

Claude chats and workspaces turn up on Google, revealing avoidable privacy flaw

 cybernews.com/ai-news/claude-chats-artifacts-indexed-google

Niamh Ancell

July 27, 2026

Key takeaways:

- Anthropic faces backlash after shared Claude chats and artifacts appeared in Google and other search results.
- Reported exposed data included personal details, clinical trial records, access codes, resumes, API keys, and financial information.
- Anthropic says “anyone with a link” shares a snapshot of prior messages and artifacts, not later private messages.
- Developers argue Anthropic should block search indexing by default, while others say users knowingly made links public.

Key Takeaways by nexos.ai, reviewed by Cybernews staff.

Anthropic is under fire after a viral Reddit post revealed a massive privacy issue affecting any Claude user who shared their chats or projects using “anyone with a link.”

Developers were shocked to learn that all Claude chats and artifacts shared via “anyone with a link” contained a serious flaw that let crawlers index them on Google and other major search engines.

The underlying issue raised by developers is that sensitive information shouldn’t be indexed by Google, Bing, and other search engines by default.

However, others argue that users are responsible for leaking their own information.

What was leaked?

What Reddit users are calling a “simple yet critical mistake” has already caused major issues, as sensitive information like Social Security numbers has reportedly been leaked as a result.

One user posted a clinical trial clearly from Claude, which was indexed by Google, revealing patients’ full names, ages, genders, ethnicities, skin types, and treatment dates.

Another link led *Cybernews* to a “Location Data Collection” database that appeared to show locations and apartment access codes.

Another interesting find publicly available on Google is Jerome Glenn's AGI Strategy Flow Chart, which has been viewed over 2,000 times.



jpg flow chart claude

Screenshot from Claude

This strategy, while unverified, could be related to the CEO of The Millennium Project, who has said that artificial general intelligence (AGI) should be the world's top priority, [according to CIRSD](#).

One X user, Om Patel, who is behind the AI agent platform BigIdeasDB, broadcast the leak to his 26,000 followers, revealing that the situation is much worse than just chats.

People are likely to bake financial information, roadmaps, legal documents, personal health data, tax documents, and bank statements into [artifacts](#), according to Patel.

Patel reportedly uncovered resumes with real names and contact information as well as API keys, crypto wallets, and Social Security numbers, [reports explainai](#).

These sensitive data types raise security concerns surrounding conversation and workspace sharing in Claude.

“Anyone with a link” is quite literal

Anthropic's “anyone with a link” truly does mean that ANYONE with the link can view the information in your chats and artifacts.

Once a Claude user clicks “anyone with a link,” a separate URL is created, which functions as a snapshot of the conversation or artifact – not the whole thing.

Anyone with the link can view the shared snapshot, which “includes all messages that were sent prior to sharing the chat, including any artifact,” [according to Anthropic](#).

“All messages sent after sharing a chat will remain private by default.”



A smartphone with private messages, a child's face behind it

Image by Cybernews

One “experienced developer” replied to the thread saying that Anthropic “literally points out that it will be accessible via search results when you go to publish an artifact.”

Developers and artifact users have created and use third-party sites that display a large number of published artifacts that have presumably been shared.

This may also be a good source for Google and Bing to crawl.

While users have to approve and acknowledge that publishing an artifact “will make it accessible to anyone on the internet and potentially visible in search engine results,” said one user, developers argue that “shareable” shouldn’t mean “public.”



anthropic-consumer-terms

Image by Cybernews.

Anthropic could’ve avoided this quite easily, devs argue

Many people, including developers, seemed to blame users, while others argued that “link” and “not indexed” are “two separate promises.”

“Any product that lets you generate a public link with one click should default those routes to no-index / X-Robots-Tag and only make them crawlable if someone opts in on purpose,” said one Redditor.

A recurring argument amongst the community is that Anthropic could have easily implemented a tag that tells search engine crawlers how to interact with the page.

If Anthropic had added robot.txt or noindex tags to shareable URLs, then the problem would likely not be as prominent.



404 error, bots

Image by Cybernews.

Anthropic only provides two options when publishing artifacts – “Only me” and “Anyone with a link.”

Developers feel that by default, these links should be protected and shouldn’t be indexed by search engines due to the amount of proprietary information and possible personally identifiable information in the artifacts.

“It’s weird how many people are defending this as something expected, common, and acceptable?” said one user.

Anthropic didn’t learn from OpenAI

In almost an identical fashion, ChatGPT’s shared links feature created a unique URL for the conversation, which became accessible to anyone.

Once the URL is shared on social media or a publicly accessible website, it can be caught by crawlers, which will index it on Google if there’s no command against it.

OpenAI warned users not to include sensitive information, but many, like Claude users, assumed that their private moments with ChatGPT wouldn't be aired out in public.