Hundreds of Thousands of Users' Grok Chats Exposed in Google Search Results

cybersecuritynews.com/grok-chats-exposed-in-google-search-results

Guru Baran August 23, 2025

A significant data exposure has revealed hundreds of thousands of private user conversations with Elon Musk's AI chatbot, Grok, in public search engine results.

The incident, stemming from the platform's "share" feature, has made sensitive user data freely accessible online, seemingly without the knowledge or explicit consent of the users involved.

The exposure was discovered when it became clear that using Grok's share button did more than just generate a link for a specific recipient. It created a publicly accessible and indexable URL for the conversation transcript.

Consequently, search engines like Google crawled and indexed this content, making private chats searchable by anyone. A Google search on Thursday confirmed the

scale of the issue, revealing nearly 300,000 indexed Grok conversations, with some reports from tech publications placing the number even higher, at over 370,000.

An analysis of the exposed chats highlights the severity of the privacy breach. Transcripts seen by the BBC and other outlets included users asking Grok for deeply personal or sensitive information. Examples ranged from creating secure passwords and detailed medical inquiries to developing weight-loss meal plans.

Through the CybersecurityNews team's analysis using Google Dork Queries, we were able to identify multiple pages with the query *site:https://x.com/i/grok?conversation=*.

Grok Conversation on Google Search (Source: cybersecuritynews.com)

The data also revealed users testing the chatbot's ethical boundaries, with one indexed chat containing detailed instructions on how to manufacture a Class A drug. While user account details may be anonymized, the content of the prompts themselves can easily contain personally identifiable or highly sensitive information.

Grok Conversation on Google Search (Source: cybersecuritynews.com)

This incident is not an isolated case in the rapidly evolving AI landscape. OpenAI, the creator of ChatGPT, recently reversed an experiment that also resulted in shared conversations appearing in search results.

Similarly, Meta faced criticism earlier this year after its Meta AI chatbot's shared conversations were aggregated into a public "discover" feed. These repeated events underscore a troubling pattern of prioritizing feature deployment over user privacy.

Experts are sounding the alarm, describing the situation as a critical failure in data protection. "AI chatbots are a privacy disaster in progress," Professor Luc Rocher of the Oxford Internet Institute told the BBC, warning that leaked conversations containing sensitive health, business, or personal details will remain online permanently.

The core of the issue lies in the lack of transparency. Dr. Carissa Véliz, an associate professor at Oxford's Institute for Ethics in AI, emphasized that users were not

adequately informed that sharing a chat would make it public. “Our technology doesn’t even tell us what it’s doing with our data, and that’s a problem,” she stated.

As of this report, X, the parent company of Grok, has not issued a public comment on the matter.

[Guru Baranhttps://cybersecuritynews.com](https://cybersecuritynews.com)
Gurubaran KS is a cybersecurity analyst, and Journalist with a strong focus on emerging threats and digital defense strategies. He is the Co-Founder and Editor-in-Chief of Cyber Security News, where he leads editorial coverage on global cybersecurity developments.