Sarahah, difendiamo i nostri dati personali

Autore: Daniela Baudino
Fonte: Città Nuova

Installando una semplice app, tipo WhatsApp, sul cellulare diamo implicitamente il consenso ad accedere a tutte le nostre informazioni e molto altro. Le cautele possibili

Quando qualche giorno fa, parlando di Sarahah, la nuova app che consente di invitare messaggi anonimi, abbiamo espresso qualche perplessità in merito al trattamento dei dati personali. Dopo qualche indagine è stato scoperto che l'app **invia ai propri server i contatti memorizzati nella rubrica del telefono su cui l'app è installata**. Centinaia di numeri di telefono ed email che vengono caricati continuamente su un server esterno. Chiamato in causa, il fondatore di Sarahah si è difeso dicendo che questo caricamento di dati serve solo per poter integrare la funzionalità che permette di trovare più velocemente quegli amici che già utilizzano la app. Il "problema" è che, però, questa funzione non è mai stata implementata e, soprattutto, **non è stato comunicato come questi dati vengano trattati ed utilizzati una volta caricati sul server**. Lo sviluppatore di Sarahah ha comunque subito annunciato marcia indietro e assicurato che «la richiesta di accesso ai dati sarà eliminata col prossimo aggiornamento» e che i server di Sarahah «non ospitano al momento contatti». E allora, dove sono finiti i dati degli utenti che hanno già consentito l'accesso? Non è dato a sapere, è questa non è una cosa bella. Questo fatto ci dà, allora, occasione di riflettere sul fatto che in realtà, come spesso accade quando installiamo una app, anche in questo caso **l'autorizzazione ad accedere alla nostra rubrica l'abbiamo data noi, anche se in maniera inconsapevole**. Sarahah non è la prima app che raccoglie e immagazzina informazioni sulla rubrica dell'utente che la utilizza. Facebook, Twitter, Instagram, Snapchat, tutte le app più famose accedono (**con il nostro tacito consenso**) ai dati dei nostri contatti per poterci suggerire più facilmente persone conosciute da aggiungere alle nostre liste. Quello che manca, in questo caso specifico, sono informazioni che indichino lo scopo della raccolta dati e i sistemi messi in atto per tutelare la privacy di chi decide di condividerli. **Raccogliere dati sui contatti: una pratica comune** Succede molto spesso, quando installiamo una app sul nostro smartphone, di non soffermarci a leggere a quali funzionalità la app potrà accedere, attraverso il consenso che diamo dando implicitamente con l'installazione. Così di fatto c**oncediamo l'uso di molti nostri dati (e non solo nostri) senza esserne troppo consapevoli**. **Come le app usano le autorizzazioni sulle funzionalità** Ogni smartphone gestisce le impostazioni in maniera diversa, ma per sapere quali autorizzazioni abbiamo dato alle diverse app che abbiamo installato sul nostro smartphone possiamo, in linea generale, andare su IMPOSTAZIONI, cercare la voce APP(LICAZIONI) e cliccando su ogni applicazione cercare all'interno della scheda la voce delle autorizzazioni o un ulteriore scheda apposita. Prendendo ad esempio l'app che la maggioranza di chi noi sicuramente utilizza, **WhatsApp**, possiamo scoprire che l'abbiamo autorizzata ad accedere al nostro calendario, ai contatti, alla fotocamera, alla memoria, al microfono, alla posizione, agli sms, al telefono e ad altre funzionalità marginali, come il bluetooth, la vibrazione, il controllo audio, accesso alla rete, etc. In alcuni modelli di smartphone è possibile leggere, per ogni singola autorizzazione, cosa significa in concreto ciò che abbiamo autorizzato. Così è possibile scoprire che l'autorizzazione all'uso del microfono significa consentire a WhatsApp di "*registrare audio con il microfono. Questa autorizzazione consente all'applicazione di **registrare audio in qualsiasi momento senza la tua conferma***". Cioè, WhatsApp non registra audio soltanto quando registriamo una nota vocale, ma potenzialmente **è come se avesse un registratore sempre accesso**. Certo, spesso installare una determinata app diventa quasi necessario, dovendo di fatto scendere a patti. Ma è importante farlo essendo consapevoli di cosa stiamo concedendo a livello di dati personali, per poter prendere delle adeguate contromisure (ad esempio non parlare con lo smartphone acceso nelle vicinanze). **Come gestire le autorizzazioni alle app** Uno dei consigli che

gli esperti di sicurezza danno è quello di non concedere l'accesso alla propria rubrica quando a chiederlo sono app che non hanno dietro grandi organizzazioni e che potrebbero quindi avere preso meno precauzioni per tutelare il trasferimento dei dati. Come nel caso di Sarahah, dove non sono state rese pubbliche informazioni chiare né sulle modalità di trasferimento dei dati né sui livelli di sicurezza dei server che gestiscono le informazioni. Questo perché è già successo in passato che grandi database, contenenti milioni di numeri di telefono ed email, siano poi stati resi pubblici o messi in vendita su forum di hacker e di altri utenti poco raccomandabili. Abbiamo il diritto di sapere come verranno trattati i nostri dati! Quindi due i consigli che possiamo imparare dal "**caso Sarahah**": innanzitutto non installare app che non spiegano in modo chiaro come verranno utilizzati i dati a cui hanno accesso. E, se il nostro smartphone lo permette, **revocare quelle autorizzazioni che ci sembrano più invadenti**.