Logo

Hit by data breach? Here's how to reboot your life and control the damage

Find out extent of damage through dedicated websites, and get into damage control mode

Bindisha Sarang December 09, 2019 Last Updated at 19:45 IST

Photo: iStock

Last Friday, a security flaw in Bharti Airtel's mobile app reportedly exposed data of 300 million subscribers. Ehraz Ahmed, a web security researcher, who flagged the flaw in a blogpost, said the breach revealed information, such as your first name, last name, email, date of birth, address, subscription information, device capability information for 4G, 3G, and GPRS, network activation date, user type (prepaid/postpaid), and current International Mobile Equipment Identity (IMEI) number.

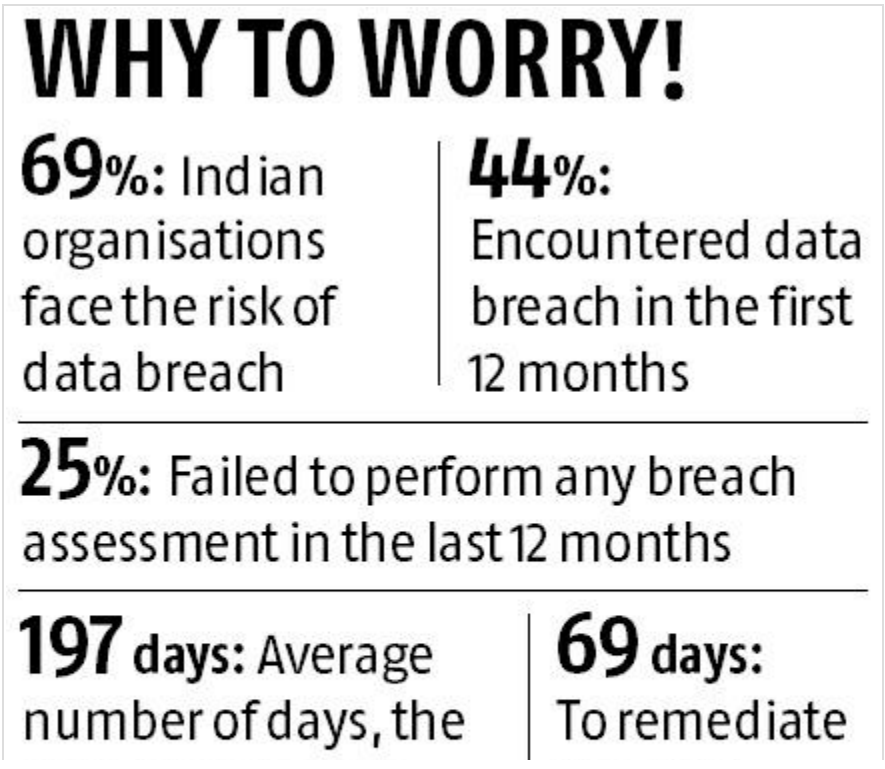
Says Ritesh Bhatia, a Mumbai-based cybersecurity expert: “Although Airtel has fixed this, I can only pray this data is not available to hackers or others who would want to misuse it.”

In an email interaction, the Airtel spokesperson said: “There was a technical issue in one of our testing application programming interfaces (APIs), which was addressed as soon as it was brought to our notice. Since these were testing APIs, we can now confirm that no data related to our customers has been impacted. Airtel’s digital platforms are highly secure. Customer privacy is of paramount importance to us, and we deploy the best of solutions to ensure the security of our digital platforms.”

According to the privacy and data protection research centre, Ponemon Institute’s 2018 Cost of a Data Breach Study, a data breach goes undiscovered for an average of 197 days. It takes another 69 days to remediate the data breach. By the time the security failure is discovered and fixed, the damage is already done. A CIO survey by Forcepoint and Frost & Sullivan found that 69 per cent of Indian organisations were at risk of data breach. Whenever there is data breach, there is a potential disaster waiting to happen.

The IMEI number, according to experts, can be used to identify the device of the user. Hackers can judge your financial position based on the IMEI number, as this reveals which phone model you use. Adds Bhatia: “A hacker can now target you, as he has almost all the information required to hack your device, including the make and model of your phone. This breached information can be used to make virtual clones of you. It can result in identity theft and an increase in spam messages.”

The first step in such situations is to find out if you have been impacted. Thankfully, there are data breach detection websites like Have I Been Pwned?, BreachAlarm, DeHashed, to name a few. These sites use your email to check which data has been breached, set data breach alters, and gives you information regarding the type of data breached. Less sensitive is a name, mobile number address, and more sensitive is email, date of birth, and other information used to verify identity. Next, update your device’s operating system, apps, and change to new unique passwords.



Bhatia says: “If there are passwords required to use the app, change the passwords immediately as there is a high possibility of the password, too, being leaked with the data.”

Then, if financial data is stolen, call the bank and block the cards. Mayur Joshi, a Pune-based cyberexpert, says: “Check your credit report and check for any recent inquires or past activities. Another thing to do is to accept the breached company’s offers to help. For instance, when Twitter was hacked, it texted the affected

user, asking him/her to change the password."

If a bank or any other financial services company is involved, it usually offers ways to help protect you against identity theft. And finally, if you have difficulty remembering passwords, use a password manager, such as Dashlane, LastPass, KeePass, and 1Password.