Grande fratello smartphone

Gps, wi-fi e apps: così ci spiano i supercellulari. La privacy violata? Un business

Tenere in tasca un apparecchio sempre collegato alla Rete ha un prezzo che non è solo quello indicato nei negozi. Il costo meno evidente, ma forse più oneroso per chi utilizza uno smartphone, è la continua cessione, più o meno inconsapevole, delle proprie informazioni personali ad aziende interessate a sapere tutto di tutti per poi vendere meglio i loro prodotti. Aziende che hanno trovato nei telefonini di nuova generazione preziosissime miniere di informazioni personali di utenti che, magari con poca cautela, regalano a chiunque piccole o grandi fette della loro vita.

Con in tasca un telefonino sempre connesso, ha ricordato pochi giorni fa anche il garante per la Privacy, Francesco Pizzetti, siamo come tanti piccoli "Pollicino" che disseminano tracce di sé un po' ovunque. Certo, anche quando si accede a Internet con un Pc comunichiamo informazioni più o meno sensibili, ma gli smartphone sono un'altra cosa. Prima di tutto perché usano sistemi di geolocalizzazione Gps che prelevano dati precisi sulla nostra posizione geografica nel momento in cui accediamo a un servizio. Non solo. Mentre su un computer dopo la navigazione è possibile cancellare i cookies, ovvero le tracce di siti o pagine visitate, su uno smartphone tutto resta registrato sul telefono e inizia a viaggiare nell'etere. Fuori dal nostro controllo.

Qualche esempio: Apple ha confermato che gli iPhone mantengono un database degli hotspot wifi e delle antenne della telefonia mobile disponibili in prossimità del dispositivo. In teoria si tratta di informazioni, come hanno spiegano i tecnici della società, che vengono sfruttate per ridurre il tempo necessario a localizzare l'utente da qualche minuto ad una manciata di secondi. Succede la stessa cosa nei dispositivi Android, dove alla prima accensione, il sistema operativo chiede il permesso di tracciare la posizione dell'utente usando reti wifi e telefoniche. Se si acconsente, una finestra di dialogo spiega che «il servizio di geolocalizzazione di Google utilizzerà, in forma anonima, alcuni dati raccolti dal proprio dispositivo mobile».

Più subdole sono le insidie per la privacy che arrivano dalle applicazioni. Le apps sono programmi che vengono scaricati sul telefono e quasi sempre forniscono servizi via web, il cui utilizzo implica quindi che i dati personali siano spostati o copiati nel cloud, cioè nei data center del fornitore del servizio. Spesso l'utente non è neppure consapevole del fatto che sta utilizzando un servizio cloud, anche se poi dà per scontata la possibilità di accedere agli stessi dati da più dispositivi senza bisogno di trasferirli manualmente ogni volta. Un'indagine del Wall Street Journal ha rivelato che la metà delle applicazioni forniscono dati personali a società terze, in alcuni casi senza nemmeno dare agli utenti la possibilità di acconsentire o meno al loro invio. I destinatari dei dati sensibili sono quasi sempre aziende che effettuano ricerche di mercato e che, una volta raccolti i dati e divisi i flussi in aree specifiche, sono in grado di fornire ai pubblicitari delle coordinate sociali precise per veicolare i propri messaggi.

Per esempio con la sua app Facebook preleva (e si tiene per sé) le informazioni sul luogo da cui lo stiamo usando. Lo stesso fa anche Google maps, che però quelle informazioni (anonime) le vende anche ad altri. Idem l'app del New York Times. Entrambi inviano a terze parti anche il codice unico di identificazione del telefono. Un numero che in sé non rivela nulla, ma che incrociato con altri dati come acquisti online, connessioni sui social network e posizioni geografiche può fornire un quadro preciso di un utente. Questo codice - che identifica anche in modo univo il dispositivo (marchio e modello) che stiamo utilizzando - viene prelevato anche da Groupon, il social network dello shopping che lo invia a società che si occupano di predisporre campagne pubblicitarie. Generalmente molto indiscreti anche i videogiochi: il famoso Angry birds invia a terze parti dati sensibili come contatti, città in cui ci troviamo e codice del telefono.

Sotto l'instancabile assedio degli spioni, il proprietario dello smartphone non sempre ha la possibilità (e a volte nemmeno la volontà) di difendere i "fatti suoi". Ma gli conviene almeno essere consapevole di quello che gli altri possono sapere di lui.

Claudia La Via

consigli

In linea sicuri

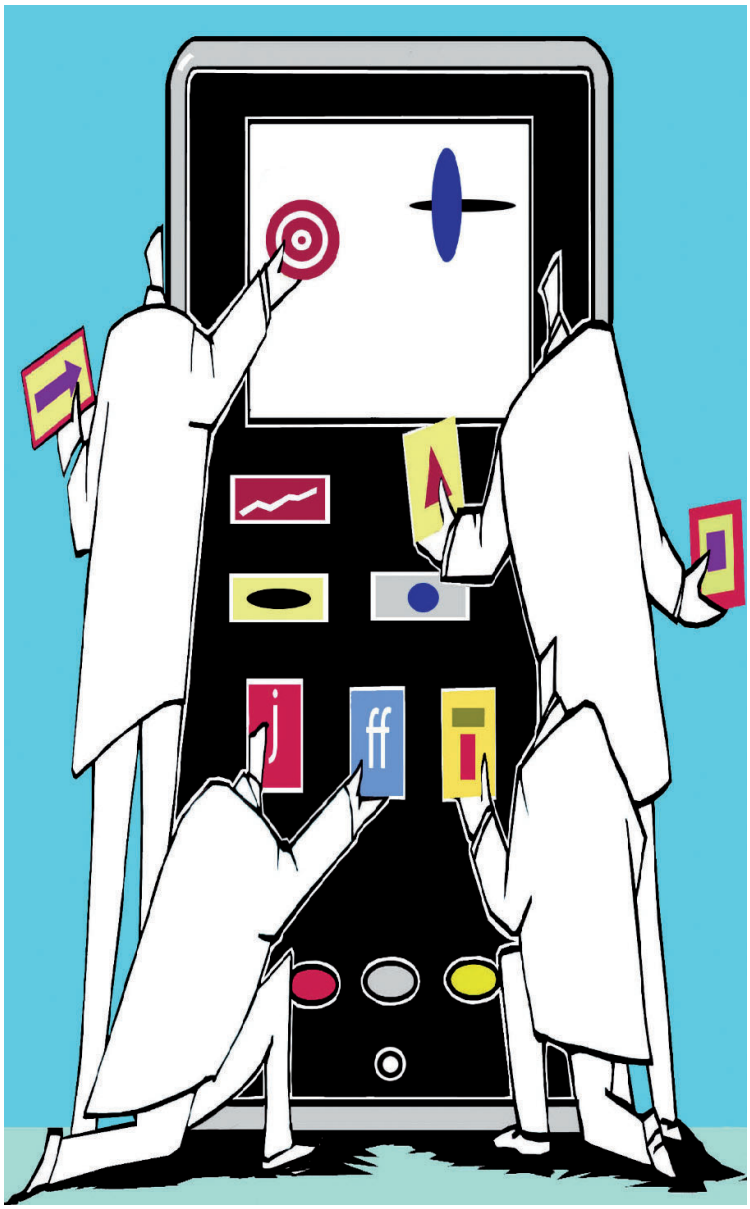
1. Creare sempre password uniche e non utilizzare mai la stessa per accedere a diversi account. Fare in modo che sia abbastanza sicura (utilizzare lettere e numeri) e cambiarla frequentemente.

2. Verificare l'attendibilità di un'applicazione prima di scaricarla e leggere i commenti di altri utenti e le politiche di privacy se presenti.

3. Fare attenzione a cliccare su link esterni che compaiono su e-mail, sms o siti di social network.

4. Disattivare il sistema di geolocalizzazione del telefono se non si vogliono utilizzare le mappe.

5. Accedere al proprio account o utilizzare la propria carta di credito solo su siti che consentono la navigazione sicura: l'indirizzo inizia per https://.



Immagini, video, amicizie e passioni: la Rete cattura pezzi della nostra vita Come difendersi con pochi e semplici passi

Chi naviga lo sa: la Rete sa dirci tutto, o quasi, su una persona che ci interessa. Basta digitare un nome sul motore di ricerca e in pochi secondi sullo schermo compaiono tutte le informazioni che Internet ha già immagazzinato. È sufficiente cercare sui siti giusti, mettere insieme un po' i pezzi del puzzle e in poco tempo riusciamo a farci un'idea di come è e cosa fa. Stessa cosa vale per noi. Mail, social network, foto: sono tanti i dati personali che immettiamo quotidianamente sul web e che diventano accessibili agli altri utenti. Nella maggior parte dei casi si tratta di informazioni che scegliamo volontariamente di consegnare nel momento in cui aderiamo a un servizio. Ma non sempre siamo consapevoli delle conseguenze di questa scelta e sappiamo fissare dei limiti al "pubblico" delle nostre informazioni.

In pochi si ricordano che ogni dato una volta immesso sul web smette di appartenerci e diventa a disposizione di tutti. Da quel momento in poi non siamo più in grado di modificarlo o eliminarlo del tutto, perché in Rete ne resterà comunque traccia, nostro malgrado. Basta una foto "taggata" su Facebook, una citazione in un blog o in un articolo per rilevare dettagli su di noi al mondo. Per questo bisogna imparare a utilizzare tutti gli strumenti in nostro possesso per controllare i dati che immettiamo. A partire da social network come Facebook che consentono di impostare il livello di privacy del proprio account per far sì che le nostre informazioni personali non siano visibili a utenti sconosciuti. In pochi lo sanno, e sono ancora meno quelli che lo mettono in pratica.

Attenzione a pubblicare senza pensarci foto personali su Facebook che non vorremmo condividere con altri. Stessa cosa vale per Youtube dove è possibile inserire video amatoriali: anche lì basterebbero pochi accorgimenti (ad esempio renderli disponibili solo a utenti che abbiamo invitato personalmente) per evitare che il video di nostro figlio faccia il giro della Rete senza il nostro consenso.

Il problema della privacy ormai è diventato una priorità, tanto che un'azienda "spiona" per definizione, come Google, ha da poco lanciato un nuovo servizio. Si chiama «Me on the web» (Io sul web) e ci avvisa via email ogni volta che veniamo nominati nella Rete. Per rendersi conto, almeno, di quello che in giro sanno di noi.

Claudia La Via