Privacy e sicurezza su dispositivi mobili

20 Febbraio 2018

Ormai praticamente chiunque possiede uno smartphone o un tablet, senza differenze legate alla fascia d'età, all'interesse per la tecnologia o all'effettiva necessità di funzionalità avanzate. Di fatto nei nostri dispositivi mobili riponiamo una quantità enorme di informazioni più o meno private, tra cui spesso dati sensibili che, se fossero utilizzati da malintenzionati, potrebbero arrecarci danni considerevoli, sia economici che d'immagine. D'altra parte è anche vero che le stesse informazioni ci sono spesso utili per gestire meglio la nostra giornata oppure per ridurre il tempo dedicato alla ricerca di un articolo che vorremmo acquistare, o ancora per organizzare un viaggio in pochi, semplici passi.

Come possiamo dunque bilanciare i benefici e i rischi che derivano dalla raccolta dati effettuata automaticamente dal nostro smartphone? Ci sono differenze legate alla sicurezza tra i vari modelli in commercio? In questo articolo cercheremo di chiarire questi dubbi e di capire come proteggere la nostra privacy, pur mantenendo attive alcune funzionalità utili.

Android e iOS: ci sono differenze?

Android (sviluppato da Google) e iOS (sviluppato da Apple) sono i due sistemi operativi più diffusi sul mercato. Su di essi si basa insomma l'intero funzionamento della stragrande maggioranza degli smartphone e dei tablet attualmente in commercio, che spesso vengono scelti dagli utenti unicamente per una preferenza estetica o per il marchio, senza una vera consapevolezza delle differenze che li contraddistinguono. In realtà, anche dal punto di vista della privacy i due sistemi operativi presentano alcune differenze:

– **Google** tende a raccogliere un maggiore numero di informazioni sull'utente, tenendo traccia non solo della sua posizione, dei luoghi che frequenta, dei percorsi che compie ogni giorno (per esempio da casa a lavoro), ma anche delle ricerche effettuate online sui motori di ricerca, delle applicazioni che si scaricano e del loro utilizzo.

– **Apple** tende ad essere leggermente meno invasivo, limitando il numero di informazioni personali raccolte e cercando di raccogliere dati sugli utenti senza crearne profili particolarmente precisi. Per esempio, molti dettagli personali registrati da Siri (il sistema di comando vocale presente ormai su tutti gli iPhone e iPad) sono salvati unicamente nella memoria del dispositivo, ma non vengono inviati ai server di Apple.

Va detto che la maggior parte di queste impostazioni possono essere modificate da ogni utente, che però deve decidere consapevolmente a quali servizi eventualmente rinunciare per aumentare il livello della propria privacy. Inoltre, come vedremo in seguito, ogni singola applicazione può possedere o meno i permessi per accedere a particolari informazioni salvate sul nostro dispositivo, indipendentemente dalle impostazioni generali del sistema operativo.

Gli usi positivi dei nostri dati

Non tutte queste funzioni, che molti considerano estremamente invasive, sono effettivamente di poca utilità per l'utente. Alcuni benefici sono sicuramente secondari,

come per esempio la visualizzazione di annunci pubblicitari non casuali, ma basati sui propri gusti personali e sulle ricerche effettuate in precedenza. Altri, invece, possono essere decisamente importanti per mantenere il proprio dispositivo in uno stato ottimale e, paradossalmente, fondamentali per la nostra sicurezza. L'invio di dati agli sviluppatori, infatti, permette un costante monitoraggio di bug e difetti nelle applicazioni che utilizziamo, permettendo una rapida risoluzione di eventuali problemi e un migliore livello di protezione da potenziali intrusioni. Inoltre, in caso di smarrimento del proprio smartphone, solo grazie alla geolocalizzazione sarà possibile ritrovarlo facilmente e bloccarlo, così da evitarne un uso improprio da parte di terzi. Infine, consideriamo anche che gran parte delle applicazioni per la sicurezza si basa sempre su queste tecnologie, che permettono a un amico o un familiare di assisterci tempestivamente in caso di incidenti o molestie.

Nel momento in cui si volessero modificare le impostazioni sulla privacy, dunque, bisognerebbe considerare attentamente le funzionalità a cui si è disposti a rinunciare pur di bloccare il monitoraggio attivo di Google o Apple.

Come proteggersi da attacchi esterni?

Nonostante sia praticamente impossibile ridurre a zero tutte le intrusioni esterne (se a voler controllare i nostri dati sono agenzie governative o colossi come Google, infatti, non possiamo fare molto per impedirlo), è comunque consigliabile adottare alcune misure abbastanza semplici, che assicurano una discreta protezione dagli hacker che potrebbero utilizzare i nostri dati per causare danni di varia natura. Vediamole qui di seguito.

1. **Mantenere il proprio dispositivo aggiornato**: avere uno smartphone o un tablet di ultima generazione, aggiornabile all'ultima versione disponibile del sistema operativo in uso, non è solo una questione di immagine o un capriccio inutile. Si tratta infatti di una delle più importanti discriminanti che rendono il nostro dispositivo più o meno vulnerabile: più datato è il sistema operativo, più facile sarà

per un hacker eluderne la sicurezza e avere accesso ai nostri dati personali. Con ogni aggiornamento, infatti, gli sviluppatori correggono bug ed errori che possono essere utilizzati da terzi per eludere i sistemi di sicurezza del sistema stesso.

2. **Bloccare il proprio dispositivo**: può sembrare una banalità, ma molti utenti ancora non impostano un sistema che blocchi lo smartphone o il tablet quando lo schermo viene disattivato. Esistono ormai svariati sistemi di blocco, tra cui un codice numerico (PIN), una sequenza disegnata tra una griglia formata da vari punti, oppure il riconoscimento dell'impronta digitale, ormai sempre più diffuso anche tra i dispositivi di fascia media. Si tratta di un'azione semplicissima che può se non altro ritardare l'attacco di terzi alle nostre informazioni private.
3. **Controllare i permessi concessi alle applicazioni installate (anche quelle più vecchie)**: come abbiamo accennato sopra, non è solo il sistema operativo a raccogliere dati sulle nostre abitudini, ma anche le singole applicazioni che abbiamo installato e utilizziamo più o meno di frequente. Nelle impostazioni è possibile scegliere quali permessi concedere (spesso ci viene richiesto al momento dell'installazione se vogliamo consentire all'applicazione l'accesso alla rubrica, alle nostre foto o al servizio di geolocalizzazione), e se chiudere un'applicazione ogni volta che blocchiamo lo schermo, evitando che continui ad operare in remoto. Ricordiamo inoltre che è importante controllare sempre la provenienza dell'applicazione, possibilmente facendo una breve ricerca sugli sviluppatori, ed evitare di utilizzare Store "alternativi", dove è molto più facile per i malintenzionati approfittare delle vulnerabilità dei nostri dispositivi.
4. **Utilizzare un'applicazione per gestire le password**: dette anche "password manager", queste applicazioni consentono di salvare le nostre password, evitando così di doverne ricordare dozzine ogni volta che ci colleghiamo ai nostri canali social o a siti web a cui siamo iscritti, ma proteggendole con una password generale. Questa ci verrà richiesta ad ogni accesso, ma rimarrà sempre la stessa (almeno finché non vorremo modificarla), garantendo un maggiore livello di protezione e riducendo al minimo i disagi per l'utente.
5. **Attenzione a spam e allegati**: anche su un dispositivo mobile, spam, link poco affidabili e allegati pericolosi rappresentano una minaccia molto importante per la nostra privacy. Bisogna prestare estrema attenzione a ogni messaggio che si decide di aprire, e valutare se effettivamente gli allegati o i link inclusi sono sicuri o meno. Quando si fosse in dubbio, suggeriamo semplicemente di eliminare il messaggio ed evitare qualunque interazione con il suo contenuto, che potrebbe contenere virus in grado non solo di rubare tutti i nostri dati, ma anche di rendere il dispositivo completamente inutilizzabile.

Vuoi dire la tua sul tema della privacy online? Sei un'azienda del settore e vuoi commentare questo articolo? Lascia il tuo parere nella parte destinata ai commenti o sulla pagina Facebook UNConsumatori. La tua opinione per noi è importante!

HAI BISOGNO DEL NOSTRO AIUTO? SCRIVI ALLO SPORTELLO GENERICO.

Questa rubrica è stata realizzata in collaborazione con QualeScegliere.it, piattaforma online che mette a disposizione una serie di strumenti utili e pratici da consultare per aiutare gli utenti nella scelta di oltre 250 categorie di prodotti.

Autore: Simona Volpe in collaborazione con Qualescegliere
Data: 19 febbraio 2018