ET CISO.in
From The Economic Times

Sharing personal data on AI carries risk of leak to dark web, warn experts

Cybersecurity experts are warning individuals against sharing sensitive personal information on AI platforms due to escalating cyberattack risks. Data breaches could lead to the sale of private details like medical records and financial information on the dark web. Users are urged to mask personal data when interacting with generative AI tools to mitigate these growing vulnerabilities.

Cybersecurity experts on Wednesday cautioned people against sharing personal information on artificial intelligence (AI) platforms, citing the growing threat of cyberattacks in the event of data breaches.

"Many people tend to upload sensitive information like blood reports to AI platforms, which is extremely risky. If such platforms are compromised, this data could be sold on the dark web. Personal details like addresses, names of relatives, financial and medical records become highly vulnerable," Sanjay Katkar, joint managing director of Quick Heal Technologies, said.

The dark web is the illegal marketplace on the internet and a breeding place for cybercriminals.

The experts highlighted that online users were increasingly inputting sensitive data like Aadhaar and PAN details into prompts amid the widespread adoption of generative AI, exposing themselves to potential leaks, with cybercriminals deploying sophisticated tools to manipulate AI systems into bypassing their security protocols.

"As AI becomes more integrated into our daily lives, it also introduces new types of risks. Issues like accidental data leaks, misinformation and algorithmic manipulation are now serious security concerns," Ashish Biji, partner at advisory firm BDO India, said.

Many chatbots operate through application programming interfaces (APIs) that connect them to broader AI platforms. While these platforms continuously enhance their security measures, the experts said cyberattackers were evolving their tactics and adopting more sophisticated methods. "People should mask personal data when interacting with generative AI tools," Katkar said.

Quick Heal recently launched version 26 of its cybersecurity platform, featuring predictive threat detection, an intelligent digital assistant and anti-fraud capabilities.

A 2025 IBM study revealed that numerous Indian organisations were prioritising rapid AI adoption over proper security and governance protocols, significantly increasing their vulnerability to breaches. The study also reported that the average cost of a data breach in India rose to Rs 22 crore in 2025.

"AI is being embedded across business functions at a rapid pace, but security and governance are lagging. The lack of access controls and AI governance tools isn't just a technical gap, it's a strategic risk," Viswanath Ramaswamy, VP of Technology at IBM India and South Asia, said.