Date: 08.11.2023	**Publication:** Business Standard
Page no.: 2	**Edition:** New Delhi | Mumbai | Bangalore | Chennai | Ahmedabad | Chandigarh | Hyderabad
Headline: Cyber threat alert: Verify if your data was compromised	

Cyber threat alert: Verify if your data was compromised

Lock up Aadhaar biometric, keep a close tab on SMS inbox, credit report

BINDISHA SARANG

An alleged data breach involving 815 million Indians has surfaced on the Dark Web. According to media reports, millions of Indians' Aadhaar and passport details, names, phone numbers, and temporary and permanent addresses have been stolen.

Says Ritesh Bhatia, cyber-crime investigator, cybersecurity, and data privacy consultant, "Investigations by several hacker groups show that the number could be much smaller — a few lakhs. Nonetheless, it's important to take a few measures after this breach, besides being constantly vigilant."

Measures you should take

The first step you should take, according to Bhatia, is to lock your biometrics for additional security. Your biometric data is stored securely in the Aadhaar system. Using the mAadhaar app, you can lock and unlock your biometrics at your convenience. Says Bhatia, "You can also lock your biometrics from the www.uidai.gov.in website."

Know your status

By running a few checks, it is possible to learn if you are among those whose data has been compromised. Says Ajay Setia, chief executive officer (CEO), Invincible Ocean, a Metaverse platform, "Check for exposed data on sites like LeakPeek or DeHashed."

Safeguards against future attacks

Data breaches are becoming common. Take a few pre-emptive measures to protect yourself against future attacks.

First, ensure that your antivirus software is updated. Second, avoid clicking on links within text messages sent by unknown sources. Says Setia, "Delete stored passwords from your systems. Also, update your passwords regularly, particularly for internet banking and other crucial websites."

Your SMS inbox can also be a source of data breach. Clear it periodically of one-time passwords (OTPs) and other banking-related information. Says Bhatia, "Check every SMS you get. Many people ignore them. Remember if there is an activity in your account, your financial institution will send you an SMS, not a WhatsApp message."

Be cautious about downloading apps. Some of them could access your messages and other information stored on your phone. Says Setia, "Monitor your financial statements frequently for unauthorised transactions."

Check your credit report periodically for unexplained entries or inquiries you haven't made.

YOUR MONEY

Know your rights

India guarantees data protection rights under its constitution and the Information Technology Act of 2000. 'Body corporates' face penalties for mishandling sensitive data. Courts recognise the right to claim damages for privacy violations.

However, the Act's strict definition of 'body corporate' raises concerns regarding whether it applies to specific government bodies. Says Pratyush Miglani, managing partner, MVAC Advocates & Consultants, "The Digital Personal Data Protection (DPDP) Act further bolsters data protection, imposing penalties of up to ₹250 crore for data breaches. Nevertheless, the DPDP Act allows for exemptions to entities engaged in research, archiving, and statistics. The government, too, has the power to exempt institutions from its applicability, raising questions about its application to public institutions."

Buy cyber insurance cover

Today, buying cyber insurance has become a must not just for corporates but even for individuals. In the event of a data breach, this cover provides an individual the following: credit monitoring services, compensation for loss of wage while pursuing a resolution, and legal costs incurred on claiming damages from a third party for the data breach. Says T A Ramalingam, chief technical officer, Bajaj Allianz General Insurance, "The cyber policy for individuals also covers financial loss arising from a cyber-attack, cost of data restoration and malware decontamination, and cost incurred on dealing with a cyber-extortion attempt. It also offers covers to smart devices that may have been affected."

Cyber insurance also offers protection against identity theft, cyberstalking, phishing, email spoofing, media liability claims, cyber extortion, and data breach by a third party. The sum assured available can range from ₹1 lakh to 1 crore. Says Naval Goel, CEO and founder, PolicyX.com, "Currently, only three companies offer cyber insurance. Some of them provide worldwide coverage. Usually, these plans are targeted at individuals, but you can buy a top-up cover to protect your spouse, children, and other family members."

ONLINE IDENTITY THEFT: STEPS VICTIMS MUST TAKE

- Identity theft is the deliberate and unauthorised use of someone else's personal information to commit fraud or gain financial benefits
- Check all your accounts to see if multiple accounts have been compromised
- Change all your passwords immediately, opt for alphanumeric ones
- Contact your banks, lenders, and insurance companies immediately; request banks to close all affected accounts and open new ones
- Contact credit bureaus and raise a dispute
- Inform the nearest police station or cyber cell
- Check your computer and mobile for viruses, install anti-virus software