- Social networking / Data breach

How to ensure your data is safe after Facebook and LinkedIn leaks

The National - News · 12 Apr 2021 · 15 · Alkesh Sharma

With a series of data breaches hitting the social networking site Facebook and the world's largest professional network LinkedIn, it is difficult to determine if your sensitive data has been compromised or not. The National looks at recent leaks and explores potential tools to find out if your digital identity is safe.

Facebook and LinkedIn leaks The data of more than 533 million Facebook users resurfaced on an online hacking forum on April 3. The data, which was first leaked in 2019, included millions of files containing users' personal information. Data from more than 500 million LinkedIn profiles was put up for sale on another hacker forum last Tuesday, according to the CyberNews website.

"It is unknown whether the [LinkedIn] leak data is new or old ... it may not be a leak at all but rather a bot that has scraped the information and built a massive database," said Morey Haber, chief technology officer and chief information security officer at Georgia-based BeyondTrust. Have I been "pwned"? Users can check if their email ad dresses or phone numbers are part of the data leaks within a few seconds by logging on to haveibeen pwned.com. "Data breaches are rampant and many people don't appreciate the scale or frequency with which they occur," said Brisbane-based security researcher Troy Hunt, who runs HIBP. "There is rather a lot of leaked data floating around at the moment." The primary value of the recent Facebook data breach is the association of phone numbers to identities, HIBP said on its website.

"Each stolen record includes a phone number but only 2.5 million contained an email address. Most records contained names and genders, with many also including dates of birth, location, relation ship status and employer," it said.

What do experts recommend? Facebook users need to take "control and ownership" of their online identity, said Sam Curry, chief security officer at Boston cyber security company Cybereason.

"Consumers should check their credit card bills regularly, run a credit report, monitor their credit and consider putting a voluntary freeze on their credit," he said.

"If something is free ... remember that consumers are most likely the product, not the customer. Many consumers might not value their behavioural and personal data, but someone else values it enough to pay for it."

Industry experts said while some platforms encourage efforts by users to confirm whether their identities were compromised, the scope of such efforts and sometimes the process could be "malicious".

"Tools such as HIBP will allow you to search if your email address has been associated with a breach ... [but] not all breaches involve email addresses as part of the criteria exposed, which is true in Facebook's case as well," said Ammar Enaya, regional director for the Middle East, Turkey and North Africa at cyber security company Vectra AI.

Facebook has no plans to notify half a billion compromised users

Although Facebook admitted that the recent resurfacing of leaked files dated back to a 2019 incident, the social media network does not plan to notify users whose details have been stolen.

The California-based company said malicious actors obtained this data by scraping it from its platform before September 2019, and not by hacking. Scraping is a common tactic that often relies on automated software to lift public information from the internet.

“We have teams dedicated to addressing these kinds of issues and understand the impact they can have on the people who use our services,” Facebook said.

Italian and Irish agencies investigating

LinkedIn faces a probe by an Italian privacy watchdog. The regulator said anyone who receives such data and uses it could face sanctions. Ireland’s privacy authority is looking into the Facebook breach.