

Facebook, i dati di 533 milioni di profili pubblicati online

Coinvolti anche 35 milioni di italiani: in Rete, gratuitamente, ci sono numeri di telefono e in alcuni casi nome e cognome, data di nascita e indirizzo di posta elettronica. I consigli dell'esperto

I numeri di telefono e in alcuni casi nome e cognome, data di nascita e indirizzo di posta elettronica di circa 35 milioni di italiani iscritti a Facebook stanno circolando in Rete, gratuitamente, dopo essere stati pubblicati su un sito per hacker. Questi dati fanno parte di un più corposo database di 533 milioni di profili di più di cento Paesi: l'Italia è fra i più colpiti, con un numero di persone coinvolte che corrisponde alla quasi totalità degli utenti del social network (negli Stati Uniti sono 32 milioni e nel Regno Unito 11).

A riportare la notizia, sabato scorso, l'esperto di sicurezza Alon Gal e il sito Business Insider. Altri esperti contattati dal Corriere hanno confermato la veridicità dei dati che sono riusciti a consultare e che risalirebbero al 2019.

Perché se parla adesso? Anzi, perché se ne riparla: un furto con le stesse caratteristiche è noto almeno dallo scorso gennaio, quando sull'app di messaggistica Telegram era possibile interrogare un bot per ottenere a pagamento il numero di telefono di un utente Facebook di cui si conosceva il codice identificativo (Facebook ID) e viceversa.

Dopo le nuove rivelazioni, è stato il colosso di Menlo Park stesso a dichiarare che si tratta «di dati e di un problema individuato e risolto nel 2019»: una vulnerabilità che permetteva a chiunque fosse in grado di realizzare un software ad hoc di setacciare il social network (scraping è il termine tecnico) alla ricerca dei numeri degli iscritti, che possono essere stati inseriti in fase di iscrizione o per questioni di sicurezza.

La novità, adesso, è che il database è disponibile gratis ed è «accessibile a chiunque abbia conoscenze tecniche di base. Non è un problema da poco ed è la conferma della quantità di informazioni in possesso di queste piattaforme e di quanto è difficile tenerle sotto controllo» spiega l'esperto di cybersicurezza Riccardo Meggiato. Il rischio maggiore, prosegue, è quello legato all'incrocio dei diversi database a disposizione dei malintenzionati: «Prendiamo l'Italia, dove negli ultimi mesi è stato colpito l'operatore Ho.mobile: combinando i dati, a quelli rubati a Facebook si può aggiungere anche l'indirizzo di casa».

Non è il caso di farsi prendere dal panico, ma è giusto essere consapevoli dell'accaduto e adottare piccole ma sostanziali accortezze. Sul sito haveibeenpwned.com si può verificare se la propria mail si trova nel database (e anche se le password al momento non c'entrano, cambiarla è auspicabile). Meggiato consiglia, se possibile, di non usare più il numero di telefono associato a Facebook per le verifiche in due fattori (quando ci facciamo mandare un Sms per cambiare la password), su quello e altri portali, perché persone in possesso di più informazioni sulla nostra identità potrebbero tentare di clonarlo. Stesso discorso per il phishing: chi sa qualcosa di noi o sfrutta la data di nascita per colpire gli anziani con meno dimestichezza con la Rete, può provare a orchestrare truffe convincenti e farci o farli cliccare su link malevoli con riferimenti a interessi o date o luoghi noti alla vittima. Attenzione, dunque.

Anche se la vulnerabilità era precedente all'entrata in vigore del regolamento europeo per la protezione dei dati personali Gdpr, nel 2019 Facebook aveva contattato il Garante irlandese per la privacy, che adesso sta verificando se i dati sono effettivamente gli stessi di due anni fa. Fonti interne del Garante italiano dicono che l'Autorità è al lavoro per limitare i rischi.

Martina Pennisi

Corriere della Sera

6 Aprile 2021