533 million Facebook users' phone numbers and personal data leaked online

Personal data belonging to hundreds of millions of Facebook users were reportedly leaked online.

A user in a low-level cybercriminal forum posted phone numbers, Facebook IDs, full names, locations, birthdates, bios, marital status, employer, and, in some cases, email addresses of more than 533 million Facebook users.

The accounts on record reveal personal information from users across 106 countries, with over 32 million files on users from the US, 11 million on users in the UK, and 6 million in India. The leaked data were tested and verified by the Insider supporting the validity of the record set.

A Facebook spokesperson addressed the issue with Insider. The statement says that "the data had been scrapped because of a vulnerability that the company patched in 2019". The vulnerability they refer to relates to the company's contact importer tool.

A Gateway to Fraud and Impersonation

Alon Gal, chief technology officer of the cybercrime intelligence firm Hudson Rock, discovered the data leaks.

He said that even if the data is over two years old, it could still be helpful to cybercriminals. These individuals prey on people's data to commit fraud, impersonation, or blackmail users in exchange for their login credentials.

He stressed that the database of personal data is considerable enough for "bad actors taking advantage of the data to perform social-engineering attacks or hacking attempts."

Since it is accessible to anyone on the internet, those who have rudimentary data skills may use it for social engineering scams and other fraudulent activities online.

Not the First Time

Facebook users' phone numbers were exposed online before. The same dataset has been around since the beginning of the year.

Motherboard reported an automated bot wherein people could pay to acquire phone numbers from Facebook users. This information was also posted in the same forum. With this new development, payment is unnecessary as the dataset is published for free.

According to Facebook, the exposed vulnerability in 2019 led to millions of phone numbers being scraped from the platform's servers, violating the terms of the agreement.

They reportedly fixed the software vulnerability in August of 2019. However, Facebook plans to forcefully regulate mass-data scraping considering massive violations of Facebook's terms of service during the 2016 election campaign.

A Huge Breach of Trust

Gal stated that since the database has already been out in the open, there is nothing much Facebook can do to protect its users.

However, he also stressed that Facebook should notify the affected users so they could be aware and remain cautious about individuals who may take advantage of their personal data.

He also asserted that even though Facebook is free, the private information provided by people signing up should be treated with the utmost respect. Therefore, "personal information leaked is a huge breach of trust and should be handled accordingly."