Fatti smart! Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet

VADEMECUM
Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet

Non ci pensiamo quasi mai, forse. Smartphone e tablet ci accompagnano ovunque e custodiscono parti importanti e spesso delicate delle nostre vite, sotto forma di foto, filmati, messaggi e dati telematici. E noi stiamo sempre attenti a proteggere adeguatamente queste informazioni con piccole ma utili precauzioni?

In un video-tutorial il Garante per la protezione dei dati personali offre alcune utili indicazioni per tutelare la nostra privacy quando utilizziamo smartphone e tablet.

Attenzione ai dati conservati su smartphone e tablet

Non conservare su smartphone e tablet informazioni troppo personali che potrebbero essere smarrite o rubate, o perfino clonate o attaccate da pirati elettronici. Non si dovrebbero mai conservare, ad esempio, password personali, codici di accesso e dati bancari in chiaro.

Ricorda, poi, che smartphone e tablet venduti, regalati o buttati possono contenere ancora dati privati. Se te ne liberi, quindi, **cerca di adottare alcune piccole precauzioni di sicurezza** come:

- ripristinare le impostazioni di fabbrica

rimuovere la scheda SIM e la scheda di memoria

eliminare tutti i backup contenuti nella memoria.

Proteggi i tuoi dati

Se vuoi evitare che qualcuno legga di nascosto le tue e-mail e i tuoi sms o che usi a tua insaputa il tuo smartphone o il tuo tablet, usa alcune precauzioni.

Imposta sempre un codice PIN abbastanza complicato, evitando, ad esempio, di usare il tuo nome e cognome, la data di nascita, il nome dei figli o quello del gatto di casa, o comunque altre parole che ti renderebbero in qualche modo riconoscibile.

Magari imposta anche un **codice di blocco**, quello che si attiva automaticamente quando il cellulare è acceso ma non viene utilizzato per un pò di tempo. E anche in questo caso, evita codici un po' troppo facili da scoprire.

Alcuni sistemi operativi consentono anche di impostare password di sicurezza che bloccano completamente l'accesso ai dati personali. Per farlo, basta collegare smartphone e tablet con il pc e utilizzare il software per la gestione del prodotto.

Conserva con cura il codice IMEI, che trovi sulla scatola del prodotto che acquisti e che in caso di furto o smarrimento puoi utilizzare per bloccare a distanza l'accesso al tuo smartphone o tablet.

Quando navighi su smarthone e tablet

Se ti connetti a Internet e ai social network via smartphone e tablet, **verifica le impostazioni privacy e leggi le condizioni d'uso dei servizi**.

Per navigare sul web, inoltre, **installa sempre - se disponibile - software di sicurezza anti-virus informatici o contro le intrusioni da parte di pirati telematici e ladri d'identità digitali**.

Quando usi connessioni wi-fi gratuite, ad esempio nei locali pubblici, **verifica che la navigazione sia protetta con protocolli di scambio dati criptati** e che l'autenticazione ai siti che eventualmente vengono visitati utilizzi il **protocollo Https**. In caso contrario, se si utilizzano credenziali di accesso a siti e servizi come la posta elettronica o l'home banking, il rischio che non ci siano adeguate garanzie di sicurezza per i propri dati è reale.

APP-rova di privacy

Se scarichi delle applicazioni, **evita le fonti sconosciute e utilizza sempre i market ufficiali**, a meno che tu non sia in grado di valutare autonomamente l'affidabilità della fonte - ad esempio leggendo i commenti eventualmente lasciati dagli altri utenti - per comprendere se ci sono eventuali rischi o problematiche.

Una volta installata un'applicazione, verifica se richiede **l'accesso a contenuti presenti sul tuo smartphone o sul tuo tablet** (ad esempio, le tuo foto o i contatti in rubrica) e leggi con attenzione le **condizioni d'uso del servizio**, soprattutto per evitare di dover pagare servizi non richiesti o di vedere esposte oltremisura informazioni di carattere personale (ad esempio: foto, video, contatti, ecc.).

Occhio allo spam

Smartphone e tablet sono terreno di caccia per lo spam.

Attenzione ai link presenti in e-mail, sms e messaggistica istantanea, perché, in alcuni casi, cliccandoli, potresti inconsapevolmente accettare di ricevere comunicazioni indesiderate, divenendo bersaglio di messaggi pubblicitari non richiesti da cui, poi, può anche essere abbastanza difficile liberarsi.

Vuoi sempre far sapere dove sei?

Smartphone e tablet hanno **funzioni di geolocalizzazione**, ma sei tu a decidere se, quando e chi può conoscere la tua posizione.

Per **disabilitare la geolocalizzazione**, puoi disattivare - controllando le impostazioni dello smartphone o tablet - il GPS o la connessione wi-fi quando non usi questi servizi o altri ad essi collegati.

E' bene, inoltre, controllare anche le **impostazioni di geolocalizzazione dei servizi di social network** che eventualmente utilizzi su smartphone o tablet. La scelta finale di far sapere o meno dove sei, in fin dei conti, è sempre la tua.

Per approfondimenti su smartphone e protezione dei dati, vedi anche:
www.gpdp.it/temi/smartphone/microfoni