Twitter’s two-factor authentication change “doesn’t make sense”

reader comments

107 with

Share this story

Twitter announced Friday that as of March 20, it will only allow its users to secure their accounts with SMS-based two-factor authentication if they pay for a Twitter Blue subscription. Two-factor authentication, or 2FA, requires users to log in with a username and password and then an additional “factor” such as a numeric code. Security experts have long advised that people use a generator app to get these codes. But receiving them in SMS text messages is a popular alternative, so removing that option for unpaid users has left security experts scratching their heads.

Twitter’s two-factor move is the latest in a series of controversial policy changes since Elon Musk acquired the company last year. The paid service Twitter Blue—the only way to get a blue verified checkmark on Twitter accounts now—costs $11 per month on Android and iOS and less for a desktop-only subscription. Users being booted off of SMS-based two-factor authentication will have the option to switch to an authenticator app or a physical security key.

“While historically a popular form of 2FA, unfortunately, we have seen phone-number-based 2FA be used—and abused—by bad actors,” Twitter wrote in a blog post published Friday evening. “So starting today, we will no longer allow accounts to enroll in the text message/SMS method of 2FA unless they are Twitter Blue subscribers.”

Advertisement

In a July 2022 report about account security, Twitter said that only 2.6 percent of its active users have any type of two-factor authentication enabled. Of those users, nearly 75 percent were using the SMS version. Almost 29 percent were using authenticator apps, and less than 1 percent had added a physical authentication key.

SMS-based two-factor authentication is insecure because attackers can hijack targets’ phone numbers or use other techniques to intercept the texts. But security experts have long emphasized that using SMS two-factor is significantly better than having no second authentication factor enabled.

Increasingly, tech giants like Apple and Google have eliminated the option for SMS two-factor and transitioned users (typically over many months or years) to other forms of authentication. Researchers worry that Twitter’s policy change will confuse users by giving them so little time to complete the transition and making SMS two-factor seem like a premium feature.

“The Twitter blog is right to point out that two-factor authentication that uses text messages is frequently abused by bad actors. I agree that it is less secure than other 2FA methods,” says Lorrie Cranor, director of Carnegie Mellon’s usable privacy and security lab. “But if their motivation is security, wouldn’t they want to keep paid accounts secure too? It doesn’t make sense to allow the less secure method for paid

accounts only.”

https://arstechnica.com/?p=1918817