GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

APProva di privacy

Suggerimenti per usare le app proteggendo i propri dati

I suggerimenti del Garante per tutelare la tua privacy quando usi delle app

Le **app** sono strumenti presenti ormai su numerosi dispositivi e strumenti digitali che si utilizzano quotidianamente (smartphone, tablet, pc, dispositivi indossabili, smart car, smart TV, dispositivi domotici, console per videogiochi) e offrono una vasta gamma di servizi, dalla messaggistica agli acquisti online, dalle videochiamate all'home banking, dalla formazione alla misurazione di parametri sportivi e sanitari, dalla prenotazione di viaggi e alberghi ai giochi, dalla gestione da remoto di dispositivi domotici (aspirapolvere, antifurto, illuminazione, ecc.) ai giochi, dai servizi della pubblica amministrazione alla gestione delle diete alimentari.

Sono strumenti utili, divertenti, a volte indispensabili.

Ma non sempre quando si utilizza una app ci si preoccupa anche di tutelare la propria privacy

Per proteggere i nostri dati personali e la nostra vita privata occorre quindi conoscere alcune regole fondamentali e mettere in campo adeguate cautele. Vediamo quali.

Fai attenzione a quanti e quali dati può trattare una app

Prima di installare una app, cerca di capire **quanti e quali dati** verranno **raccolti** e come verranno **utilizzati**, consultando **l'informativa** sul trattamento dei dati personali.

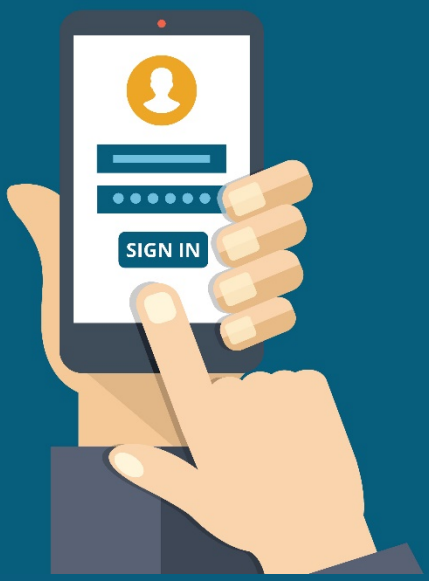
In particolare, verifica:

- **chi** tratterà i tuoi dati personali e con **quali finalità**;
- **per quanto tempo** verranno conservati i dati personali che ti riguardano;
- se i tuoi dati potranno essere **condivisi con terze parti** per finalità commerciali o di altro tipo.

Se per il **download** dell'app o per la sua installazione è prevista una **registrazione**, limitati a fornire i dati personali strettamente necessari all'attivazione del servizio.

Verifica se alcune informazioni raccolte dall'app possono **essere diffuse automaticamente** online (ad esempio, se è possibile che l'app produca post automatici sui social media) e – nel caso le impostazioni lo prevedano - valuta se disattivare questa funzionalità.

Potresti infatti **rivelare involontariamente a tutti informazioni personali**.



In generale, è bene **evitare** di memorizzare nella app i dati delle **credenziali di accesso** (username, password, PIN) di carte di credito e sistemi di pagamento. I malintenzionati sono sempre in agguato.

[VEDI ANCHE LA PAGINA TEMATICA SULLA CYBERSECURITY].

Una app può richiedere **accesso alle immagini e ai file che conservi in memoria**, ai **contatti in rubrica**, ai dati sulla **geolocalizzazione** (cioè dati che contengono informazioni sulla tua posizione in un dato momento e suoi tuoi spostamenti), al **microfono e alla fotocamera** dei tuoi dispositivi.

Valuta sempre con attenzione se consentire l'accesso a determinate informazioni e funzionalità. Se una app richiede obbligatoriamente accesso a dati e funzionalità **non** strettamente necessari rispetto ai servizi offerti, evita di installarla.

IMPORTANTE: Occorre fare particolare attenzione alle app che, grazie all'impiego dell'**intelligenza artificiale**, consentono di modificare foto e video (ad esempio, per invecchiare i volti), inserire la propria faccia sui corpi altrui (ad esempio, di personaggi famosi) oppure trasformare il genere sessuale (da uomo a donna e viceversa). Le immagini e le informazioni raccolte in questo modo potrebbero essere utilizzate anche da malintenzionati per fini dannosi per la dignità e la reputazione delle persone, come avviene nel fenomeno del deepfake (creazione di foto e video falsi a partire da immagini vere).

In ogni caso:

- ❑ se la app chiede accesso alla fotocamera o all'archivio di immagini del tuo smartphone, pc o tablet, verifica che siano spiegati in modo chiaro dal fornitore della app tutti i possibili utilizzi delle tue immagini;
- ❑ ricorda che dai volti si può risalire a informazioni di natura sensibile come i dati biometrici, che potrebbero anche essere utilizzati da malintenzionati per finalità illecite (basti pensare ai dati biometrici del volto, già oggi utilizzati, ad esempio, come *password* per l'accesso agli smartphone) o ceduti a terzi per finalità ignote.

Alcuni spunti di riflesssione

Molte app, tra cui quelle social, possono individuare e condividere con terzi la tua posizione e i tuoi spostamenti nel tempo, ad esempio utilizzando alcune funzioni del tuo *smartphone*.
Se preferisci mantenere riservate queste informazioni, puoi disattivare la raccolta dei dati di posizione da parte delle singole app, modificando le impostazioni del tuo dispositivo relative ai servizi di geolocalizzazione.

Se utilizzi una app che prevede funzioni per la condivisione di foto e video sui social o tramite messaggistica, accertati sempre che le persone riprese siano d'accordo a diffondere online la propria immagine ed eventuali informazioni sulla loro vita privata.

[VEDI ANCHE la scheda **Consigli Flash per tutelare la tua privacy se metti immagini online**]

Alcuni spunti di riflesssione

Se usi una *app* per il dating (appuntamenti online), ricorda di informarti su come verranno trattate e conservate le informazioni che ti riguardano, e a chi verranno eventualmente resi noti aspetti della tua vita privata che potresti voler mantenere riservati.

Le app che misurano le tue prestazioni sportive o monitorano e registrano il tuo stato fisico (esempio: battito cardiaco, pressione, ecc.) sono in grado di raccogliere dati sensibili che potrebbero essere trasmessi a terzi per finalità non sempre conosciute.

Verifica quindi sempre quali informazioni possono essere rilevate e trattate dalla app, stabilisci tu con chi condividerle (ad esempio, scegliendo nelle impostazioni di renderle visibili a tutti, solo agli “amici” o a nessuno) e decidi eventualmente di disattivare la rilevazione e il trattamento dei dati non indispensabili per il servizio (ad esempio, si può scegliere di monitorare la durata e la distanza percorsa correndo o andando in bicicletta anche senza rilevare il battito cardiaco).

Ricorda che insieme alle app potresti scaricare inavvertitamente virus e malware pericolosi per la tua privacy

Per evitare rischi:

- installa sul dispositivo che ospita le app anche un software **anti-virus** in grado di proteggere i dati personali da eventuali violazioni;
- imposta **password** di accesso sicure e aggiornale periodicamente;
- **aggiorna periodicamente la app**: le nuove versioni contengono di solito anche miglioramenti sul fronte della sicurezza informatica;
- **non disattivare mai i controlli di sicurezza previsti dal tuo dispositivo**, se non sei assolutamente consapevole di ciò che stai facendo;
- **fai sempre attenzione alla provenienza delle app**. In particolare:

  - ❑ evita di scaricare app tramite siti web che non ti sembrano affidabili o cliccando link che ti vengono inviati tramite SMS o messaggistica. In generale, è meglio scaricare le app dai **market ufficiali**, che garantiscono la presenza di controlli da parte dei gestori del market sull'affidabilità dei prodotti e permettono di consultare le eventuali recensioni di altri utenti (sull'uso di una determinata app, sugli sviluppatori o sul market stesso) per verificare se sono, ad esempio, segnalati problemi riguardanti la sicurezza dei dati. Se il market prevede la creazione di un account, ricorda di informarti sempre su come tratterà i dati richiesti per la sua attivazione;
  - ❑ leggi con attenzione le **descrizioni delle app** che intendi installare (se, ad esempio, nei testi sono presenti errori e imprecisioni, c'è da sospettare).

Pensa ai rischi che possono correre i minori

Meglio evitare che i **minori** possano scaricare e utilizzare app da soli. I più giovani, infatti, sono meno consapevoli dei pericoli e più esposti al rischio di una raccolta e diffusione incontrollata di dati personali propri o dei familiari.

Inoltre, potrebbero diventare oggetto di attenzione di **malintenzionati** che cercano di contattarli, oppure **fare involontariamente acquisti online o diffondere inconsapevolmente dati sensibili o informazioni sul conto bancario o la carta di credito dei genitori**.

Se i minori utilizzano dispositivi quali PC, tablet, smartphone, smart TV, console per videogiochi, servizi di streaming online, usati anche da altri familiari, si può decidere di creare un **profilo con impostazioni d'uso limitate**, in modo che alcune delle app installate o alcuni contenuti non siano accessibili ai minori.

Per informazioni e tutela

Nei casi in cui ci siano dubbi sull'effettivo rispetto delle norme o sul corretto uso dei propri dati personali, ci si può rivolgere al Garante per la protezione dei dati personali.

www.garanteprivacy.it