

Grok AI Chats Exposed In Google Search Results

 cybersecurityintelligence.com/blog/grok-ai-chats-exposed-in-google-search-results-8672.html

More than 370,000 Grok chats have been indexed by search engines, exposing hundreds of sensitive prompts that include medical and psychological questions, business details, and at least one password.

The chats have been exposed due to a Grok's "share" feature, which users might use to send a record of a conversation to another person, or even to their own email. The share feature creates a unique URL when for the conversation.

Those links were automatically published on Grok's website and left open to search engines, seemingly without users' knowledge.

Amongst chat transcripts there were examples of Musk's chatbot being asked to create a secure password, provide meal plans for weight loss and answer detailed questions about medical conditions. Some indexed transcripts also showed users' attempts to test the limits on what Grok would say or do. It is not the first time that peoples' conversations with AI chatbots have appeared more widely than they perhaps initially realised when using share functions.

OpenAI recently rowed back an experiment which saw ChatGPT conversations appear in search engine results when shared by users. Earlier this year, Meta faced criticism after shared users conversations with its chatbot Meta AI was on a public feed on its App.

Loss Of Privacy

While users' account details may be anonymised or obscured in shared chatbot transcripts, their prompts may still contain, and risk revealing, personal, sensitive information about someone. Experts say this highlights increases concerns over users' privacy. [Carissa Veliz](#), associate professor in philosophy at Oxford University's Institute for Ethics in AI, has said users not being told shared chats would appear in search results is problematic.

Users increasingly treat chatbots as confidants, feeding them sensitive details like health information, financial details, or relationship issues they likely would not want to be public.

Even if chats are anonymised, prompts often contain identifying details that could be traced back to users or mined by malicious actors, data brokers, or hackers for targeted campaigns. Some people have already identified a business case for Grok's

public chats. Apparently some marketing professionals are already discussing ways to exploit shared Grok conversations to boost business visibility.

Since the Grok conversations are published as web pages with individual URLs, businesses could potentially script chats that mention their products alongside keywords in order to game search results or create backlinks, although it's unclear how successful this would be.

This tactic might pass on some SEO value and help to manipulate Google's rankings, but it could also be perceived as spam by Google and ultimately hurt visibility.

Image: [hapabapa](#)

You Might Also Read:

[The Problem With Generative AI - Leaky Data:](#)

If you like this website and use the comprehensive 7,000-plus service supplier Directory, you can get unrestricted access, including the exclusive in-depth Directors Report series, by signing up for a [Premium Subscription](#).

Individual £5 per month or £50 per year. [Sign Up](#)

Multi-User, Corporate & Library Accounts Available on Request

Inquiries: [Contact Cyber Security Intelligence](#)

Cyber Security Intelligence: Captured Organised & Accessible

[« VPS Server Rental Explained: Secure Hosting For Growing Projects](#)
[Converging Physical & Cyber: Securing Cloud-Connected Cameras Across Multi-Site](#)
[»](#)

Visa is a global payments technology company that connects consumers, businesses and banks in more than 200 countries and territories worldwide.

