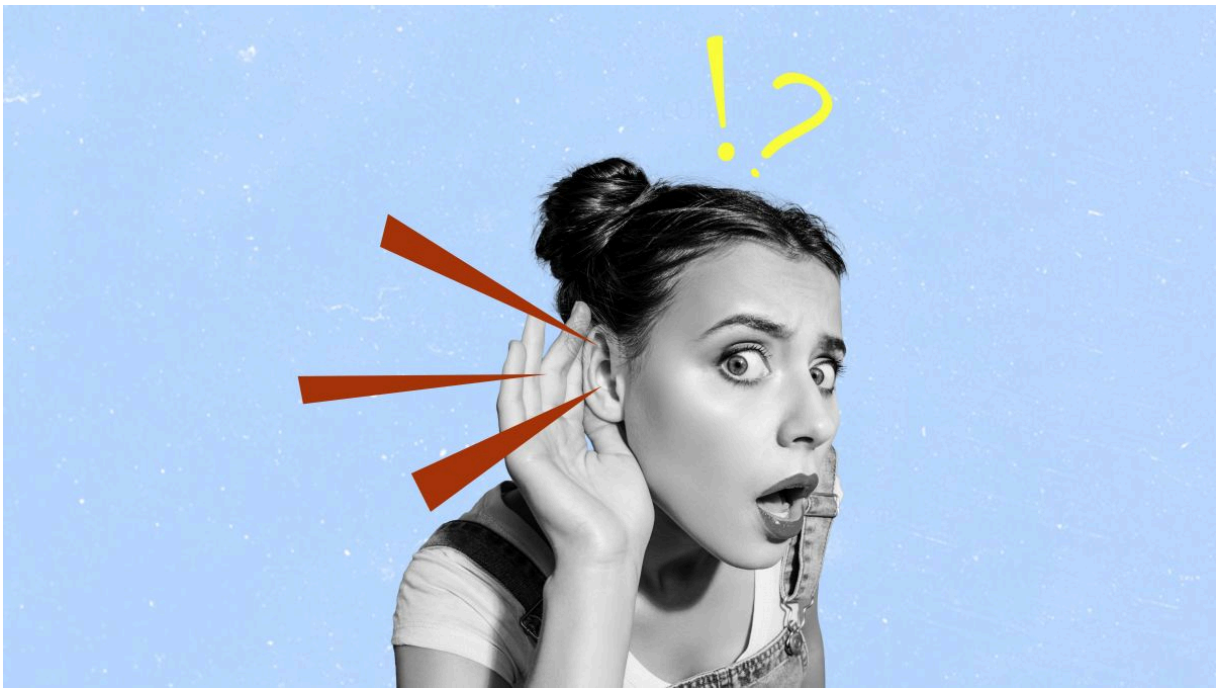
AI chat app leak exposes 300 million messages tied to 25 million users

malwarebytes.com/blog/news/2026/02/ai-chat-app-leak-exposes-300-million-messages-tied-to-25-million-users

Pieter Arntz February 9, 2026



An independent security researcher uncovered a major data breach affecting Chat & Ask AI, one of the most popular AI chat apps on Google Play and Apple App Store, with more than 50 million users.

The researcher claims to have accessed 300 million messages from over 25 million users due to an exposed database. These messages reportedly included, among other things, discussions of illegal activities and requests for suicide assistance.

Behind the scenes, Chat & Ask AI is a “wrapper” app that plugs into various large language models (LLMs) from other companies, including OpenAI’s ChatGPT, Anthropic’s Claude, and Google’s Gemini. Users can choose which model they want to interact with.

The exposed data included user files containing their entire chat history, the models used, and other settings. But it also revealed data belonging to users of other apps developed by Codeway—the developer of Chat & Ask AI.

The vulnerability behind this data breach is a well-known and documented Firebase misconfiguration. Firebase is a cloud-based backend-as-a-service (BaaS) platform

provided by Google that helps developers build, manage, and scale mobile and web applications.

Security researchers often refer to a set of preventable errors in how developers set up Google Firebase services, which leave backend data, databases, and storage buckets accessible to the public without authentication.

One of the most common Firebase misconfigurations is leaving Security Rules set to public. This allows anyone with the project URL to read, modify, or delete data without authentication.

This prompted the researcher to create a tool that automatically scans apps on Google Play and Apple App Store for this vulnerability—with astonishing results. Reportedly, the researcher, named Harry, found that 103 out of 200 iOS apps they scanned had this issue, collectively exposing tens of millions of stored files.

To draw attention to the issue, Harry set up a website where users can see the apps affected by the issue. Codeway's apps are no longer listed there, as Harry removes entries once developers confirm they have fixed the problem. Codeway reportedly resolved the issue across all of its apps within hours of responsible disclosure.

How to stay safe

Besides checking if any apps you use appear in Harry's Firehoundregistry, there are a few ways to better protect your privacy when using AI chatbots.

- Use private chatbots that don't use your data to train the model.
- Don't rely on chatbots for important life decisions. They have no experience or empathy.
- Don't use your real identity when discussing sensitive subjects.
- Keep shared information impersonal. Don't use real names and don't upload personal documents.
- Don't share your conversations unless you absolutely have to. In some cases, it makes them searchable.
- If you're using an AI that is developed by a social media company (Meta AI, Llama, Grok, Bard, Gemini, and so on), make sure you're not logged in to that social media platform. Your conversations could be linked to your social media account, which might contain a lot of personal information.

Always remember that the developments in AI are going too fast for security and privacy to be baked into technology. And that even the best AIs still hallucinate.

Browse like no one's watching.