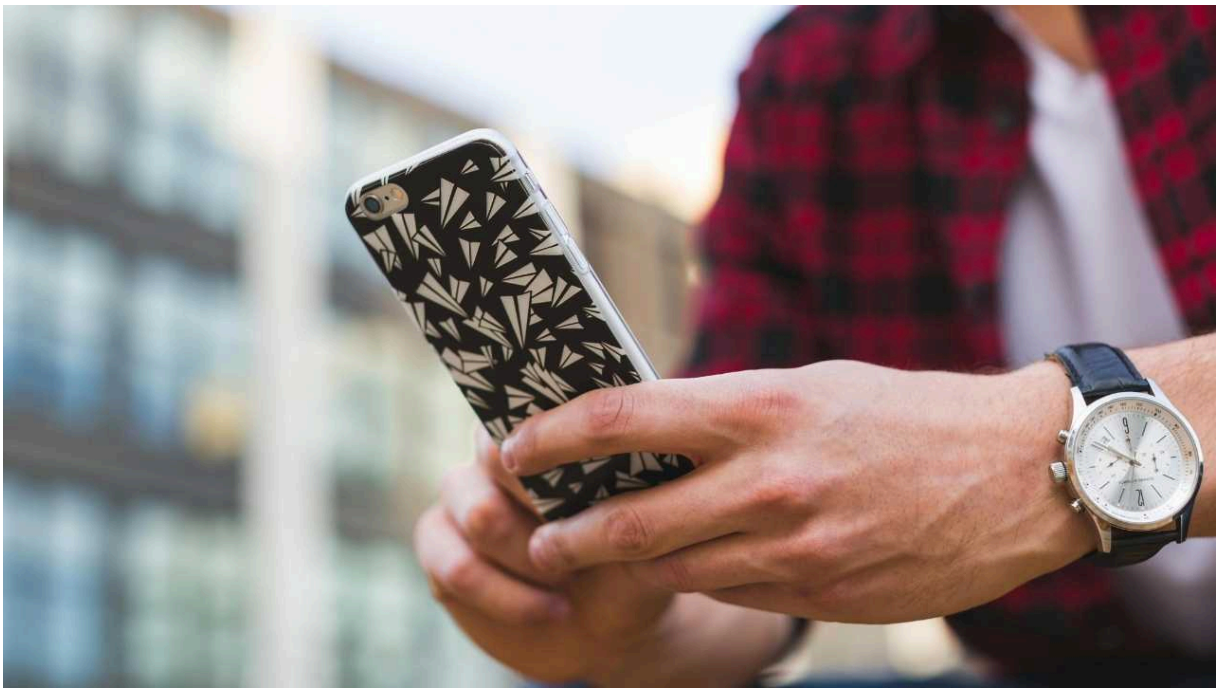
Millions of AI chat messages exposed in app data leak

cyberguy.com/security/millions-ai-chat-messages-exposed-app-data-leak

Kurt Knutsson February 5, 2026

- **A popular AI chat app with more than 50 million users exposed hundreds of millions of private conversations online.**
- **The leak was caused by a misconfigured database that allowed outsiders to access stored chat histories.**
- **Exposed messages included deeply personal topics, illegal activity, and mental health struggles.**
- **The incident shows why users should assume AI chats may be stored and limit what they share.**

A popular mobile app called Chat & Ask AI has more than 50 million users across the Google Play Store and Apple App Store. Now, an independent security researcher says the app exposed hundreds of millions of private chatbot conversations online. The exposed messages reportedly included deeply personal and disturbing requests. Users asked questions like how to painlessly kill themselves, how to write suicide notes, how to make meth, and how to hack other apps. These were not harmless prompts. They were full chat histories tied to real users.



What exactly was exposed

The issue was discovered by a security researcher who goes by Harry. He found that Chat & Ask AI had a misconfigured backend using Google Firebase, a popular mobile app development platform. Because of that misconfiguration, it was easy for outsiders to gain authenticated access to the app's database. Harry says he was able to access roughly 300 million messages tied to more than 25 million users. He analyzed a smaller sample of about 60,000 users and more than one million messages to confirm the scope.

The exposed data reportedly included:

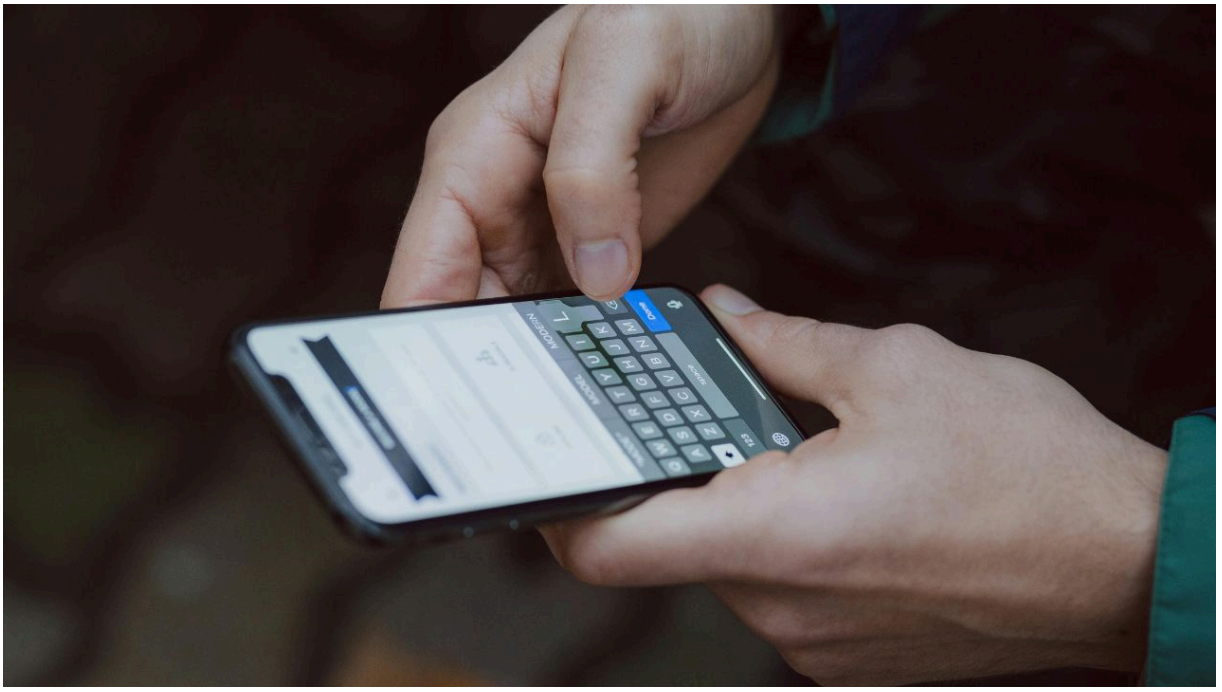
- Full chat histories with the AI
- Timestamps for each conversation
- The custom name users gave the chatbot
- How users configured the AI model
- Which AI model was selected

That matters because many users treat AI chats like private journals, therapists, or brainstorming partners.

How this AI app stores so much sensitive user data

Chat & Ask AI is not a standalone AI model. It acts as a wrapper that lets users talk to large language models built by bigger companies. Users could choose between models from OpenAI, Anthropic, and Google, including ChatGPT, Claude, and Gemini. While those companies operate the underlying models, Chat & Ask AI handles the storage. That is where things went wrong. Cybersecurity experts say this type of Firebase misconfiguration is a well-known weakness. It is also easy to find if someone knows what to look for.

We reached out to Codeway, which publishes the Chat & Ask AI app, for comment, but did not receive a response before publication.



Why this matters to everyday users

Many people assume their chats with AI tools are private. They type things they would never post publicly or even say out loud. When an app stores that data insecurely, it becomes a gold mine for attackers. Even without names attached, chat histories can reveal mental health struggles, illegal behavior, work secrets, and personal relationships. Once exposed, that data can be copied, scraped, and shared forever.

Ways to stay safe when using AI apps

You do not need to stop using AI tools to protect yourself. A few informed choices can lower your risk while still letting you use these apps when they are helpful.

▶

💰 Free live class: Protect Your Money
Join us Saturday, August 29, at 10 AM ET for simple steps to help protect against scams, fraud and identity theft. Get the checklist plus the recording afterward.

Reserve Your Free Spot
🛒 This week's top Amazon deals
See Kurt's latest Amazon picks for useful gadgets, smart home upgrades and everyday tech worth grabbing while the deals last.

See picks

1) Be mindful of sensitive topics

AI chats can feel private, especially when you are stressed, curious, or looking for answers. However, not all apps handle conversations securely. Before sharing deeply personal struggles, medical concerns, financial details, or questions that could create legal risk if exposed, take time to understand how the app stores and protects your data. If those protections are unclear, consider safer alternatives such as trusted professionals or services with stronger privacy controls.

2) Research the app before installing

Look beyond download counts and star ratings. Check who operates the app, how long it has been available, and whether its privacy policy clearly explains how user data is stored and protected.

3) Assume conversations may be stored

Even when an app claims privacy, many AI tools log conversations for troubleshooting or model improvement. Treat chats as potentially permanent records rather than temporary messages.

4) Limit account linking and sign-ins

Some AI apps allow you to sign in with Google, Apple, or an email account. While convenient, this can directly connect chat histories to your real identity. When possible, avoid linking AI tools to primary accounts used for work, banking, or personal communication.

5) Review app permissions and data controls

AI apps may request access beyond what is required to function. Review permissions carefully and disable anything that is not essential. If the app offers options to delete chat history, limit data retention, or turn off syncing, enable those settings.

6) Use a data removal service

Your digital footprint extends beyond AI apps. Anyone can find personal details about you with a simple Google search, including your phone number, home address, date of birth, and Social Security number. Marketers buy this information to target ads. In more serious cases, scammers and identity thieves breach data brokers, leaving personal data exposed or circulating on the dark web. Using a data removal service helps reduce what can be linked back to you if a breach occurs.

While no service can guarantee the complete removal of your data from the internet, a data removal service is really a smart choice. They aren't cheap, and neither is your privacy. These services do all the work for you by actively monitoring and systematically erasing your personal information from hundreds of websites. It's what gives me peace of mind and has proven to be the most effective way to erase your personal data from the internet. By limiting the information available, you reduce the risk of scammers cross-referencing data from breaches with information they might find on the dark web, making it harder for them to target you.

Incogni, a service I trust 100% and use myself, helps automate the process by submitting removal requests to hundreds of data brokers and people-search sites on your behalf.

Incogni automatically contacts data brokers on your behalf and requests the removal of your personal information. It also continues monitoring those sites and submits new removal requests if your data reappears.

- Incogni currently removes personal data from **420+ data broker and people-search websites**, and its **Unlimited plan** allows you to request removals from as many additional sites as you need.
- Incogni has also received **third-party assurance from Deloitte**, validating its marketing claims.
- The goal is simple: **make it much harder for strangers, scammers, and cybercriminals to find your personal information online.**

CyberGuy Exclusive: 60% off

CyberGuy readers get 60% off Incogni's annual plans using the links in this article.

The service also includes a **30-day money-back guarantee**, so you can try it risk-free and see how much of your information is exposed online.

Is your personal information exposed online?

Run a free scan to see if your personal info is compromised. Results arrive by email in about an hour.

Related Links:

- Can AI chatbots trigger psychosis in vulnerable people?
- Fake AI chat results are spreading dangerous Mac malware
- Third-party breach exposes ChatGPT account details

Kurt's key takeaways

AI chat apps are moving fast, but security is still lagging behind. This incident shows how a single configuration mistake can expose millions of deeply personal conversations. Until stronger protections become standard, you need to treat AI chats with caution and limit what you share. The convenience is real, but so is the risk.

Do you assume your AI chats are private, or has this story changed how much you are willing to share with these apps? Let us know your thoughts in the comments below.

FOR MORE OF MY TECH TIPS & SECURITY ALERTS, SUBSCRIBE TO MY FREE CYBERGUY REPORT NEWSLETTER HERE