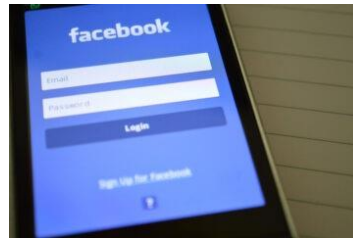


Facebook, in Rete i dati di milioni di utenti: cosa fare

6 Aprile 2021 | Autore: [Carlos Arija Garcia](#)



Nomi, indirizzi e-mail, numero di telefono rubati: tutto gratis in un database a disposizione di chi ci sa fare. I consigli degli esperti per difendersi.

Nome, cognome, data di nascita. Perfino il numero di telefono o l'indirizzo di posta elettronica. Tutto finito in Rete, in chiaro e gratis. Tutto convogliato in un sito per hacker. Ecco la fine che hanno fatto i dati personali di circa 35 milioni di italiani iscritti a Facebook, secondo quanto riporta il sito del *Corriere della Sera*. Il danno non è stato fatto, però, solo in Italia, che resta uno dei Paesi più colpiti: in tutto il mondo, gli utenti interessati sono 533 milioni, residenti in più di 100 Stati. Negli Usa, i cittadini coinvolti sono 32 milioni, circa 11 milioni nel Regno Unito.

Il fatto sconvolgente è che questa storia va avanti da due anni, dal 2019, secondo alcuni esperti di sicurezza informatici che hanno confermato la notizia. Come spiega il *Corriere*, un furto simile di dati 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.

Il problema è che se una volta era possibile ottenere questi dati a pagamento, ora il database con milioni e milioni di informazioni circa gli utenti del social network più famoso al mondo è diventato gratuito. Chiunque vi può accedere o, almeno, chiunque sia un po' pratico a muoversi in Rete con una certa dimestichezza a caccia di dati altrui. Il guaio non è tanto che qualcuno veda nome, cognome o indirizzo e-mail di un utente quanto l'uso che ne può fare. Come spiega al *Corriere* un esperto di cybersicurezza, qualche mese fa è stato colpito dagli hacker l'operatore Ho.mobile. Combinando i suoi dati, a quelli rubati a Facebook si può aggiungere anche l'indirizzo di casa.

Cosa si può fare a questo punto? Intanto, c'è la possibilità di verificare se il proprio indirizzo e-mail si trova nel database in questione, attraverso il sito [haveibeenpwned.com](#). Dopodiché (ma anche prima), cambiare la password dell'e-mail sarebbe una mossa conveniente.

Altro consiglio offerto dagli esperti è quello di non utilizzare più il numero di telefono riportato nel proprio profilo Facebook per fare delle verifiche incrociate, ad esempio sul cambio di una password. Come noto, spesso quando si vuole cambiare la chiave di accesso sia sul social sia su altri portali (compreso quello della carta di credito, ad esempio), si riceve un sms con un codice da inserire. Quello che si consiglia è di non utilizzare il numero associato al profilo Facebook per questo tipo di operazioni. Anche perché, così facendo, aumentano le informazioni a disposizione dei potenziali malintenzionati.

A monte, sarebbe opportuno inserire nel profilo di qualsiasi social network il minor numero possibile di dati personali.

( da [www.laleggepertutti.it](http://www.laleggepertutti.it) )