nytimes.com

Twitter C.E.O. Jack Dorsey’s Account Hacked

By Kate Conger

5-7 minutes

Technology|Twitter C.E.O. Jack Dorsey’s Account Hacked

Image

Jack Dorsey’s Twitter account began posting racial epithets, profanities and bomb threats on Friday afternoon.CreditCreditEric Thayer for The New York Times

SAN FRANCISCO — Hackers took over the Twitter account of Twitter's chief executive, Jack Dorsey, on Friday and used the account to broadcast a string of racist messages and bomb threats.

In the posts, the attackers claimed that Twitter's San Francisco headquarters would be bombed, and used Mr. Dorsey's account to retweet posts from several individuals appearing to claim responsibility for the hack.

The brief takeover of Mr. Dorsey's Twitter account is a reminder of the risks facing celebrities, businesses and public officials that use Twitter. They are prominent targets for hackers and other troublemakers, but their accounts are often poorly protected and can be accessed by determined attackers.

The breach of Mr. Dorsey's account should also serve as a nudge to tech executives and everyday internet users who go online to shop, bank or simply post photos to pay close attention to the security of their online accounts.

Increasingly, protecting social media against hacking has had global political implications, and security experts have worried for several years that world leaders' accounts do not have sufficient

protections.

In 2017, President Trump's Twitter account was momentarily deactivated by a contractor with Twitter, adding grist to conservative complaints that social media companies are biased.

Although Mr. Dorsey's account was only compromised for a few minutes, it was long enough for the hackers to unleash a string of offensive messages. The posts were quickly deleted from the account.

Hackers used a messaging service called CloudHopper, which Twitter acquired in 2010, to make posts under Mr. Dorsey's name. CloudHopper allows Twitter users who link their phone number to their account to tweet simply by sending a text message to Twitter.

Twitter confirmed in a statement that the account had been compromised because Mr. Dorsey's mobile provider made "a security oversight" that allowed hackers to send tweets via text message from his phone number.

"We're aware that @jack was compromised and investigating what happened," the company said in a tweet. "There is no indication that Twitter's systems have been compromised."

The group that took over Mr. Dorsey's account called itself Chuckling Squad and posted several hashtags promoting itself, as well as a link to a chat room on the online chat service Discord. Tali Fischer, a Discord spokeswoman, said the chat room was removed minutes after it was reported.

In testimony before a Senate committee last September, Mr. Dorsey said that he used two-factor authentication to secure his account. That is a security feature that requires a person to prove their identity using a password as well as a second credential, like a code sent to the person by text message or a hardware token.

But two-factor authentication is not infallible. Hackers sometimes trick or bribe phone company employees into transferring their target's phone number to a new SIM card, which stores a phone's number.

This practice, known as SIM-swapping, allows a hacker to intercept security codes sent by text message. Previous targets of Chuckling Squad hacks, including several prominent YouTube personalities, have had their accounts compromised after the hackers took control of their phone numbers.

The San Francisco Police Department said it was aware of the threat and had been in contact with Twitter.

The hackers also posted several messages from Mr. Dorsey's account using racial slurs and praising Adolf Hitler. Twitter has frequently been criticized for not acting quickly to remove offensive and anti-Semitic content on its platform, though it removed the posts made to Mr. Dorsey's account shortly after they were posted.

The incident on Friday was not the first time that Mr. Dorsey, who is also the chief executive of the financial technology company Square, has lost control of his Twitter account. In 2016, a group of hackers going by the name OurMine conducted a similar attack that allowed them to post from Mr. Dorsey's account.

The group also took over social media accounts belonging to Sundar Pichai, the chief executive of Google, and Mark Zuckerberg, the chief executive of Facebook.

But OurMine's messages were not racist or violent. Instead, the hackers claimed they were simply testing the security practices of some of the most influential figures in the technology industry. OurMine also successfully took over a New York Times account

and posted a hoax about a missile attack.

In 2014, in one of the broadest attacks on the online activities of celebrities, the private photos of dozens of well-known women were stolen and posted to message boards like 4chan and Reddit. Four years later, a Connecticut man was sentenced to eight months in prison for his part in the incident.

Follow Kate Conger on Twitter: @kateconger

Nathaniel Popper contributed reporting from San Francisco.

Interested in All Things Tech? Get the Bits newsletter for the latest from Silicon Valley. And sign up for the personal tech newsletter for advice and tips on the technology changing how you live.

A version of this article appears in print on Aug. 31, 2019, Section B, Page 3 of the New York edition with the headline: Hackers Tweet Racial Slurs From Twitter Chief's Account. Order Reprints | Today's Paper | Subscribe