Software: l'anima del telefono



Usare app e programmi a 10 o 12 anni sembra essere diventato normale: lo smartphone è come una macchina digitale sempre pronta a partire, e ogni applicazione è una strada diversa da esplorare, una per giocare, una per chattare, un'altra per imparare o creare e così via. Ma, proprio come sulla strada vera, non tutte i tipi di strade sono adatte a chi ha appena iniziato a guidare. Alcune richiedono più esperienza, più attenzione, e il rispetto di regole precise. App come TikTok, Instagram, WhatsApp, Telegram o Discord funzionano un po' così: nei loro "codici della strada", chiamati Termini di servizio, è scritto che bisogna avere almeno 13 anni (e in Europa spesso 16) per poterle usare da soli. Non è una regola messa lì per bloccare o punire, ma per proteggere: prima di entrare in certi spazi digitali, serve imparare a riconoscere i cartelli, i limiti di velocità e le situazioni di pericolo.

Il mondo digitale è una rete di strade infinita e affascinante, ma per guidarci serve conoscenza, prudenza e un po' di esperienza. Non è un limite per rovinare il divertimento, ma una regola di sicurezza, come il casco in bici o la cintura in auto. Inoltre queste piattaforme raccolgono informazioni personali, mostrano pubblicità mirate e permettono contatti con persone sconosciute: per gestirle bene serve consapevolezza e maturità. Molti ragazzi, però, creano profili anche se troppo giovani, magari cambiando la data di nascita o con l'aiuto dei genitori distratti. Ma prima di scaricare o registrarsi, è importante informarsi:

- Qual è l'età minima per usarla?
- Posso controllare chi vede le mie foto o i miei messaggi?
- Esiste una versione "kids" o una modalità "famiglia"?

In questo modo avrai una cintura di sicurezza digitale: puoi esplorare il mondo online, ma con le protezioni giuste.

La tecnologia non è un pericolo, ma uno strumento. L'importante è conoscerla, rispettarne le regole e usarla con curiosità e buon senso.

Così ogni software diventa davvero un alleato, non un rischio.

Se l'hardware è il corpo, **il software è l'anima dello smartphone**. È ciò che trasforma pezzi di metallo, plastica e circuiti in un oggetto vivo, capace di comunicare, calcolare, ricordare e persino divertirci. Senza software, il telefono sarebbe un guscio vuoto: non potresti neppure accenderlo.

Immagina un robot aspirapolvere: il corpo di metallo e le ruote sono l'hardware, ma è il software che gli dice come muoversi, o riconoscere un ostacolo. Senza istruzioni, il robot resterebbe fermo e muto.

Che cos'è il software

Il software è l'insieme delle istruzioni che dicono al telefono cosa fare. Ad esempio:

Quando tocchi lo schermo, è il software che interpreta il gesto.

Quando scatti una foto, il software elabora luce e colore.

Quando apri un'app, è il software che la “traduce” in azioni.

Il sistema operativo: il direttore d'orchestra

Ogni smartphone ha un sistema operativo (OS), il direttore che coordina tutti i software e molto altro. I sistemi operativi più diffusi sono:

- **iOS (Apple):** fluido, sicuro, aggiornato regolarmente, ma disponibile solo su iPhone.
- **Android (Google):** aperto, personalizzabile, usato da marchi come Samsung, Xiaomi, Oppo e tanti altri.
- **Linux:** Android si basa su un “cuore” (kernel) derivato da Linux, un sistema operativo libero nato negli anni '90. Senza Linux, probabilmente Android non esisterebbe così come lo conosciamo.
- **Storici:** Symbian (Nokia), BlackBerry OS, Windows Phone: protagonisti di un'epoca passata.

Le app: organisimi digitali

Le applicazioni o app sono i veri software che usiamo ogni giorno. Senza app, lo smartphone sarebbe come una casa senza mobili: abitabile, ma vuota. Nel 2025 si contano oltre 8 milioni di app disponibili nei vari store per scaricarle (Google Play, App Store...). Alcune categorie di app includono:

- **Utilità:** per la vita pratica (calcolatrice, meteo, mappe).
- **Studio e lavoro:** per imparare e collaborare a distanza.
- **Social:** per condividere foto, video, storie.
- **Giochi:** per divertirsi e sfidare amici.
- **Salute e benessere:** per allenarsi, rilassarsi.

Ogni volta che usiamo un'app o un social, **lasciamo una traccia digitale**. Il software non solo ci aiuta, ma raccoglie anche dati personali: **posizione, gusti, abitudini, perfino le foto che scattiamo**.

- **Condivisione** consapevole: pubblicare un contenuto significa renderlo potenzialmente visibile a migliaia di persone. Una foto su Instagram o un video su TikTok può fare il giro del mondo in pochi minuti.
- **Privacy:** molte app chiedono accesso a microfono, fotocamera, contatti. Alcune lo fanno per necessità, altre per raccogliere dati da usare a fini commerciali. (Vai su Privacy > Gestione autorizzazioni per controllare i permessi delle app)
- **Protezione:** scegliere bene cosa condividere, usare impostazioni di privacy (Impostazioni > Privacy) aiuta a difendere la propria identità digitale.

Il software è un mondo invisibile che plasma la nostra quotidianità. Senza rendercene conto, affidiamo al telefono non solo messaggi e foto, ma anche la nostra identità digitale. **Usare lo smartphone significa non solo sfruttare la sua potenza, ma anche imparare a proteggere la propria privacy.**

Tabella – Categorie di software e app

Categoria	Esempi	Funzione	Pro	Contro	
Sistema operativo	iOS, Android, Linux	Gestisce l'intero telefono	Stabilità, sicurezza	Limitazioni (es. poca personalizzazione su iOS)	
Social	Instagram, TikTok, Facebook	Condivisione e connessione	Creatività, amicizie	Dipendenza, rischio privacy	
Messaggistica	WhatsApp, Telegram, Signal	Comunicazioni rapide	Gratuiti, immediati	Spam, cyberbullismo	
Giochi	Roblox, Fortnite, Candy Crush	Intrattenimento	Divertimento, abilità	Dipendenza, acquisti in-app	
Utilità	Google Maps, Torcia, Meteo	Vita quotidiana	Utili e pratiche	Possono raccogliere dati di posizione	
Studio/Lavoro	Zoom, Google Classroom, Notion	Apprendimento e collaborazione	Accessibili ovunque	Sovraccarico notifiche	
Salute/Fitness	Strava, Fitbit, Calm	Benessere e attività fisica	Motivazione e monitoraggio	Ansia da performance	
Shopping	Amazon, eBay, Shein	Acquisti digitali	Comodità, scelta infinita	Sovraconsumo	

Reti e connessioni: come lo smartphone parla col mondo



Immagina di avere un telefono superpotente... ma che non può chiamare, mandare messaggi né collegarsi a internet. Sarebbe come avere un'auto velocissima senza strade!

Le reti e connessioni sono le strade invisibili che permettono agli smartphone di parlare tra loro e con il mondo. Senza di esse, il telefono resterebbe un oggetto isolato.

Le connessioni principali:

Rete cellulare (Telefonia e dati per Internet)

È la rete che permette di fare telefonate, inviare SMS e collegarti a internet.

Funziona grazie a migliaia di antenne sparse sul territorio (le famose “celle”).

Generazioni di rete:

2G: solo chiamate ed SMS.

3G: + dati internet, ma molto lenti.

4G: + navigazione veloce, streaming, giochi online.

5G: + velocità fino a 100 volte maggiore del 4G, pensato anche per auto autonome e realtà aumentata.

Wi-Fi

È la rete che trovi a casa, a scuola o in biblioteca. Può essere protetta da una password.

Non usa le antenne telefoniche, ma **un router** collegato a internet tramite cavo o fibra ottica.

Permette di navigare gratis (dopo aver pagato l'abbonamento) senza consumare i “giga” della SIM dati mobili.

Bluetooth

Serve a collegare dispositivi vicini (fino a circa 10 metri) come ad esempio: cuffie wireless, stampanti, smartwatch, casse musicali o per scambiarsi dei file con altri dispositivi. Consuma poca batteria ma meglio disattivarlo se non necessario.

GPS

Non serve per comunicare, ma per localizzarti.

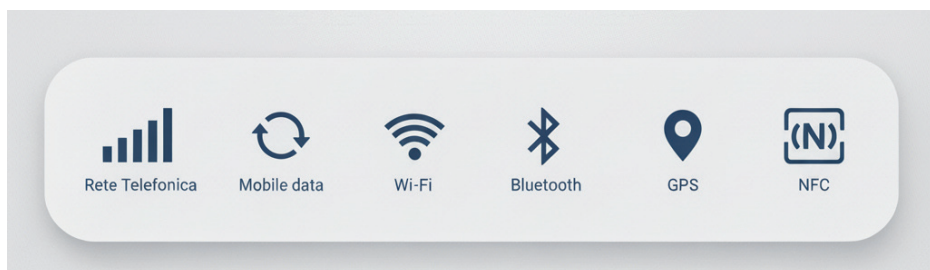
Funziona grazie a una rete di satelliti che orbitano intorno alla Terra.

È ciò che rende possibili le mappe e le app di navigazione.

NFC

Sta per Near Field Communication (comunicazione a corto raggio). Permette di pagare avvicinando lo smartphone a un lettore contactless. Utile anche per scambiare dati rapidamente.

Le icone (generiche) per identificare le diverse connessioni:



Sicurezza e rischi delle connessioni

- **Wi-Fi pubblici** (es. in bar o stazioni) possono essere pericolosi: un hacker potrebbe spiare i tuoi dati. Fai attenzione a cosa cerchi e condivi quando sei connesso a queste reti spesso non protette da nessuna password.
- **Bluetooth** acceso inutilmente consuma batteria e può esporre a intrusioni.
- **GPS**: le app possono tracciare i tuoi spostamenti e consumano molta batteria → meglio attivarlo solo quando serve.

Le connessioni sono una grande conquista: ci permettono di parlare con amici lontani, imparare cose nuove e persino salvarci in situazioni di emergenza. Ma come tutte le strade, vanno usate con prudenza: senza regole, indicazioni e attenzione alla guida, rischiano di portarci in luoghi sconosciuti e non sempre sicuri.

CONNESSIONI SMARTPHONE

Icona	Connessione	Pro	Contro
	Rete cellulare (2G-5G)	Copertura quasi ovunque Chiamate e internet anche fuori casa	Costo dei giga Segnale debole in zone isolate
	Wi-Fi	Navigazione veloce Perfetto per streaming e giochi	Pubblici poco sicuri Limitato alla zona del router
	Bluetooth	Consuma poca batteria Connette cuffie, casse, smartwatch	Funziona solo a breve distanza Rischio intrusioni se sempre acceso
	GPS	Navigatore e mappe Utile per sport e viaggi	Consuma energia Può tracciare i movimenti

Restare connessi è utile, ma può anche diventare stancante. Ogni notifica interrompe la concentrazione, e saltare da una chat a un video rende difficile “staccare la spina”. Alcuni suggerimenti:

- Se hai meno di 14 anni chiedi ai tuoi genitori di attivare “Controllo genitori” o Family Link.
- Usa la modalità aereo o non disturbare per dormire meglio.
- Verificare sempre il lucchetto HTTPS nei siti.
- Disattivare il GPS quando non serve.
- Non condividere mai password o fallo solo di chi ti fidi.
- Non connetterti a reti Wi-Fi sconosciute.

Scollegati ogni tanto

Proprio come il telefono ha bisogno di ricaricarsi, anche tu hai bisogno di disconnetterti. Stabilisci dei momenti “offline” (prima di dormire, durante i pasti, mentre studi). Tieni il telefono in un'altra stanza mentre fai i compiti. Scopri quanto è bello annoiarsi: spesso nascono le idee migliori.

Imposta dei limiti automatici e spegni le connessioni inutili

- Attiva la funzione “Tempo di utilizzo” (iPhone) o “Benessere digitale” (Android).
- Imposta timer per le app più “infinite” (es. YouTube, TikTok).
- Dopo un'ora, fai una pausa vera: guarda fuori dalla finestra, parla con qualcuno, cammina.
- Spegni Bluetooth, GPS e Wi-Fi quando non servono: risparmi batteria e ti proteggi.
- Elimina periodicamente le app che non usi.

Crea connessioni reali

La rete è utile, ma non sostituisce i legami veri.

Usa la tecnologia per organizzare cose dal vivo (sport, giochi, gite). Invia messaggi positivi: anche le parole digitali lasciano tracce. Ricorda: la connessione più potente resta quella tra persone.

Fotocamera: gli occhi digitali del telefono



Un tempo, per immortalare un momento speciale, serviva una macchina fotografica dedicata, un rullino da sviluppare e giorni di attesa per vedere le immagini stampate. Oggi basta un semplice tocco sullo schermo.

La fotocamera dello smartphone è diventata il nostro diario visivo quotidiano: raccoglie sorrisi, viaggi, feste di compleanno, panorami mozzafiato, ma anche dettagli pratici come documenti scolastici o la lista della spesa fotografata al volo. Inoltre la fotografia mobile ha democratizzato l'arte dello scatto: chiunque, in qualsiasi momento, può diventare fotografo.

Cosa c'è dietro dietro ogni "scatto" fotografico

- **Sensore CMOS o CCD:** cattura la luce come la retina dell'occhio umano.
- **Ottiche miniaturizzate:** lenti in vetro e plastica che concentrano i raggi luminosi sul sensore.
- **ISP (Image Signal Processor):** chip che ottimizza colori e riduce il "rumore digitale".
- **Software e AI:** riconoscono scene, volti e sorrisi, scegliendo automaticamente le impostazioni migliori.

Filtri, editing e intelligenza artificiale

Scattare per molti non è più sufficiente: la maggior parte delle immagini passa per un filtro o un ritocco.

Filtri social: migliorano i colori o trasformano il viso.

Software e app di editing (Photoshop, Snapseed, Lightroom): correggono imperfezioni, aggiungono testi, fondono più immagini.

AI generativa: elimina oggetti, crea immagini da un semplice testo, trasforma foto in illustrazioni o crea scenari mai esistiti.

Buone pratiche per foto e video consapevoli

La tecnologia ci permette di catturare tutto. Ma la vera sfida è decidere cosa tenere, cosa condividere e cosa vivere senza schermo.

Ecco alcune buone abitudini per fotografare e filmare meglio:

1. Stampa ogni tanto le tue foto.

Le immagini digitali rischiano di perdersi tra migliaia di file. Stampare una foto la rende reale, da toccare e ricordare.

2. Crea album o cartelle tematiche.

Dividi per viaggi, persone, eventi. Ti aiuterà a non perdere i ricordi e a riviverli con ordine.

3. Riguarda le tue foto senza fretta.

Non serve pubblicare tutto subito: scegliere cosa tenere è già un modo di dare valore.

4. Fai video brevi ma significativi.

Racconta una storia con inizio, centro e fine. Non serve la perfezione: serve emozione.

5. Rispetta la privacy altrui.

Non filmare o condividere volti di amici o sconosciuti senza permesso.

6. Pulisci la galleria.

Cancella foto doppie o inutili: lo spazio libero aiuta anche la mente a essere più leggera.

7. Vivi anche senza la fotocamera accesa.

Alcuni momenti vanno solo vissuti. A volte, la memoria del cuore è più duratura di quella del telefono.

Rischi e responsabilità legali

Se nei video compaiono persone, luoghi e voci: bisogna riflettere prima di pubblicare o condividere qualcosa. Pubblicare video con persone o luoghi riconoscibili senza consenso può violare la loro privacy. Chiedere l'autorizzazione è sempre la scelta più sicura e spesso necessaria per legge.

Privacy, sicurezza e condivisione delle foto e dei video

Se prima il problema era non perdere il rullino, oggi la vera sfida è proteggere le immagini digitali.

- **Condivisione consapevole:** pubblicare una foto o un video non significa solo mostrarla agli amici, ma anche consegnarla a piattaforme che possono conservarla e analizzarla.
- **Dati nascosti (metadati EXIF):** ogni foto contiene informazioni invisibili, come data, ora e posizione GPS. Un semplice scatto davanti a scuola può rivelare dove vivi o studi.
- **Cloud e backup:** salvare foto online è comodo, ma bisogna verificare la sicurezza del servizio e impostare una buona password.
- **Rischio di abuso:** immagini e video personali possono essere copiate, manipolate o usate senza permesso (ad esempio nei cosiddetti deepfake).

Consigli pratici:

- **Disattiva la geolocalizzazione** quando non serve.
- Condividi foto private **solo con persone fidate**.
- Usa cartelle protette o **app con riconoscimento biometrico**.
- Ricorda che “cancellare” da uno smartphone non significa sempre eliminare dal web. Se ad esempio eliminiamo un video dal telefono ma il telefono viene sincronizzato in Cloud, il video andrà eliminato anche da lì.

In definitiva, la fotocamera dello smartphone è molto più che un sensore: è occhio, penna e voce insieme.

Ma il potere di catturare immagini, suoni e parole porta anche una grande responsabilità: saper distinguere l'autenticità dall'illusione, la memoria dal falso, la creatività dal rischio

Password e sicurezza: le chiavi del castello



Immagina che ogni password sia la chiave del tuo castello digitale. Dentro ci sono: le chat con gli amici, i giochi, i voti di scuola, magari anche la carta dei genitori collegata. Se qualcuno ruba una chiave, può travestirsi da te e fare pasticci al posto tuo. La buona notizia? Con poche regole facili puoi trasformare il tuo castello in una fortezza difficile da assaltare.

Cosa proteggono le password

Le password non servono solo a bloccare lo schermo ma proteggono tante cose importanti come:

- **Identità:** nome, foto profilo, contatti.
- **Messaggi:** nessuno deve scrivere fingendo di essere te.
- **Progresso scolastico e nei giochi:** compiti, voti, punti, skin.
- **Acquisti:** abbonamenti, store, streaming.
- **Famiglia:** email dei genitori o gruppi di classe.

Come avvengono i furti di password

- **Data breach:** un sito (o app) a cui sei iscritto viene “bucato” e le password finiscono online.
- **Riutilizzo password:** stessa password ovunque, se cade una cadono tutte.
- **Spia sulla spalla:** qualcuno guarda mentre digiti, come un ladro alla finestra.
- **SIM swap:** rubano il numero e ricevono i tuoi SMS.

Menzione a parte per la più subdola delle truffe, il **Phishing**: è una truffa online in cui i criminali tentano di rubare dati sensibili (come password, numeri di carte di credito o altre informazioni personali) inducendo le vittime a rivelarli, spacciandosi per enti o persone fidate. Gli attacchi, che possono avvenire tramite email (phishing), SMS (smishing) o app di messaggistica (come Whatsapp), sfruttano un falso senso di urgenza o paura, spingendo le persone ad agire senza pensare. (Ad esempio sei stai aspettando un pacco, sarai propenso a cliccare su un link del trasportatore).

Come funziona il phishing

Fingersi attendibili: I truffatori inviano messaggi che appaiono legittimi, utilizzando loghi e design di aziende note (es. banche, servizi di e-commerce come PayPal o Amazon).

Creare urgenza o paura: Il messaggio può segnalare attività sospette, il blocco del conto o un problema urgente, spingendo la vittima a cliccare su un link.

Raccogliere dati: Cliccando sul link, la vittima viene indirizzata a un sito web falso, identico a quello originale, dove le viene richiesto di inserire le proprie credenziali o dati sensibili, che finiscono così nelle mani dei criminali.

Altre varianti: smishing truffe via SMS o chiamate fasulle dette vishing.

Segnali di allarme e a cosa prestare attenzione:

- **Urgenza o paura:** Tattiche che inducono a rispondere immediatamente, senza riflettere.
- **Richieste di denaro o dati sensibili:** Una richiesta inaspettata di informazioni personali o finanziarie, anche da parte di una persona che conosci, è un segnale di pericolo.
- **Errori grammaticali o di ortografia:** Molti messaggi di phishing contengono errori, specialmente se scritti da persone la cui lingua madre non è quella del messaggio.
- **Messaggi generici:** I messaggi legittimi sono spesso specifici, mentre quelli di phishing possono essere generici e non rivolgersi all'utente per nome.
- **Link e indirizzi email falsi:** Controllare attentamente gli URL (indirizzi web) e gli indirizzi email per verificare che siano corretti e non abbiano piccole differenze rispetto a quelli legittimi. (Ad esempio g00gle.com e google.com)
- **Allegati con strane estensioni** (.zip, .exe, .scr)
- **Vincite di soldi iPhone, sconti incredibili o altro** truffe che richiedono di cliccare\inserire dati personali.
- **QR-code** attaccati su cartelli o volantini (possono portare a siti fake).

Regole d'oro per una password forte

- **Lunghezza:** almeno 12 caratteri, meglio se una frase.
- **Varietà:** lettere maiuscole e minuscole, numeri e simboli.
- **Unicità:** non riutilizzare mai la stessa password.
- **Non personale:** niente nome, squadra, compleanno.

Esempi:

Debole: mario2008

Media: Mario2008!

Forte: G8!z-pAv3#Qm19

Una password forte e più semplice da ricordare è quella che sfrutta una frase lunga che ricordi facilmente detta **Passphrase**: Ad esempio: IL-MIO-GATTO-SI-CHIAMA-007 è lunga, facile da ricordar e difficile da indovinare.

Evita frasi famose o canzoni: meglio combinazioni originali.

Oppure, per una password ancora più breve ma comunque molto sicura, puoi utilizzare il trucco della **Passphrase criptata**: “A scuola alle 8 entro con 3 amici!” diventa As@8ec3a!

Manager di password: il tuo caveau digitale

Ricordare decine di password fortissime è impossibile. Ecco perché esistono i password manager: **tengono tutte le password in un archivio cifrato, protetto da una sola password maestra** (che dev'essere la più lunga e segreta di tutte).

Ecco cosa fanno i password manager:

- Creano password complesse automaticamente
- Le salvano e sincronizzano tra dispositivi.
- Avvisano se una password è debole o riutilizzata.
- Segnalano possibili fughe di password da altri siti ma in qualche modo legate a te (Data Breach)

Pro & contro dei password manager

Pro: sicurezza molto più alta, meno stress, password uniche.

Contro: devi proteggere bene la password maestra; se la dimentichi, può esser complicato recuperarla o irrecuperabile (per design). Ecco alcune soluzioni sia gratuite che a pagamento:

Tabella comparativa (sintesi)

Servizio	Sicurezza	Piattaforme	Note	Costo indicativo
iCloud Keychain	Alta (ecosistema Apple)	Apple	Ottimo se usi solo Apple	Incluso
Google Password Manager	Alta	Android/Chrome/iOS	Integrato, pratico a scuola	Gratis
Bitwarden	Molto alta (open-source)	Tutte	Trasparente, auditabile	Gratis / ~10€/anno Premium
1Password	Molto alta	Tutte	Eccellente per famiglie/team	~3-4€/mese
Dashlane	Molto alta	Tutte	Monitoraggio dark web + VPN	~4-6€/mese
KeePassXC	Molto alta (offline)	Win/Mac/Linux 	Archivio locale, no cloud integrato	Gratis

Impostazioni utili sul telefono:

iOS (iPhone)

- **Face ID/Touch ID + Passcode:** attiva e richiedi passcode complesso.
- **Aggiornamenti automatici:** sempre ON.
- **Password:** Impostazioni → Password → raccomandazioni di sicurezza.
- **Portachiavi iCloud:** per sincronizzare password in modo cifrato.

Android

- **Blocco schermo forte** (PIN lungo o password; impronta per comodità).
- **Aggiornamenti di sistema** e Play Protect attivi.
- **Google Password Manager**: <chrome://password-manager>.
- **Permessi app**: Impostazioni → Privacy → controlla microfono, fotocamera, posizione.

Nota: i dati biometrici (impronta/volto) sono comodi ma non sostituiscono la necessità di password robuste. Sono un “chiudiporta” in più.

Autenticazione a due fattori (2FA/MFA): doppia porta

La 2FA aggiunge un secondo controllo oltre alla password. Così, anche se qualcuno scopre la password (primo fattore), non entra comunque nel dispositivo grazie al secondo controllo (secondo fattore.) Ci sono diversi metodi per attivare il secondo fattore (SMS, App authenticator, notifica push etc) vai su Impostazioni → Sicurezza → 2FA/MFA dell’account.

Tabella riassuntiva – Metodi di protezione

Cosa fai	Protezione ottenuta	Difficoltà
Password lunghe e uniche	Molto alta	Media
Password manager	Molto alta	Bassa (dopo setup)
2FA con Authenticator	Molto alta	Media
Aggiornamenti automatici	Alta	Bassa
Attenzione ai link	Alta	Media (allenamento)

Privacy: proteggi i tuoi dati



Ogni volta che usi lo smartphone lasci dietro di te tracce digitali: **messaggi, foto, ricerche, posizione, abitudini di consumo**. Tutte queste informazioni compongono la tua identità online, una sorta di “gemello digitale” che parla di te molto più di quanto immagini. **Proteggere la privacy significa difendere il controllo su chi sei, su come vieni percepito e su come le aziende e le persone possono influenzarti.**

“La privacy non è nascondere qualcosa, è il potere di scegliere cosa condividere.” — Anonimo

“Se un servizio è gratis, allora il prodotto sei tu.” — Andrew Lewis

“La privacy è un diritto umano fondamentale.” — Tim Cook

Perché la privacy è importante

- **Reputazione:** un post o una foto di oggi può riemergere tra dieci anni, in contesti molto diversi.
- **Sicurezza:** più dati condividi, più diventi un bersaglio per truffe, furti d'identità o cyberbullismo.
- **Autonomia:** ogni tuo comportamento online alimenta algoritmi che decidono cosa mostrarti (pubblicità, notizie, perfino truffe e fake news).
- **Libertà:** senza privacy ogni scelta viene osservata, e questo frena l'espressione personale e la creatività.

Cronaca e casi reali

Cambridge Analytica (2018): milioni di profili Facebook usati senza consenso per influenzare elezioni politiche.

Data breach Yahoo (2013–14): violati 3 miliardi di account, con perdita di email, password e domande di sicurezza.

TikTok e minori (2021–23): multe in UE per la gestione inadeguata dei dati degli adolescenti.

WhatsApp (2021): polemiche sulla condivisione dei dati con Facebook.

Italia (2023): il Garante blocca temporaneamente ChatGPT per scarsa trasparenza nell'uso dei dati.

Quali dati raccoglie lo smartphone?

- **Posizione:** GPS, celle telefoniche, Wi-Fi.
- **Contatti e rubrica telefonica** della SIM o del telefono.
- **Messaggi e chiamate** (metadati: chi, quando, quanto).
- **Navigazione web:** siti visitati, ricerche, click.
- **Utilizzo app:** tempo di utilizzo, funzioni più usate, scroll.
- **Microfono e fotocamera:** accessibili con permessi.
- **Dati sanitari:** battito, sonno, passi registrati da app fitness.

Le regole fondamentali della privacy personale

1. Pensa prima di condividere

Ogni informazione che pubblichi online racconta qualcosa di te: chiediti sempre se è davvero necessario.

2. Ricorda che internet ha memoria lunga

Un post, una foto o un commento possono riapparire anche dopo molti anni e in contesti imprevisti.

3. Condividi solo ciò che serve

In generale, meno dati sensibili diffondi, più sei al sicuro. Proteggi la tua vita privata limitando le informazioni personali.

4. Controlla i permessi delle applicazioni

Non accettare automaticamente tutte le richieste: se un'app non ha bisogno di accedere a contatti, foto o posizione, nega il consenso.

5. Disattiva ciò che non usi

GPS, Bluetooth e Wi-Fi aperti senza motivo rendono più facile il tracciamento. Accendili solo quando servono davvero.

6. Proteggi i tuoi archivi

Backup, foto e documenti devono essere custoditi in modo sicuro: usa password robuste e, quando possibile, sistemi di cifratura.

Strumenti di protezione della privacy

- **Modalità privacy dei browser:** utile, ma non anonima.
- **VPN:** cifra il traffico, fondamentale nei Wi-Fi pubblici.
- **Motori di ricerca alternativi:** DuckDuckGo, Ecosia, Qwant.
- **Browser privacy-friendly:** Firefox, Brave.
- **Ad blocker / anti-tracker:** uBlock Origin, Privacy Badger.
- **Gestione cookie:** buona regola è rifiutare quelli di terze parti.
- **Controllo attività Google/Apple:** si possono disattivare cronologie e tracciamenti.

Norme e diritti

GDPR (Regolamento europeo sulla protezione dei dati) è il regolamento europeo sulla protezione dei dati che stabilisce norme per il trattamento dei dati personali e la loro libera circolazione, per garantire alle persone un maggiore controllo sui propri dati e alle imprese condizioni uniformi. Cosa prevede in breve:

- **Consenso esplicito:** le aziende devono chiedere il permesso per usare i tuoi dati.
- **Diritto di accesso:** puoi sapere quali dati hanno su di te.
- **Diritto all'oblio:** puoi chiederne la cancellazione.
- **Portabilità:** puoi scaricare i tuoi dati e trasferirli altrove.

Le aziende rischiano multe fino al 4% del fatturato globale.

Proteggere la tua privacy non significa vivere con paura, ma avere il controllo della tua vita digitale.

Ogni volta che usi lo smartphone, ricorda: sei tu a decidere cosa mostrare e cosa tenere per te.

Se impari a scegliere con attenzione, internet può essere un posto bellissimo dove divertirti, imparare e condividere con gli amici, senza rischiare di perdere la tua libertà o la tua sicurezza.

Tabella rischi e soluzioni

Rischio	Esempio	Conseguenza	Contromisura
Profilazione pubblicitaria	Pubblicità basata su ricerche	Perdita di riservatezza	Blocca cookie terze parti, browser privacy
Data breach	Hackeraggio di un social	Furto password, identità	Password uniche + 2FA
App invadenti	Torcia che chiede contatti	Raccolta dati inutili	Controllo permessi app
Geolocalizzazione continua	Social con check-in automatico	Sorveglianza movimenti	Disattiva GPS se non serve
Social oversharing	Foto con indirizzo di casa	Furti, stalking	Non condividere dettagli sensibili

7 suggerimenti pratici per la tua privacy online

1. Controlla periodicamente i permessi delle app.
2. Cancella le app inutilizzate.
3. Imposta i post social su “Solo amici”.
4. Usa un’email secondaria per iscrizioni non importanti.
5. Evita foto con posizione in tempo reale.
6. Scegli chat con cifratura end-to-end (Signal, WhatsApp).
7. Leggi almeno le sezioni chiave delle informative privacy.

La privacy non è una fissazione né un modo per creare paura: è una parte fondamentale dell’educazione digitale. In famiglia e a scuola si possono introdurre semplici attività:

Parlare apertamente di privacy

Spiegare che proteggere i propri dati non significa “nascondere qualcosa”, ma scegliere chi può vedere certi aspetti della nostra vita.

Fare esperimenti concreti

Cercare il proprio nome online e osservare insieme i risultati: quali informazioni compaiono? Ci sono foto, commenti, indirizzi? È un modo efficace per capire quante tracce lasciamo senza accorgercene.

Collegare la privacy al rispetto reciproco

Così come non si leggono i diari privati degli altri, allo stesso modo non si devono diffondere dati o immagini senza permesso. Educare alla privacy significa anche educare al rispetto degli altri

Checklist rapida Password e Privacy



Password forti e 2FA



Profili social privati



Posizione attiva solo se serve



Permessi app controllati



Backup sicuri e cifrati

Navigazione protetta
(VPN/browser privacy)

Proteggere la privacy non significa isolarsi, ma scegliere consapevolmente cosa condividere, con chi e per quanto tempo.

La consapevolezza trasforma lo smartphone in uno strumento di libertà, non in una finestra aperta sulla tua vita.

Benessere digitale: tra online e offline



Lo smartphone è uno strumento fantastico: ti permette di parlare con gli amici, studiare, scoprire musica, giocare, fotografare, condividere momenti.

Ma, come tutte le cose potenti, può diventare anche un problema se usato senza equilibrio e consapevolezza.

Il benessere digitale significa imparare a gestire il tempo online in modo che la tecnologia migliori la tua vita, invece di controllarla.

“Non c’è niente di male nell’accendere lo smartphone. Il problema è non riuscire a spegnerlo.” — Anonimo

Perché è importante parlare di benessere digitale

- **Tempo:** le ore davanti allo schermo possono togliere spazio a famiglia, sonno, sport, amici dal vivo.
- **Concentrazione:** notifiche continue interrompono lo studio e rendono più difficile ricordare le cose.
- **Relazioni:** troppa vita online può ridurre la qualità dei rapporti faccia a faccia.
- **Emozioni:** social e like influenzano l’autostima, soprattutto in adolescenza.
- **Salute fisica:** postura, vista e sonno peggiorano con un uso eccessivo.

Cronaca e casi reali

OMS (Organizzazione Mondiale della Sanità): raccomanda massimo 2 ore al giorno di tempo ricreativo davanti a schermi per bambini e adolescenti.

Instagram e adolescenti: ricerche interne di Meta hanno mostrato che un uso eccessivo può peggiorare la percezione del proprio corpo, soprattutto tra le ragazze.

Italia e Germania in alcune scuole superiori sono stati introdotti “**giorni senza smartphone**” per migliorare attenzione e socialità.

Segnali di un uso poco sano dello smartphone

Non riesci a staccarti nemmeno per pochi minuti.
Controlli il telefono di notte, perdendo ore di sonno.
Ti distrai continuamente durante lo studio.
Ti senti nervoso o triste se non hai like o messaggi.
Preferisci stare online piuttosto che uscire con gli amici.

Regole fondamentali per il benessere digitale:

- **Tempo consapevole:** controlla quanto usi lo smartphone (funzioni “Tempo di utilizzo” o “Digital Wellbeing”).
- **Routine sane:** niente telefono a tavola e poco prima di dormire.
- **Notifiche ridotte:** disattiva quelle non necessarie.
- **Equilibrio:** per ogni ora online, ritagliati tempo offline (famiglia, amici, sport, libri, artigianato).
- **Spazi liberi da schermo:** camera da letto e momenti di studio senza distrazioni.

Strumenti utili

- **Timer e limiti app:** Android e iOS permettono di bloccare app dopo un certo tempo.
- **App benessere digitale:** Forest, Freedom, Digital Detox.
- **Modalità “Non disturbare”:** per studiare o dormire senza notifiche.
- **Report settimanali:** controlla i dati e valuta se ridurre.

Educazione familiare e scolastica

Parlarne apertamente: genitori e figli possono stabilire insieme regole d'uso.

Giornate detox: provare a passare un pomeriggio senza smartphone e vedere l'effetto.

Esempi concreti: fare ricerche su quanto tempo passa online tutta la classe e discuterne.

Regole condivise: stabilire orari senza telefono a casa o a scuola.

Tabella – Rischi digitali e buone pratiche per adolescenti

Rischio	Conseguenza	Buona pratica
Tempo eccessivo online (5–6 ore al giorno sui social o giochi)	Riduzione del sonno, meno sport e tempo per amici dal vivo	Impostare limiti app e alternare attività online/offline
Notifiche continue	Distrazioni durante studio e lettura, calo di concentrazione	Usare modalità “Non disturbare” e disattivare notifiche non essenziali
Dipendenza da like e commenti	Ansia, bassa autostima, ricerca continua di approvazione	Ricordare che i like non definiscono il proprio valore; condividere solo ciò che fa star bene
Gaming eccessivo (sessioni notturne)	Stanchezza, rendimento scolastico più basso, irritabilità	Stabilire orari fissi e pause regolari
Multitasking forzato (chat mentre si studia)	Memoria ridotta, difficoltà a finire i compiti	Tenere lo smartphone lontano dallo spazio di studio



Il benessere digitale non significa rinunciare allo smartphone, ma usarlo in modo che arricchisca la vita senza rubarla.

Con scelte consapevoli puoi trasformare il tempo online in un alleato per imparare, crescere e divertirti, senza che diventi un ostacolo al tuo futuro.

Social Network: il villaggio globale



I social network sono come **una piazza mondiale, dove tutti possono parlare, mostrare, condividere, raccontare e ascoltare.**

A differenza delle piazze reali, però, ogni parola resta scritta, ogni foto può essere salvata, ogni video può fare il giro del mondo in pochi secondi.

Per questo sono strumenti affascinanti ma anche delicati: possono avvicinare le persone o ferirle, informare o confondere, divertire o isolare.

Età minima e regole

Tutti i social impongono **un'età minima di 13 anni** (in Europa, può essere 14 o 16 in base alla legge locale).

Questo serve per proteggere i minori **da pubblicità invasive, raccolta di dati personali e contenuti non adatti come violenza e pornografia, e contro adescamenti e truffe.**

Eppure, secondo un rapporto di EU Kids Online 2024, più del 40% dei bambini europei tra 9 e 12 anni ha già un profilo social, spesso con **età falsa**.

Dichiarando un'età diversa per iscriversi ai social, si rinunciano a molte tutele: la piattaforma non è obbligata a intervenire in caso di problemi.

I lati positivi dei social

Usati con attenzione, i social possono essere spazi di crescita e di scoperta:

- **Restare in contatto** con amici e parenti lontani.
- **Esprimere la propria creatività:** musica, disegni, video, storie.
- **Scoprire contenuti educativi o scientifici** (divulgatori, musei digitali, scuole online).
- **Collaborare in progetti**, cause sociali, raccolte fondi o attività scolastiche.
- Imparare il valore della **reputazione digitale**.

I rischi nascosti dei social

- 1. Cyberbullismo** – insulti, minacce o prese in giro pubbliche che possono lasciare cicatrici emotive profonde.
- 2. Confronto sociale** – il continuo paragone con vite apparentemente “perfette” abbassa l'autostima e crea ansia.
- 3. Dipendenza digitale** – lo “scroll infinito” può farti perdere ore senza accorgertene.
- 4. Fake news e disinformazione** – notizie false o manipolate si diffondono più velocemente di quelle vere.
- 5. Adescamento online** – adulti che fingono di essere coetanei per ottenere fiducia o foto personali.
- 6. Perdita di privacy** – ogni “like” o commento lascia una traccia utile a chi vuole profilarti o venderti qualcosa.

Come funzionano gli algoritmi dei social

Dietro ogni feed, c'è un algoritmo (cioè una sequenza di istruzioni chiaramente definite per risolvere un problema o svolgere un compito) che decide cosa mostrarti ogni volta.

Non sceglie a caso: osserva tutto ciò che fai sulla piattaforma, i post che guardi, i video che non salti, i commenti che scrivi, le pagine che segui, i “mi piace” e i “cuoricini” che lasci e **usa queste informazioni per costruire un profilo digitale su di te.**

Questo processo si chiama profilazione.

In pratica, il social impara a conoscerti: sa che musica ascolti, che sport segui, che orari preferisci e persino quando sembri più felice o più triste.

Con questi dati, ti propone contenuti simili, pubblicità mirate e persone “affini”. Ad esempio: Immagina di guardare molti video di cani. L'algoritmo penserà: “Gli piacciono gli animali!”.

Da quel momento inizierà a mostrarti ancora più video di cani, la pubblicità di croccantini e magari anche campagne per adottare un cucciolo. Funziona bene, vero?

Sì, ma il rovescio della medaglia è che vedrai sempre di più lo stesso tipo di contenuto, come se il resto del mondo sparisse.

Cos'è la profilazione

La profilazione è la raccolta e analisi dei tuoi comportamenti digitali per creare un identikit dei tuoi gusti, interessi e abitudini. Ogni piattaforma ne fa uso: YouTube consiglia video, Instagram suggerisce post, TikTok regola il “Per Te” in base a quanto tempo resti su ogni clip. Questi sistemi non leggono la tua mente, ma leggono i tuoi gesti. ***Alcuni dei dati usati per la profilazione:***

- **Tempo trascorso su certi contenuti**
- **Like, commenti, condivisioni**
- **Persone o hashtag seguiti**
- **Luogo, lingua e orario di connessione**
- **Tipo di dispositivo usato**

Tabella – Profilazione: pro e contro

Aspetto	Vantaggi (Pro)	Rischi e svantaggi (Contro)
Personalizzazione	Ti mostra contenuti più vicini ai tuoi gusti e interessi.	Ti chiude in una “bolla” e riduce la varietà di opinioni.
Esperienza utente	Navigazione più fluida e veloce: trovi ciò che ti piace.	Ti rende “prevedibile” e più facile da influenzare o manipolare.
Pubblicità mirata	Ricevi offerte più utili e pertinenti.	Le aziende possono sapere troppo di te e sfruttare le tue debolezze emotive.
Sicurezza dei minori	I social filtrano certi contenuti non adatti all'età dichiarata.	Se dichiari un'età falsa, perdi le protezioni e ricevi contenuti inappropriati.
Ricerca e apprendimento	Puoi scoprire più facilmente ciò che ti appassiona (scienza, musica, sport).	Rischi di restare intrappolato solo in un tipo di informazione.
Controllo e trasparenza	Alcune piattaforme offrono opzioni per gestire i dati raccolti.	Spesso le impostazioni sono nascoste o difficili da capire.

La profilazione non è sempre un male: se gestita bene, può rendere il web più utile e personalizzato.

Il problema nasce quando non ne siamo consapevoli e lasciamo che siano gli algoritmi a scegliere per noi.

Trend, influencer e viralità

Ogni giorno nascono nuove sfide, meme, mode e influencer.

Alcune sono innocue e divertenti, altre invece possono essere pericolose.

Le sfide virali possono spingere a comportamenti rischiosi (come nel caso del Blackout Challenge o di video con atti vandalici).

Gli influencer mostrano solo una parte della loro vita: ciò che vediamo è selezionato, filtrato, montato.

La viralità non misura il valore, ma la velocità con cui qualcosa si diffonde e non sempre è un bene. In generale, non tutto ciò che diventa virale è bello e utile. A volte, è solo fastidioso rumore.

Tabella – Buone pratiche sui social

Situazione	Rischio principale	Buona pratica consigliata
Creare un profilo con età falsa	Mancanza di protezione legale e privacy	Usare la vera età o attendere il momento giusto
Pubblicare foto personali	Uso improprio, furti di identità	Limitare visibilità, usare solo canali privati
Accettare tutti come "amici"	Truffatori o adulti sconosciuti	Aggiungere solo persone realmente conosciute
Litigare o rispondere agli insulti	Escalation di conflitti, cyberbullismo	Segnalare, bloccare, parlarne con un adulto
Credere a ogni post o video	Fake news e manipolazione	Controllare la fonte e confrontare diverse testate
Passare ore a scrollare	Perdita di tempo e concentrazione	Impostare limiti o usare app di monitoraggio del tempo
Partecipare a "sfide virali"	Pericoli fisici o psicologici	Informarsi prima e rifiutare le challenge rischiose
Copiare influencer	Perdita di autenticità, stress da confronto	Seguire solo chi trasmette valori positivi e reali

Strumenti di protezione

- **Impostazioni di privacy** → controlla chi può vedere post, storie e messaggi.
- **Segnalazione e blocco** → strumenti efficaci contro chi molesta o diffonde odio.
- **Controllo del tempo** → quasi tutti i social offrono timer o notifiche di limite.
- **Contenuti per età** → attiva i filtri per bambini o adolescenti.
- **Condivisione consapevole** → prima di postare, chiediti: mi dispiacerebbe se questa foto finisse in mano a chiunque?

I social network sono come un coltello affilato: possono tagliare la noia o ferire profondamente.

Non sono buoni o cattivi in sé: dipende da come li usi.

Sta a te decidere se diventeranno una fonte di ispirazione o una prigionia di paragoni e ansie.

Usa i social come un megafono per le tue idee, non come una gabbia per i tuoi pensieri.

E fai sempre attenzione agli sconosciuti che incontri online, come nella realtà, dietro uno schermo, anche i lupi possono travestirsi da pecore.

Tabella – Età minima e regole principali dei social network (Europa / Italia, aggiornamento 2025)

Piattaforma / App	Età minima ufficiale	Funzionalità limitate per minori	Note utili e strumenti di protezione
TikTok	13 anni	Account privato per default sotto i 16 anni, messaggi disattivati <16, live e donazioni vietate <18	Centro famiglia "Family Pairing", limiti di tempo e filtro contenuti
Instagram	13 anni	Profilo privato automatico <16, pubblicità limitata, messaggi solo da amici	Supervisione genitori, filtro contenuti sensibili, promemoria "Take a break"
YouTube	13 anni (account standard)	Commenti disattivati per video per bambini, pubblicità limitata	YouTube Kids per under 13 con profili controllati e timer di utilizzo
Facebook	13 anni	Pubblicità personalizzata limitata, suggerimenti di amici controllati	"Tempo di utilizzo" e controllo genitori attivi
Snapchat	13 anni	Geolocalizzazione disattiva per default, amici solo tra contatti reciproci	"Family Center" per genitori, segnalazioni rapide in chat
WhatsApp	13 anni (globale, ma 16 consigliati in UE)	Nessuna pubblicità, crittografia automatica	Controllo genitori su Android/iOS, avviso automatico per under 16
Telegram	16 anni (consigliato)	Nessun controllo reale sull'età, gruppi pubblici accessibili	Usare solo con supervisione; rischio contenuti inappropriati
Discord	13 anni	Filtri automatici per contenuti espliciti, ma server pubblici aperti	"Safety Hub" e parental control disponibili
X (Twitter)	13 anni	Nessun filtro automatico, pubblicità ridotta per minori	Sconsigliato sotto i 16 anni; verifica manuale profili
BeReal	13 anni	Nessuna pubblicità mirata, contenuti solo tra amici	Focus su autenticità, ma condivisione quotidiana obbligatoria
Pinterest	13 anni	Filtri per contenuti sensibili, pubblicità limitata	Ambiente relativamente sicuro e creativo
Twitch	13 anni	Chat e donazioni vietate <18, streaming sotto supervisione	Attivare "Safe Mode" e parental control

Messaggistica: media e parole in tasca



Ogni giorno miliardi di messaggi attraversano il mondo in pochi secondi: “ci vediamo dopo?”, “hai fatto i compiti?”, “guarda questo video!”.

La messaggistica istantanea è diventata la forma principale di comunicazione per ragazzi e adulti. È veloce, gratuita e diretta. Ma in tasca non abbiamo solo le parole: ci sono foto, audio, video, link, emoticon, vocali e file, tutti elementi che, se usati con leggerezza, possono diventare armi o prove.

“Le parole sono come frecce: una volta scoccate, non tornano indietro.” Proverbio arabo

“La tecnologia è neutrale: ciò che conta è l’uso che se ne fa.” — Tim Berners-Lee

“Il messaggio più sicuro è quello che non ferisce nessuno.” — Anonimo

La rivoluzione delle chat

Le prime chat digitali nascono negli anni '90 con ICQ, MSN Messenger e Yahoo! Chat.

Poi arrivano gli SMS, costosi ma rivoluzionari: 160 caratteri che hanno cambiato la comunicazione.

Nel 2009 WhatsApp introduce la messaggistica gratuita via internet.

Oggi, tra WhatsApp, Telegram, Signal, Messenger, Discord e Snapchat, si scambiano oltre 100 miliardi di messaggi al giorno.

Le chat sono diventate il nostro salotto digitale: rapide come una telefonata, ma scritte come una lettera. E permanenti, come un post.

Cosa succede davvero quando invii un messaggio

Quando premi “Invia”, il tuo messaggio viene:

1. **Cifrato (nei sistemi sicuri)** → trasformato in codice indecifrabile.
2. **Trasferito ai server dell'app** (es. Meta per WhatsApp/Messenger, Telegram, Apple per iMessage).
3. **Consegnato al destinatario**, dove viene decifrato e mostrato sullo schermo.

Anche se cancelli un messaggio, potrebbe essere già stato salvato o inoltrato.

Nulla scompare del tutto da internet: screenshot, backup automatici, cloud e archivi conservano molto più di quanto pensiamo.

3) Privacy e sicurezza nelle chat

Non tutte le chat sono uguali. Alcune garantiscono la **cifratura end-to-end (E2E)** — cioè solo mittente e destinatario possono leggere — altre invece conservano i messaggi sui propri server.

App	Crittografia	Backup cifrato	Punti di forza	Rischi o limiti
WhatsApp	E2E su tutte le chat	Sì (opzionale)	Diffusa, sicura	Molti gruppi, possibili catene
Telegram	Solo nelle “chat segrete”	No	Canali, bot, cloud potente	Chat normali non E2E
Signal	E2E di default	Sì	Massima privacy, open-source	Meno usata, serve numero
Messenger	Non sempre E2E	No	Diffusa, social integrato	Pubblicità, tracciamento
Discord	No	No	Comunità e gruppi tematici	Chat pubbliche, moderazione variabile
iMessage	E2E tra dispositivi Apple	Parziale	Integrata su iOS, sicura	Solo per utenti Apple

Le parole che restano

Il grande inganno della messaggistica è la falsa sensazione di intimità.

Scriviamo come se fossimo in privato, ma in realtà:

- Un screenshot può diffondere il messaggio ovunque.
- Le chat di gruppo moltiplicano i destinatari (a volte sconosciuti).
- I vocali e i media rimangono nei backup o nelle gallerie.

Scrivere in chat è come parlare davanti a un microfono: meglio fermarsi un secondo prima di inviare.

Un messaggio impulsivo, un commento offensivo o una foto sbagliata possono diventare prove digitali permanenti.

Chat e linguaggio

Le chat hanno creato un nuovo linguaggio: abbreviazioni, emoji, sticker, GIF.

Sono veloci, espressive, ma possono anche far perdere il tono.

Un “ok” può sembrare freddo; un “va bene!” con il punto esclamativo può sembrare arrabbiato; un’emoji può cambiare completamente il senso di una frase.

3 suggerimenti:

1. Scrivi con chiarezza, non con fretta

Un messaggio impulsivo può sembrare scortese o incompleto. Meglio rileggere prima di inviare.

2. Attento a punteggiatura e maiuscole ed emoji

Un “ok” può sembrare freddo, un “VA BENE!!!” può sembrare urlato. La punteggiatura dà un tono al messaggio.

3. Rispetta i tempi dell’altro

Se non risponde subito, non significa che non voglia parlare. Non bombardare di messaggi: lascia spazio.

Foto, video e media

Oltre ai testi, la chat veicola immagini, vocali, file, link e video. È qui che spesso nascono i problemi più seri:

- Foto e video private condivise senza consenso (reato).
- Video virali o catene false (fake news).
- Giochi pericolosi o “sfide” che girano tra adolescenti.
- Condivisione inconsapevole di dati sensibili (documenti, moduli, password).

Ricorda, un contenuto una volta inviato, non è più tuo. Anche se cancelli un contenuto, può essere salvato, copiato, inoltrato.

Gruppi e dinamiche sociali

I gruppi sono lo specchio digitale della classe o della famiglia: un luogo utile per coordinarsi, ma anche un rischio di caos o bullismo. I rischi tipici riguardano messaggi fuori orario, foto o video offensivi, esclusioni o prese in giro.

Etichetta digitale – Le 10 regole d'oro

1. Non scrivere mai a caldo: conta fino a dieci prima di inviare.
2. Evita urla digitali (MAIUSCOLO) e insulti.
3. Rispetta la privacy altrui: non pubblicare chat o screen senza consenso.
4. Niente spam o catene.
5. Usa il buon senso: emoji e abbreviazioni senza esagerare.
6. Nei gruppi scolastici, resta sul tema.
7. Non inoltrare immagini o video privati.
8. Evita audio troppo lunghi: scrivi se puoi.
9. Chiedi prima di aggiungere qualcuno a un gruppo.
10. Ricorda: il messaggio più potente è la gentilezza.

Strumenti utili comuni nelle app di messaggistica

- **Silenzia chat:** per non essere travolto da notifiche.
- **Archivia:** per tenere ordine senza cancellare.
- **Segnala/blocca** contatti molesti.
- **Backup cifrato:** per salvare conversazioni *importanti in modo sicuro*.

Tabella – Le principali app di messaggistica

App	Età minima	Punti di forza	Limiti o rischi	
WhatsApp	13 anni (16 in UE)	Diffusa, semplice, sicura con crittografia end-to-end; chat, gruppi e chiamate gratuite.	Troppe chat e gruppi, rischio catene e fake news, può creare dipendenza da notifiche.	
Telegram	16 anni	Veloce, supporta canali, bot, grandi gruppi e archiviazione in cloud.	Le chat normali non sono cifrate end-to-end; alcuni canali diffondono contenuti non controllati.	
Signal	13 anni	Massima privacy, open-source, nessuna pubblicità né tracciamento.	Poco diffusa, serve numero di telefono, interfaccia meno familiare.	
Messenger	13 anni	Integrata a Facebook, comoda per contatti social, supporta video e sticker.	Raccolta dati a fini pubblicitari, non sempre cifrata end-to-end.	
Discord	13 anni	Ottima per gruppi di gioco o studio, canali tematici e chat vocali.	Rischi di linguaggio tossico, moderazione variabile, privacy limitata.	
Snapchat	13 anni	Messaggi e foto temporanei, stimola creatività con filtri e storie.	Illusione di "sparizione" dei messaggi: possono essere salvati o catturati.	

Le chat non sono solo tecnologia: sono comunicazione umana. Scrivere con cura, rispettare chi legge, proteggere le immagini e i dati significa essere consapevoli e responsabili.

Le parole in tasca sono potenti: usale per costruire, non per ferire.

Il messaggio più importante è quello che trasmette rispetto.

Browser e navigazione: la porta sul web



Il browser è la finestra sul mondo digitale.

È grazie a lui che possiamo cercare informazioni, guardare video, leggere articoli, studiare e persino lavorare.

È una porta potentissima e come tutte le porte, può aprirsi verso stanze sicure o corridoi pericolosi.

Sapere come funziona significa imparare a orientarsi, come in una città: ci sono vie principali, scorciatoie, ma anche vicoli bui.

Cos'è un browser

Un browser (come Chrome, Safari, Firefox, Edge o Brave) è un programma che ti permette di visualizzare pagine web.

Tradotto: prende il linguaggio dei siti (HTML, CSS, JavaScript) e lo trasforma in immagini, testi e video comprensibili.

Esempio: quando digiti `www.wikipedia.org`, il browser:

1. Contatta un server (un computer lontano che ospita il sito).
2. Riceve le informazioni (testi, immagini, codici).
3. Le mostra sullo schermo in una forma leggibile e interattiva.

Senza browser, il web sarebbe solo ***codice incomprensibile***.

Breve storia della navigazione

1990: Tim Berners-Lee inventa il primo browser: WorldWideWeb (il famoso www).

1993: nasce Mosaic, che introduce le immagini nelle pagine web.

1994–1998: nascono Netscape Navigator e Internet Explorer.

2004: arriva Firefox, open-source e attento alla privacy.

2008: Google lancia Chrome, veloce e minimalista: diventa il più usato al mondo.

2016+: cresce Brave (senza pubblicità invasive) e Edge (nuovo browser Microsoft).

Le nuove generazioni di browser puntano su velocità, privacy e intelligenza artificiale integrata.

Come funziona la navigazione

Ogni sito ha un indirizzo (**URL**), es:

`https://www.museoscienza.it/mostre/fisica.html`

https:// → indica il protocollo di sicurezza (HTTPS è cifrato, HTTP no).

www.museoscienza.it → è il dominio, cioè “l’indirizzo di casa” del sito.

/mostre/fisica.html → è la pagina specifica.

Quando scrivi un indirizzo o una parola da cercare, il browser fa un piccolo viaggio digitale.

Prima interroga il DNS (Domain Name System), una specie di rubrica telefonica di Internet.

Il DNS traduce i nomi dei siti (come `www.museoscienza.it`) nei numeri IP, che sono gli indirizzi reali dei server dove le pagine vivono, un po’ come le coordinate GPS di una casa.

Una volta trovato l’indirizzo giusto:

1. Il browser bussa al server e chiede: “Mi mandi questa pagina?”
2. Il server risponde inviando testi, immagini, video e codice.
3. Il browser mette tutto in ordine e lo mostra sullo schermo, seguendo le regole grafiche stabilite dal sito (HTML per il testo, CSS per lo stile, JavaScript per l’interattività).

Tutto questo avviene in frazioni di secondo.

Ogni volta che navighi, milioni di pacchetti di dati viaggiano avanti e indietro, invisibili ma coordinati come una danza perfetta tra il tuo dispositivo e il mondo.

Navigare in sicurezza

Navigare bene non significa solo trovare ciò che cerchi, ma farlo in modo sicuro attraversando **siti affidabili**. Ecco come riconoscerli:

- Hanno **https://** (la “s” indica connessione cifrata e sicura) ad esempio **https://www.google.com**
- Mostrano un lucchetto accanto all’indirizzo.
- Non hanno errori, messaggi strani o pubblicità eccessive.
- Mostrano informazioni chiare su chi li gestisce (contatti, “chi siamo“, partita iva, privacy policy etc).

Attenzione a:

- Siti che chiedono dati personali senza motivo.
- Link abbreviati o sospetti (`bit.ly/xyz`).
- Finte pagine di login simili a quelle ufficiali (phishing).
- Pop-up che promettono premi, sconti o regali.

In generale su internet, se qualcosa sembra troppo bello per essere vero, probabilmente non lo è.

Strumenti comuni per navigare meglio

- Segnalibri: per salvare siti affidabili o utili.
- Estensioni: piccole funzioni extra (es. dizionari, traduttori, blocca-pubblicità o script indesiderati).
- Lettura semplificata: rimuove elementi superflui per leggere meglio.
- Controllo ortografico e traduzioni: utile per scrivere correttamente nei moduli online e tradurre in tutte le lingue.
- Ricorda: la sicurezza non dipende solo dal browser, ma anche da cosa clicchi e in che siti navighi.
- Aggiorna sempre il browser all’ultima versione disponibile
- Controlla nelle impostazioni la sezione **Sicurezza e Privacy**: è lì che si trovano le vere difese digitali.

Come riconoscere le bufale online e i titoli clickbait

Non tutti i siti sono affidabili. Per distinguere verità e fake news:

- 1. **Controlla la fonte:** è un sito noto o sospetto?
- 2. **Leggi l'autore:** è indicato un giornalista, un nome reale o un nickname inventato?
- 3. **Verifica la data:** notizie vecchie possono riapparire come nuove.
- 4. **Confronta più fonti:** se solo un sito o fonte parla di una cosa, soprattutto se incredibile, probabilmente non è vera.
- 5. **Attento ai titoli gridati:** “Shock!”, “Incredibile!”, “Non crederai ai tuoi occhi!” = **segnale d’allarme di titoli click bait** (cioè un testo che spinge l’utente a cliccare, ma non sempre informa in modo corretto e onesto)

Browser a confronto

Browser	Punti di forza	Limiti o rischi	
Google Chrome	Veloce, compatibile con tutto, sincronizzazione con account Google.	Raccoglie molti dati per pubblicità, alto consumo di memoria.	
Mozilla Firefox	Open-source, molto attento alla privacy, personalizzabile.	Leggermente più lento su siti pesanti.	
Safari	Ottimizzato per Apple, efficiente e con protezione anti-tracking.	Solo per dispositivi Apple.	
Microsoft Edge	Integrato in Windows, veloce, include strumenti per scuola e lettura.	Alcuni tracciamenti Microsoft attivi per impostazione predefinita.	
Brave	Blocca pubblicità e tracker automaticamente, veloce, privacy elevata.	Alcuni siti non funzionano correttamente con il blocco attivo.	
Opera	Veloce, VPN integrata, risparmio dati su mobile.	Proprietà straniera, meno trasparente nella gestione dati.	

INDICE

1. Hardware: il corpo dello smartphone
2. Software: l'anima del telefono
3. Reti e connessioni: lo smartphone parla col mondo
4. Fotocamera: gli occhi digitali del telefono
5. Password e sicurezza: le chiavi del castello
6. Privacy: proteggere i tuoi dati
7. Benessere digitale: equilibrio tra online e offline
8. Social network: il villaggio digitale
9. Messaggistica: le parole in tasca
10. Browser e navigazione: la porta sul Web

Per fare i quiz collegati a
www.quiz-patente-smartphone.it
o inquadra il codice QR.



GLOSSARIO ESSENZIALE

Glossario essenziale per utilizzare il tuo smartphone



1. 2FA (Due Fattori)

La doppia porta del castello. Oltre alla password, serve un secondo codice (via SMS o app). Anche se rubano la password, senza il tuo telefono non entreranno.



2. Algoritmo

Il motore invisibile. Istruzioni che osservano cosa ti piace e commenti per decidere cosa mostrarti dopo. Il suo scopo è farti restare sull'app il più a lungo possibile.



3. Backup

La fotocopia di sicurezza. Salvataggio dei dati (foto, documenti) in uno spazio esterno (es. Cloud). Fondamentale per non perdere tutto se il telefono si rompe.



4. Clickbait

L'"esca" per i clic. Titoli esagerati ("Non crederai mai a...") scritti per incuriosirti. Spesso, dietro al link, la notizia è deludente o falsa.



5. Cloud

Cassaforte tra le nuvole. Spazio digitale su server lontani dove salvare i dati per averli sempre a disposizione su qualsiasi dispositivo connesso a Internet.



6. Cookie

Le "briciole" digitali. File lasciati nel browser per ricordarsi di te. Quelli "di terze parti" tracciano la navigazione per mostrarti pubblicità mirate.



7. CPU (Processore)

Il cervello dello smartphone. Chip che prende decisioni ed esegue i programmi. Più è potente, più il telefono è veloce nel multitasking.



8. Data Breach

Falla nelle difese. Hacker rubano dati a un'azienda (email e password). Se usi la stessa password ovunque, tutti i tuoi account sono a rischio.



9. Deepfake

L'illusione perfetta. Video o audio manipolati con l'IA. Sostituiscono o imitano realisticamente volti e voci, facendo dire cose mai avvenute.



10. DNS

Rubrica di Internet. Traduce gli indirizzi dei siti leggibili (www.google.com) nei numeri IP che i computer usano per trovarsi tra loro.



11. E2E (Crittografia)

Il lucchetto segreto. Rende i messaggi indecifrabili. Solo tu e chi riceve avete la chiave. Nemmeno l'app (es. WhatsApp) può leggerli.



12. Fake News

Bugie vestite da notizie. Informazioni false create per ingannare, fare soldi o influenzare opinioni. Verificare la fonte è vitale per difendersi.

CONTINUAZIONE GLOSSARIO (G - V)



13. GDPR

Lo scudo per i dati. Legge europea sulla privacy. Obbliga le aziende a chiedere il permesso per usare i tuoi dati e ti permette di cancellarli.



14. GPS

Bussola spaziale. Usa i satelliti per indicare dove ti trovi. Se lasciato sempre acceso, permette alle app di tracciare ogni tuo spostamento.



15. GPU (Scheda Grafica)

Il pittore del telefono. Processore specializzato nel gestire la grafica, rendendo fluidi i video in HD e gli effetti speciali dei videogiochi.



16. Metadati (EXIF)

Segreti nelle foto. Ogni scatto salva non solo l'immagine, ma anche dati invisibili: data, ora, modello del telefono e le coordinate esatte (se GPS attivo).



17. OS (Sistema Operativo)

Direttore d'orchestra. (Es. iOS o Android). È il software di base che fa dialogare i componenti fisici (hardware) con le app installate.



18. Passphrase

La password furba. Invece di una parola complessa, usa una frase lunga (es. "Il-Mio-Cane-Mangia-Pasta"). Impossibile da hackerare, facile da ricordare.



19. Phishing

Pesca a strascico. Messaggio falso (banca, corriere) creato per spaventarti o incuriosirti, spingendoti a cliccare un link per rubare le tue password.



20. Profilazione

L'identikit dei gusti. I social uniscono le "tracce" che lasci navigando per capire chi sei e suggerirti contenuti o pubblicità perfettamente su misura.



21. VPN

Il tunnel segreto. "Maschera" il tuo traffico web e ti protegge sulle reti Wi-Fi pubbliche non sicure, impedendo agli estranei di curiosare nei tuoi dati.

Oltre le parole, la consapevolezza

Conoscere questi termini è il primo passo per non subire la tecnologia, ma per governarla.

Uno smartphone è solo uno strumento: la vera differenza la fa chi lo tiene in mano.

Sii curioso, sii prudente e naviga con intelligenza!