149 milioni di nomi utente e password trapelati online. Ci sono 48 milioni di account Gmail

Un ricercatore ha scoperto un database con oltre 149 milioni di nomi utente e password trapelati online, tra cui moltissimi account Gmail e social. Ecco di cosa si tratta.
(Fonte: https://www.money.it/ 26 gennaio 2026)

Ormai sappiamo che i nostri **dati personali** sono esposti ogni giorno a un impressionante numero di violazioni. Nonostante ciò le misure di sicurezza adottate dagli utenti sono spesso carenti o insufficienti, complice una certa tendenza a sottovalutare la reale portata del fenomeno. A ricordarci di questo errore c'è il lavoro dei professionisti informatici, cominciando dall'esperto in cybersecurity Jeremiah Fowler. Questo ricercatore ha scoperto una fuga di credenziali davvero allarmante, si parla di **149 milioni di login** con nomi utente e password in balia di ogni malintenzionato.
Tra questi ci sono **48 milioni di account Gmail**, il provider più diffuso nel complesso di **96 GB di dati grezzi** trapelati online, ma non mancano social network, conti bancari, giochi, siti di incontri e perfino siti governativi. Fowler, oltre ad avvisare tempestivamente gli organi competenti e i siti web interessati, ha condiviso con il pubblico l'esito del suo lavoro proprio per sensibilizzare gli utenti. È tempo che la protezione dei dati personali passi a un livello più attento e mirato, anche per chi ritiene di non avere nulla da temere. Nel rapporto dell'esperto si legge chiaramente che non viene mossa alcuna accusa ai sistemi di sicurezza dei provider, né tanto meno si vuole generare allarmismo su presunti pericoli. Più semplicemente:

149 milioni di credenziali online, di cui 48 milioni di account Gmail

Il ricercatore **Jeremiah Fowler**, impegnato nella promozione della cybersecurity e nell'analisi dei pericoli, ha individuato una fuga di dati contenente **149.404.754 login e password**. Un database da 96 GB disponibile online, completamente accessibile al pubblico come molti altri. L'esperto spiega che questo evidenzia la vulnerabilità degli stessi **hacker** alle violazioni dei dati, poiché le credenziali rubate attraverso malware e inganni non possono davvero rimanere nascoste, vista la necessità di archiviarle online in brevissimo tempo.

In quest'ultima scoperta, che avvisa non essere la prima, Fowler ha trovato dati di ogni piattaforma e Paese, comprese alcune credenziali governative che hanno imposto maggiore allerta. Tra i più diffusi c'erano però:

- **Gmail** (48 milioni);
- **Yahoo** (4 milioni);
- Outlook (1,5 milioni);
- iCloud (900mila);
- .edu (1,4 milioni);
- **Facebook** (17 milioni);
- **Instagram** (6,5 milioni);
- TikTok (780mila);
- Netflix (3,4 milioni);
- OnlyFans (100mila);
- Binance (420mila).

Questo non significa che ci siano stati **illeciti** da parte dei servizi citati, né di fatto che questi account siano più vulnerabili di altri. Potrebbe trattarsi meramente di una questione probabilistica, vista la diffusione di certi servizi, ma i dati pubblici sono insufficienti per verificare questa tendenza. L'opinione dell'esperto è che si tratti di un **database** rifornito periodicamente con svariate credenziali trafugate in ogni dove, tant'è che nel periodo tra la scoperta e la rimozione i numeri hanno continuato a crescere.

Fowler non ha infatti esitato a contattare l'hosting del database, non essendo disponibili indicazioni sulla proprietà, che però ha avuto qualche difficoltà ad intraprendere delle azioni visto che si trattava di un dominio indipendente. Alla fine, comunque, il database è stato **rimosso**, ma ciò non limita in alcun modo i rischi cui tutti gli utenti sono esposti ogni giorno.

A tal proposito, il ricercatore invita i siti web a fornire canali ben strutturati per la segnalazione di abusi, ma elenca anche preziosi consigli per gli utenti: "software **antivirus**, **autenticazione forte**, password uniche", ma pure aggiornamenti regolari, uso di servizi affidabili e riconosciuti. Insomma, pratiche semplici che possono fare grandi differenze nella salvaguardia dei dati dalle violazioni su larga scala, che sono ormai sempre più comuni.

Cancella la tua impronta digitale prima di pentirtene. Si fa così