Secure messaging arrives on Twitter—sort of. 'Don't trust it yet,' Musk warns

May 12 2023, by David Hamilton

The Twitter splash page is seen on a digital device, April 25, 2022, in San Diego. Twitter launched encrypted messaging Wednesday, May 10, 2023, offering select users the ability to communicate more securely. But its new service is much more of a baby step than a giant leap forward. Credit: AP Photo/Gregory Bull, File

Twitter launched encrypted messaging Wednesday, offering select users the ability to communicate more securely. But its new service is much more of a baby step than a giant leap forward.

For starters, it lacks basic protections that security experts consider essential for shielding messages from hackers and other prying eyes. Senders and receivers must also be subscribed to Twitter's Blue service for $11 a month ($8 for desktop-only) or otherwise affiliated with an organization "verified" by Twitter for $1,000 a month plus $50 per user.

The company's official message announcing the rollout promised additional features soon. But CEO Elon Musk offered his own caution via a tweet: " Try it, but don't trust it yet. "

WHAT IS ENCRYPTED MESSAGING AGAIN?

Ordinary messages sent across the internet, whether by email, direct message, Twitter or other means—are generally vulnerable to interception that could allow other people or organizations to read them. That includes the companies offering the message services. Those companies can also be required to produce user messages in response to a legal subpoena or court order.

Encryption technology offers protection against spies and nosy online neighbors by encoding messages so that only the sender and the recipient can decipher them.

SO HOW DOES TWITTER'S NEW ENCRYPTION STACK UP?

Not super well. The gold standard in secure messaging is set by services such as Signal and ProtonMail, which use strong "end-to-end" encryption

to shield messages so that no one else—not even the companies themselves—can read them.

Twitter's service doesn't currently do that. For the moment, its encrypted messages are vulnerable to a so-called "man-in-the-middle" attack that allows an attacker to insinuate themselves into an encrypted conversation to listen in and even modify messages as they're sent. Twitter itself, in fact, has the ability to do this.

"The acid test is that I could not see your DMs even if there was a gun to my head," Musk tweeted on Tuesday. But Twitter isn't there yet.

Twitter also doesn't offer any way to report encrypted messages for harassment or abuse, although it will be possible to block individual senders.

ARE THERE OTHER DRAWBACKS?

Yes. For instance, Twitter's encrypted messages can only be sent to another individual. Twitter says it will "soon" be expanding encryption to groups. Encrypted messages are also limited to text and links; photos, video and other attachments aren't supported yet, the company says.

Twitter encryption also doesn't provide what's called "forward secrecy," which would prevent an attacker who gets hold of a user's private key from using it to read earlier and subsequent messages.

In its official document, Twitter says forward secrecy techniques aren't compatible with user expectations that they'll always be able to obtain their historical messages from the cloud. As a result, the company doesn't plan to offer forward secrecy at all.

A final issue: Users won't have any way to make encrypted messages a

default setting; they'll have to deliberately choose encryption each time they start a new conversation.