Facebook Data Breach

Why in news?

\n\n

Facebook has put out more details about the data breach that exploited a vulnerability in its code between July 2017 and September 2018.

\n\n

What is the recent picture on data breach?

\n\n

\n
- Facebook has claimed that fewer users - 30 million, not 50 million - had their access tokens stolen by exploiting 400,000 accounts.
\n
- But crucially, the new revelation is that 15 million of the 30 had their name and contact details (phone numbers or e-mails) stolen.
\n
- This was depending on what people had on their profiles.
\n
- Another 14 million had details like gender, relationship status, their birth date, recent searches, and the last 10 places the person had checked into or were tagged in stolen.
\n
- This was along with name and contact details like others.
\n
- Just 1 million of the 30 had none of their data compromised.
\n
- But Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, Pages, payments, third-party apps, or advertising or developer accounts have not been affected.
\n

\n\n

How was it done?

\n\n

\n

- The attackers moved from account to account using an automated script collecting tokens.
\n
- This was done by repeatedly exploiting the vulnerability using access tokens for about 400,000 people.
\n
- The attackers then used the list of friends they collected to “eventually steal access tokens for about 30 million people.
\n
- So starting with the accounts they controlled directly, they moved to their friends and to their friends’ friends, and so forth.
\n

\n\n

\n
- The attackers could see things about users like-
\n

\n\n

\n
i. posts on their Timelines
\n
ii. their list of Friends
\n
iii. groups they’re members of
\n
iv. the names of some recent Messenger conversations
\n

\n\n

\n
- Facebook claims that the message content was not available to attackers.
\n
- But even this could have been seen if the person was Page admin and had received a message from someone.
\n

\n\n

What next?

\n\n

\n
- Facebook is sending customised messages to the 30 million users, suggesting steps to protect themselves.
\n

- On the Facebook Help Center, users can check if they have been affected and what information may have been accessed.
  \n
- Reportedly, accounts have already been secured by what Facebook did recently when they prompted millions of users to reset the access tokens.
  \n
- So no one needs to log out again or change passwords.
  \n
- But the risk is that stolen data could be used to target phishing mails etc to the users, knowing their preferences.
  \n
- So users have to be careful of suspicious e-mails, text messages or calls that could be made using this information.
  \n

\n\n

\n\n

Source: Indian Express

\n

