Nothing Phone says it will hack into iMessage, bring blue bubbles to Android

Enlarge / The Nothing Phone 2 all lit up.
Ron Amadeo

reader comments

136 with

Can an Android OEM really just hack its way into Apple's iMessage? That is the hard-to-believe plan from upstart phone manufacturer "Nothing," which says the new "Nothing Chats" will allow users to use "iMessage on Android" complete with a blue bubble sent to all their iPhone friends.

Nothing Chat will be powered by Sunbird, an app developer that has claimed to be able to send iMessage chats for about a year now, with no public launch. According to a Washington Post article with quotes from the CEOs of Nothing and Sunbird, Nothing will "start" rolling out "an early version" of Nothing Chats with iMessage compatibility on Friday. The only catch, supposedly, is that you'll need a Nothing Phone 2.

Is this for real or a publicity stunt? Apple is on record saying that iMessage on Android would only serve to weaken Apple, and it doesn't want to do that. Surely, any Android OEM offering "iMessage" support would immediately have the project shut down by Apple.

The quotes in the Post article from Nothing and Sunbird come across as *a dare* more than anything else. Nothing CEO Carl Pei

told the paper, “There’s nothing illegal about this setup. I think whatever we do is gonna be passed along within Cupertino, but we’re so small that it will look really bad if Apple takes any action.” Sunbird CEO Danny Mizrahi added, “We don’t see a scenario where Apple tries to, or can, block these messages. Apple’s focus has openly been on providing the best experience to their end users and both Nothing Chats and Sunbird help with that.”

It’s hard to believe something like this could be a long-running service, and it seems destined to be immediately shut down.

The many red flags of Sunbird

Sunbird has claimed to be able to send iMessages on Android for a long time, has missed its deadline for launch, and generally doesn’t come off as a serious company. The company announced itself to the world with the promise of iMessage on Android during a press briefing in December 2022. I attended this meeting and did not write about it because Sunbird’s suspect presentation did not meet my standards for a story. To me, the purpose of a press meeting like this would be to overcome the skepticism about the claim that you could imperviously, permanently hack into iMessage. Being honest with the press would have helped, but Sunbird refused to take open questions in its big debut. Sunbird’s PR person approved and asked all the questions, the Zoom chat was turned off, and the company didn’t answer a single one of the basic technical questions.

Advertisement

Enlarge / Sunbird’s app, which has never launched.

How does Sunbird work? Why should people trust Sunbird with their ultra-important Apple account credentials, which contain some people’s entire online lives and, in some cases, a literal bank account? How are these credentials secured? Are they stored on Sunbird’s servers somewhere? Doesn’t hacking into iMessage with a third-party client violate Apple’s terms of service, possibly leading to an account ban? Won’t Apple just shut this down the instant you launch? These are all critical and obvious questions that *were* asked at the meeting, some of them by me, and they all went unanswered. Instead, the Sunbird people focused on how great it would be if the whole world could hold hands and share access to blue-colored chat bubbles. It wasn’t just ridiculous—the company completely failed to convince a skeptical listener that it was for real

or acknowledge that there was any skepticism to overcome.

Even today, almost a year later, the company does not answer these questions in its FAQ. Sunbird has a “Privacy & Security” page that doesn’t answer anything about the privacy or security of your Apple credentials. This company just wants to hand-wave away any concerns. To me, without the company offering public, comprehensive explanations around Apple ID security, it seems hard to take it seriously. https://arstechnica.com/?p=1983702