Data Breach at Facebook Leaks Information of 533 Million Users

When and what happened?

A Facebook data leak with details of 533 million users has been reported, and the company has now officially responded to it in a lengthy blogpost, stating that the data is old and was actually scraped back in September 2019.

A major privacy violation by hackers allegedly took the data of almost 533 million users of Facebook from 106 countries to be posted online for free. More than 533 million private details that were posted online include records of over 32 million users in the US, 11 million users in the UK, and 6 million users in India. This breach is perhaps the largest in the social media giant's history of breaches. Hackers were selling information through a telegram bot such as phone numbers, Facebook IDs, full names, sites, birthdates, bios, and even e-mail addresses of several people are included in the breach.

How it happened and who were affected by the data breach?

Facebook in its response has tried to clarify that the data was not stolen by hacking into its system. The company states that the data or rather gathered by "scraping it from our platform prior to September 2019.

Facebook states that the malicious actors were able to 'scrape' or collect so much of this data from user profiles by using the company's "contact importer prior to September 2019." The feature is designed to help people find their friends on its service using their contact lists.

According to Facebook, the hackers were able to "query a set of user-profiles and obtain a limited set of information about those users included in their public profiles." It insists that no financial information, health information, or passwords were stolen as a result.

scraping is a common tactic that often relies on automated software to lift public information from the internet that can end up being distributed in online forums like this.

The data was scraped from people's Facebook profiles by malicious actors using facebook contact importer prior to September 2019...When they became aware of how malicious actors were using this feature in 2019, they made changes to the contact importer.

Even though Facebook stated that only information that was public on the platform when the scraping took place has been compromised, security experts have pointed out that even people who set their phone number visibility to private were affected by the leak.

What is Facebook doing to ensure this doesn't happen again?

Facebook states that any kind of scraping of data is against its terms of services and it has teams working to detect and stop such behaviour. It is also working to get this data set taken down. It adds that there is a "dedicated team focused on this work.

Further, Facebook is recommending users update their "How People Find and Contact You" control to ensure it is on the latest version. It is also recommending that a user turn on two-factor authentication on Facebook.

****