All about Facebook Data Breach

Why in news?

\n\n

Facebook has reported malicious activity in which the access tokens of 50 million users were appropriated by unknown hackers.

\n\n

What is Facebook data breach about?

\n\n

\n
- The ‘View As’ feature was introduced by Facebook as a privacy control feature, allowing users to check the information they were sharing with others.
\n
- Facebook noticed an unusual spike in the number of times the platform’s ‘View As’ feature was being used.
\n
- An access token is a digital key that allows users to stay logged into Facebook on a device or browser without having to sign in repeatedly using their password.
\n
- It extends its reach to other apps or services that users sign into using their Facebook account.
\n
- If hackers have the access tokens, they do not require passwords to get into Facebook accounts or apps like Instagram that utilise the Facebook login.
\n
- Following the data breech facebook announced that it had identified malicious activity in which the access tokens of 50 million users were appropriated by unknown hackers, and certain personal details possibly accessed.
\n

\n\n

What are the concerns with the data breech?

\n\n

\n

- While using the ‘View As' feature, Facebook’s video uploader tool also appeared on the page at times, generating an access token that was not the user's but of the person the user was looking up.
\n
- For example, if Hacker A selected User B for ‘View As,’ and the video uploader appeared on the page, it generated an access token for User B which was then available to Hacker A.
\n

\n\n

\n

- While Facebook has reportedly refreshed the access tokens of all affected parties, the extent to which the hackers had access to connected third-party apps remains unclear.
\n

\n\n

What was Facebook’s response?

\n\n

\n

- Facebook had to force the affected 50 million users, and an additional 40 million users who had used the ‘View As’ feature since last July to log in again so that their access tokens changed.
\n
- Facebook has since said it has resolved the bugs that caused what is said to be the largest breach in the history of the platform.
\n
- It also informed the Irish Data Protection Commission, since the European Union’s strict new data protection law states that it has to be informed within 72 hours if anyone in the European Economic Area is affected.
\n
- The Commission has started a probe, and Facebook faces a fine that could go over a billion dollars.
\n

\n\n

What does the data breech spolights?

\n\n

\n

- This breach again puts the spotlight on the vulnerabilities of Facebook, following the Cambridge Analytica data scandal.
  \n
- Aside from the direct impact of private data being accessed, massive data sets allow for psychological profiling a la Cambridge Analytica.
  \n
- This could lead to targeted political advertising and manipulation, especially at a time when crucial mid-term elections are due in the United States and in India, and it also undermines the faith in the ‘single sign-in.’
  \n

\n\n

\n\n

Source: The Hindu

\n

