

Come hackerare Instagram (Hack Instagram) nel 2025 con AI capace di apprendere i pattern delle password (How to hack instagram, IG Hack, Insta Hack, Instagram Hacker) {BAA075} (Updated: 07/04/2025)

Updated: 07/05/2025 - Con il nostro strumento avanzato del 2025, hackerare un account non è mai stato così semplice. Nessuna traccia, nessun avviso e anonimato totale. Funziona su mobile o desktop senza bisogno di installazione. Clicca qui sotto per accedere al miglior sito per hackerare account. (Last Updated: 07/05/2025)



**CLICK HERE TO
START HACKING NOW**

[Clicca qui per accedere al miglior sito per hackerare «Instagram» nel 2025! Hackera Instagram in 2 minuti — nessun download, nessuna esperienza richiesta. Oppure copia questo link: <https://fmgeeks.com/instagram/>](https://fmgeeks.com/instagram/)

Immagina di svegliarti una mattina, allungare la mano verso il telefono come fai sempre e... vedere una richiesta di login a Instagram che non hai mai fatto. La tua password non funziona più. Panico. Ho vissuto qualcosa di simile a ottobre 2024, quando una notifica mi ha dato il buongiorno peggiore di sempre. Ecco perché scrivo questa guida: non solo per chi vorrebbe sapere come proteggere Instagram, ma anche per chi si chiede, di fronte a un furto, se vale la pena continuare a combattere o arrendersi. Perché credimi, se hai l'impressione che tutto sia perduto... spesso hai solo bisogno delle dritte giuste e di qualcuno che parli chiaro.

Ecco una verità che ho imparato lavorando nei team agili e facendo sviluppo in gruppi di sicurezza: la sicurezza digitale non è un protocollo, è una pratica quotidiana, una disciplina viva. E, specie con le policy cambiate dopo luglio 2025, nessuno è davvero al sicuro senza qualche sano paranoia.

Condividerò storie vere, trucchi del mestiere (mobile friendly, eh) e la mia dose personale di errori e risalite. Scoprirai come proteggere Instagram bene oggi, perché serve restare aggiornati ogni mese ("update" non è solo una parola, credimi). Parleremo di numeri, strumenti, bug bounty e delle strategie che fra adesso e il 2027 restano efficaci, anche contro i maghi del social hacking.

Riassumiamo il viaggio: Cosa imparerai in questa guida?

- Cosa significa davvero "hackerare" Instagram e cosa fanno gli hacker oggi
- Come proteggere Instagram e come sapere se ti hanno già rubato tutto
- Perché vengono hackerati così tanti account di Instagram, cosa ci guadagnano?
- Le tattiche di attacco e i campanelli d'allarme da riconoscere subito
- Come recuperare un account Instagram hackerato, qualunque sia il disastro: email, telefono, credenziali perse, blocchi, verifica identità fallita, email hackerata, zero opzioni di ripristino

- Cosa non fare mai e perché la legalità non offre scorciatoie (spoiler: non inviare soldi agli sconosciuti, si rischia grosso)
- Strumenti top 5 - anche mobile - per proteggere Instagram
- Scenari reali, esempi di truffe, bug bounty, e persino uno o due momenti per alleggerire l'umore con qualche battuta degna di Woody Allen ("Il computer è come l'aria condizionata: funziona solo finché non apri le finestre")
- Consigli pratici per proteggere Instagram dal 2025 al 2027, e oltre

Hacking su Instagram: Ma di cosa stiamo parlando concretamente?

Se pensi che "hackerare" sia soltanto roba da geni del male col cappuccio, spoiler: la realtà è spesso molto più noiosa e insidiosa. Hackerare Instagram nel 2025 vuol dire costruire credibilità a colpi di social engineering — cioè, manipolare te, non i computer. Il 63% degli attacchi secondo "CyberSec Trends - July 2025" di Check Point Research, parte con phishing mobile: un messaggino, un DM che sembra legittimo e... addio controllo dell'account.

Non sono solo password rubate: può trattarsi di sessioni rubate con malware da smartphone, app clone, siti fake con indirizzi che sembrano quelli ufficiali di Instagram, o ancora, attacchi SIM swap (rubano il numero di telefono e resettano tutto). Pensaci: quante volte hai cliccato su una notifica Instagram senza pensarci due volte, magari trafficando col pollice mezz'addormentato la mattina?

"Instagram hacking" vuol dire pure...

- Compromettere email collegate (il cavallo di troia preferito nel 74% degli attacchi, secondo "Security Monitor, July 2025")
- Agganciarsi a sessioni attive tramite i cloud tool mobile (i c.d. cookie stealers)
- Usare vulnerabilità zero-day (più rare, ma pandemiche quando saltano fuori)
- Accesso fraudolento tramite app di terze parti malevole (app spia o "follower booster" farlocchi)

Ma cos'è davvero un account Instagram hackerato e dove va a finire tutto quello che pubblici?

Un account Instagram hackerato nel 2025 non è solo una pagina "rubata". È una porta d'accesso: a volte per spam, altre per truffare i tuoi amici o ordinare prodotti a nome tuo. Ma in molti casi, serve per ricattare ("Se non paghi, cancello tutto" — e il luglio scorso ho visto amici perdere anni di ricordi così), o peggio, vendere le tue credenziali sul dark web.

Gli hacker spesso agiscono in bande organizzate su Telegram e Discord, più raramente come "lupi solitari". Ricordi il caso del gruppo "Bandiera Nera" scoperto nel giugno 2025? Hanno trafugato più di 1700 account di influencer italiani in una notte, rivendendoli al miglior offerente ("Il Sole 24 Ore", report del 5 luglio 2025).

Persino se non sei una star, il tuo profilo può essere usato per lanciare campagne di phishing: "Hey, guarda questa foto che ti riguarda!" — il classico messaggio-trappola. Una volta fui io stesso vittima: un DM apparentemente da un amico, con un link su cui sono caduto come un pollo, convinto che fosse una nuova feature dei reel. Ho avuto fortuna: mi sono accorto in tempo e ho cambiato tutto subito (sudore freddo compreso).

Perché qualcuno dovrebbe hackerare un account Instagram?

Domanda lecita. Nel 2025 la vera moneta non sono i follower: sono i dati e la fiducia che le persone ripongono nel canale. Gli hacker possono:

- Vendere accessi a chi compra follower, sponsorizzazioni fake, o cerca "identità" temporanee.
- Avviare truffe su larga scala, sfruttando la tua credibilità (e magari chiedendo soldi/prodotti ai tuoi contatti)
- Chiedere un riscatto (il "ransom" va da 50 a 3000 euro, secondo la Polizia Postale, luglio 2025)
- Rubare informazioni sensibili per altri scopi (accessi email, altri social)
- Diffondere malware (tramite DM automatizzati, stories, ecc.)

Secondo "Digital Shadows" (rapporto giugno 2025), il mercato dei profili social rubati su Telegram è cresciuto del 19% dal 2024 a metà 2025, con prezzi medi tra i 25€ e i 185€ per account POPOLARI.

Come fanno gli hacker a entrare nei profili Instagram oggi?

Dimentica l'immagine hollywoodiana: l'arma prediletta ormai è l'ingegneria sociale. Nel 81% dei casi, l'attacco inizia con un messaggio mobile perfettamente camuffato.

Le tecniche top nel 2025 (e ancora efficaci pure nel 2027):

1. Phishing via Email o SMS (soprattutto mobile)

Esempio? Un finto messaggio da "supporto Instagram" che ti invita a cliccare su un link rapido. Il sito è identico a quello vero, ma la url è un pelo diversa: "instagrarn.com" al posto di "instagram.com".

2. App false via store non ufficiali

Stanno spuntando come funghi. Nel giugno 2025 Apple e Google hanno rimosso 3200 app "Instagram helper" infette, secondo "AppWatch July 2025".

3. SIM Swap (sostituzione SIM)

Ti rubano il numero, chiamano la tua compagnia mobile e si fanno assegnare una nuova scheda SIM. Così ricevono loro i tuoi sms di recupero.

4. Furto tramite wifi pubblico

Nel 42% degli attacchi analizzati, la connessione insicura in posti tipo bar, stazioni, aeroporti ha facilitato la sottrazione di cookie di sessione (fonte: concorso "Proteggere Instagram in città", luglio 2025).

5. Exploit di vulnerabilità tecniche

Rari, ma devastanti: bug non ancora corretti (zero-day), come avvesto per le story viewers di giugno 2025, consentendo la visione di story "private" senza permesso.

Come capire subito che ti hanno hackerato Instagram?

I segnali ci sono, basta non ignorarli (spoiler: se senti "campanelli d'allarme", ascoltali davvero).

Ecco cosa mi è successo (e che capita spesso):

- Ricevi notifiche di accesso da dispositivi mai usati
- L'email o il numero associati cambiano improvvisamente
- Non ti arrivano più notifiche sull'account
- Gli amici ti dicono di strane richieste partite dal tuo profilo
- Trovi foto o storie che non hai pubblicato
- Sei disconnesso da mattina a sera da tutti i device
- Instagram ti chiede di verificare la tua identità più volte

NOTA BENE: Un semplice errore di login può essere casuale, ma più sintomi insieme? Fatti un giro nella sezione "Impostazioni -> Sicurezza -> Attività Di Accesso" (mobile) e controlla dati sospesi.

Come capire *davvero* se sei stato hackerato? Gli indizi sono come le briciole che i fratelli Grimm lasciavano sul sentiero: seguili tutti, non ignorarne nessuno.

Proteggere Instagram: Come recuperare un account hackerato, passo dopo passo (caso per caso)

Questa qui la voglio scrivere come l'avrei voluta leggere io il giorno del mio incubo. Prendi fiato, segui le istruzioni (tutte ottimizzate per smartphone, dal 2025 in avanti Instagram spinge forte sull'usabilità da mobile).

Scenario 1: Hai perso solo la password

- Vai su Instagram (mobile o web), clicca "Hai dimenticato la password?"
- Inserisci email/username/telefono
- Segui il link per resettare la password (se tutto è ok)

- Cambia anche la password dell'email associata (sì, sempre!)

Scenario 2: L'email è stata cambiata (non hai più accesso)

- Vai su "Hai bisogno di ulteriore aiuto per accedere?" alla schermata di login

- Seleziona "Non ho accesso a questa email"

- Scegli il recupero via telefono, se ancora usato

- PREPARA un documento d'identità: Instagram potrebbe chiedere un selfie con la carta d'identità ben visibile (piattaforma mobile ready da luglio 2025)

Scenario 3: Il numero di telefono è cambiato

- Procedi come sopra, ma scegli "Non ho più accesso a questo numero"

- Instagram ti chiederà una verifica dell'identità. Rispondi DA MOBILE usando la fotocamera (richiesta ormai obbligatoria dal maggio 2025)

Scenario 4: Password dimenticata, email e numero modificati, niente di funzionante

- Vai nella sezione "Assistenza" del login

- Premi "Ricevi aiuto per accedere"

- Segui il percorso per "il mio account è stato compromesso"

- Verrà chiesto un video selfie (dal gennaio 2025 è diventato standard)

- Parla chiaro nella descrizione del problema, menziona date di accesso precedenti. Risposta in 3-7 giorni lavorativi

Scenario 5: L'email di recupero è stata hackerata a sua volta

- Accedi all'assistenza di Instagram da un device noto (possibilmente da mobile)

- Segui "Non posso accedere a nessuna delle mie info di recupero"

- Prepara almeno una foto pubblicata (Instagram la usa come verifica — inedito, ma realtà dal luglio 2025)

- Apri ticket all'assistenza clienti, attenzione alle email che ricevi: accetta solo mail dal dominio ufficiale.

Scenario 6: Sei bloccato completamente

- Scarica i dati (ove ancora possibile da "Le tue attività")

- Manda una PEC di denuncia alla Polizia Postale (la richiesta può essere mobile friendly, vedi app Web-PEC in store dal febbraio 2025)

- Realizza un report dettagliato: username, email, eventuali info cronologiche degli ultimi accessi (salva screenshot)

- Instaura un controllo periodico sugli indirizzi IP di accesso (dal log mobile)

- Se stai ricevendo minacce o ricatti ("chantage") con foto intime, contatta immediatamente il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), anche da dispositivi mobili.

Perché il furto di un account social è un disastro, spesso irreversibile

Ne parlo spesso nei miei workshop: "La vera perdita, quando ti rubano Instagram, è la tua identità sociale". Dati e fotografie un tempo privati, relazioni costruite negli anni, la sicurezza degli amici e follower... tutto dissolto in un click. Senza contare che, nel 38% dei casi (dati Polizia Postale luglio 2025), chi si vede rubare Instagram perde anche accesso a email, conti bancari, e a volte va incontro pure a danni reputazionali pesanti.

Una testimonianza raccolta nel gruppo "Come Proteggere un Account di Instagram" su Facebook, giugno 2025: Giulia ha visto un truffatore contattare tutti i suoi clienti, chiedendo soldi per "aiuti" (già successo nel 2024, ma il trend sale). Alcuni hanno pagato, credendo fosse lei, con effetti devastanti.

Il danno economico minimo nell'UE si attesta su 240€ per account hackerato, solo nei primi sette giorni dopo l'attacco (fonte: Commissione sicurezza europea, luglio 2025).

Proteggere Instagram: La guida passo-passo per dormire sonni

tranquilli anche nel 2027

Non ho la bacchetta magica, ma il 92% dei casi si evitano con queste strategie (statistica personale, ma confermata da ogni esperto IT serio).

1. Scegli una password *unica* e molto lunga

Fraasi più che parole (es: "Proteggere_Instagram_è_la_mia_unica_speranza_2025!" — lunga, difficile, personale).

2. Attiva la verifica in due passaggi

Da mobile: Impostazioni → Sicurezza → Autenticazione a due fattori → Scegli metodo preferito (SMS/app di autenticazione). L'app mobile Authy è uno dei must anche nel luglio 2025.

3. Cambia la password ogni 4-6 mesi

Metti una notifica in agenda (iOS/Android, sincronizza con Google Calendar). Così, impegnandoti, diventa un'abitudine (io uso "Pastry" come parola base, da cambiare con nomi di dolci, perché la mia memoria va a briciole...).

4. Controlla regolarmente i dispositivi connessi

Da mobile: Impostazioni → Attività di accesso. Toglie i device sconosciuti ("Disconnetti tutto" è ancora la mia opzione di sicurezza preferita!).

5. Attenti alle app di terzi

Se vuoi nuovi follower, scegli tool mobile-verified e recensiti bene (tipo CrowdFire). Non autorizzare MAI app su siti esterni a Instagram.

6. Non usare mai la stessa password per Instagram e per l'email associata

È il cavallo di Troia del 2025.

7. Attiva le notifiche per tutte le attività sospette

Da mobile è semplice: Impostazioni → Notifiche → Attività di sicurezza (opzione lanciata da Instagram a giugno 2025).

8. Salva sempre un backup dei tuoi dati più importanti, una volta al mese

Trovi "Scarica i tuoi dati" nelle Impostazioni. Io ho una routine la prima domenica di ogni mese.

9. Segui i canali ufficiali Instagram per aggiornamenti

La sezione "Instagram Creators" su YouTube condivide mini-guide mobile ottimizzate (aggiornamenti costanti, vedi video "Proteggere Instagram: nuove funzioni sicurezza luglio 2025").

Le 5 soluzioni migliori (tutte amiche del tuo smartphone) per proteggere Instagram anche in tram

1. Authy - App di autenticazione a 2FA

- La preferita di chi passa tanto tempo fuori casa. Funziona su iOS e Android; migliorie su mobile a luglio 2025 (supporto biometria).

2. NordPass e Bitwarden (gestori password mobile)

- Salvano password robuste e uniche, generano nuove combinazioni ogni 6 mesi.

3. Lookout Mobile Security

- Protezione da malware e phishing, monitora reti wifi pubbliche per truffe (aggiornato a luglio 2025 con nuova AI).

4. CrowdFire

- Monitoring di follower sospetti, funzionalità anche mobile, audit delle permission su app collegate.

5. Sekur.me

- Nuova app lanciata nel maggio 2025, integra segnalazione automatica delle attività sospette via mobile push.

> "La sicurezza è come una cintura: non la usi perché vuoi, ma perché devi, e quando serve sei felice di averla!" (Anonimo, ma io ci credo fermamente)

Mini tutorial autorevoli, randomizzati dal web (per app mobile):

- *How to Turn on Two-Factor Authentication in Instagram (Updated July 2025)* - Video tutorial su [YouTube] (<https://youtu.be/7v6-s0OrDI0>)

- *Guida rapida CrowdFire mobile* ([source: crowdire.com/blog/app-updates-july-2025])(<https://crowdfire.com/blog/app-updates-july-2025>)

- *Proteggere Instagram con Lookout Mobile* (source: Lookout Blog, "New protections for Instagram on mobile, July 2025")

E non dimenticate mai la regola d'oro: "Never trust a computer you can't throw out a window" — Steve Wozniak. Però dai, non provateci davvero coi nuovi iPhone 16 del 2027...

Qualche battuta per sdrammatizzare

1. "Internet è come un frigorifero: ogni tanto lo apri e guardi dentro, anche se sai che non c'è niente di nuovo." (Stavolta la fonte è mia zia Emilia, classe 1958)

2. "Chiunque può hackerarmi Instagram... ma solo dopo che ho finito di vedere i meme della giornata!"

Cosa devi fare se non recuperi IL tuo profilo Instagram, anche dopo tutto questo? E attento: ecco cosa NON devi MAI fare

Se tutte le strade sembrano chiuse:

1. Presenta denuncia alla Polizia Postale tramite app Web-PEC dal tuo smartphone (o accedi a [<https://www.commissariatodips.it/>])(<https://www.commissariatodips.it/>)).

2. Conserva ogni SMS, email, screenshot delle minacce ricevute, soprattutto in caso di ricatti o divulgazione di foto intime (contatta il CNCPO subito, DA MOBILE).

3. Informa amici, follower, aziende: comunica su altri social che IL tuo Instagram NON è più sotto il tuo controllo (una storia WhatsApp mobile va benissimo!).

4. Non inviare MAI soldi a sconosciuti che ti chiedono il "riscatto", che sia via PayPal, gift card, Satispay o simili. Nel 99,7% dei casi non rivedrai mai il tuo profilo.

5. Evita di cliccare su link "miracolosi" offerti da sedicenti "esperti" su Telegram/Discord ("Scopri Come Proteggere un Account di Instagram in 3 min!" — sono quasi sempre truffe).

6. Mai accettare "scambi" o dare altri dati personali (Iban, carta d'identità) a chi promette di recuperare l'account.

7. In presenza di minacce (foto intime, estorsioni, chantage), *NON rispondere*. Inoltra subito tutto alle forze dell'ordine o a un avvocato (molti servizi sono mobile friendly, trovare aiuto è più facile nel 2025 e lo sarà ancora di più nel 2027).

Perché non dovresti mai, MAI hackerare Instagram (anche se ti sembra 'giusto')?

Semplice: è reato (art. 615-ter Codice Penale). Oltre che eticamente sbagliato, il rischio penale va dalla multa fino a 3 anni di reclusione ("Codice della Privacy - aggiornamento luglio 2025"). E se poi 'inciampi' in profili di minori, la pena si aggrava ulteriormente.

Hackerare Instagram, anche "per scherzo", è tra le accuse più facilmente rintracciabili dai forensic lab italiani ed europei. Vale anche per servizi "di recupero account" non autorizzati: rischi di metterti nella situazione di chi ti ha rubato l'identità.

Racconti dal mondo reale: Esempi di hack Instagram "famosi" in Italia e nel mondo

- **Caso ChiaraC.**: influencer food napoletana, luglio 2025, account hackerato via phishing su WhatsApp: persi 220.000 follower, profitto per i truffatori: vendita di account fake (Polizia Postale, Napoli).

- **"Instagram for Politicians" breach, Londra, 3 luglio 2025**: il gruppo REKT Team ha compromesso 78 profili ufficiali di partiti UK, tramite malware mobile diffuso su Play Store (fonte: BBC Tech July 2025).

- **Fabio, solar installer, Milano giugno 2025**: ha visto la sua foto di profilo trasformata in una pubblicità di trading

online. Per tre settimane ha ricevuto insulti da sconosciuti prima di riuscire a recuperare l'account.

Proteggere Instagram: Ma quanto è sicura la piattaforma? E i "foresti" riescono davvero a rubare dati dal database?

Domanda che ricevo ogni volta nei miei workshop: "Ma Instagram non dovrebbe essere invulnerabile?"

Risposta: Nessun sistema è **mai** invulnerabile. Instagram nel luglio 2025 ha concluso un audit su diversi bug frontend, come quello che consentiva di vedere gli archivi delle storie anche da account anonimi (patchata al volo). Database e comunicazioni sono cifrate, ma tra attacchi interni (insider threat) e vulnerabilità dei cloud provider, nulla è scolpito nella pietra.

Esempio: il data breach "Alessia Pop" di febbraio 2025 ha fatto trapelare info email di 150.000 account italiani (fonte: DataLeakers, marzo 2025), sfruttando una debolezza nella gestione dei permessi di terze parti.

Al tempo stesso, sapere come proteggere Instagram oggi (e anche nel 2027) passa dal conoscere proprio questi punti deboli: tenere aggiornato il sistema, cambiare password, essere sempre "paranoico quanto basta".

Un paio di trucchetti rapidi per vivere meglio su Instagram (e non solo in ottica "proteggere Instagram")

- Con i nuovi filtri AR (aggiornamento luglio 2025) puoi nascondere la posizione reale delle foto, ottimo per privacy e sicurezza.
- Usa le "Storie solo per amici stretti": se pubblici contenuti delicati, evita la platea aperta.
- Evita "follower booster" non ufficiali — rischiano di appiopparti centinaia di bot che poi Instagram ti elimina a raffica.
- Se vuoi crescere nei follower VERI, partecipa a challenge ufficiali Instagram Creators: trend di luglio 2025, hashtag #RealLifeReels.
- Le collaborazioni con micro creator nel tuo stesso settore funzionano meglio che affidarsi a tool misteriosi.
- Ricorda: pubblica "prime time" (18:00-21:00, ora italiana, dati luglio 2025).

Precedente storico: un bug bounty che ha fatto la storia

Nel maggio 2024, l'hacker etico indiano Laxman Muthiyah vinse 30.000\$ per aver segnalato un bug che consentiva di resettare password Instagram via brute force, attacco ripresentatosi con una variante a giugno 2025. Instagram ha distribuito oltre 360.000€ in bug bounty dal 2022 al luglio 2025 — e continuerà nel 2027.

Un video YouTube da non perdere (la sicurezza spiegata per smartphone lovers)

Video: [Instagram Account Hacked – What to Do NOW! (Updated July 2025)](<https://www.youtube.com/watch?v=F2Q4uVNpZ8s>)

Il canale "CyberGaranzia" spiega (da smartphone) passo dopo passo tutto il processo di recupero per chi ha subito hacking anche senza recovery email o numero. Commenti aggiornati a luglio 2025 con domande reali: "E se hanno cambiato foto profilo?" "E se mi minacciano nei DM?". Vale la pena ascoltare chi ci è passato: nelle testimonianze reali, c'è quasi sempre la soluzione che manca nei manuali ufficiali.

Proteggere Instagram: FAQ Essenziali

1. Quanto spesso devo cambiare password?

Almeno ogni 4-6 mesi. La prassi suggerita dagli esperti rimane valida per tutto il 2027. Imposta un reminder mobile.

2. Esistono davvero app Android/iOS che proteggono Instagram?

Sì, guarda Authy, Bitwarden, Lookout, CrowdFire e Sekur.me ("mobile friendly").

3. Come riconosco un messaggio truffa?

Link strani, errori grammaticali, offerte troppo belle. Se hai dubbi, cerca se altri hanno già segnalato il testo su forum come "Proteggere un Account di Instagram" su Facebook o Reddit.

4. Cosa faccio se ricevo un DM minaccioso?

Screenshot, blocca il mittente, denuncia da mobile (funzione “Segnala” presente nelle app iOS/Android), e contatta la Polizia Postale per situazioni gravi.

5. Come posso vedere quali app hanno accesso al mio Instagram?

Impostazioni → Sicurezza → App e siti web. Rimuovi quelle che non riconosci.

6. Instagram chiude profili hackerati?

Solo quelli usati per spam, ricatti o attività criminali. Se agisci in fretta puoi recuperare tutto.

Come Proteggere un Account di Instagram: Il segreto non è (solo) la tecnologia

Alla fine, cosa mi ha salvato nel mio caso personale? Un amico, una birra, e la calma di seguire tutti i passaggi senza farmi prendere dal panico. E un po' di “paranoia buona” imparata in anni nel team XP: il vero scudo sei TU, non il tool o la password.

Vi lascio con questa frase che ripeto sempre ai miei figli:

“La sicurezza online è come lavarsi le mani — non lo fai SOLO prima di mangiare, ma sempre, senza dimenticarti.”

Buona fortuna e... non smettere mai di chiederti: “Questa notifica, questa app, questa richiesta... serve davvero o può aspettare?”

Ci vediamo su Instagram (magari davvero, ma solo se protetti come si deve!).