Hackers exploit Twitter security flaw

September 21 2010

Sarah Brown, wife of former British premier Gordon Brown, is one of thousands of people who have been affected by a security flaw on the social networking site Twitter. The flaw allows third-party websites to open in a Web browser just by moving the computer mouse over a link, according to an executive from computer security firm Sophos.

Twitter apologized to its millions of users on Tuesday after hackers exploited a security hole and wreaked havoc on the microblogging service.

Bob Lord, a member of Twitter's security team, said no account information was compromised in the attack, dubbed the "mouseover bug" because it was spread by users scrolling over infected links with a computer mouse.

The bug opened pop-up windows in Web browsers, linked some users to porn websites, or automatically generated the short messages known as "tweets" from a user's account.

San Francisco-based Twitter said the attack began around 2:30 am California time (0930 GMT) and was brought under control four-and-a-half hours later.

But not before thousands of users saw bizarre strings of computer code in their incoming message feed and inadvertently passed them on to other users in their list of followers.

The infected links looked like regular messages but contained lines of random computer code or were completely blacked out like a message that has been redacted.

Those hit by the bug included Sarah Brown, the wife of the former British prime minister who has over 1.1 million followers on Twitter, and White House press secretary Robert Gibbs, who has 97,000 followers.

"My Twitter went haywire," Gibbs wrote on @presssec. "Paging the tech guys."

"Don't know what everyone else got, but my bug sent me an advert for a weight loss program - as if that would work!" Brown joked at @sarahbrownuk.

Twitter's Lord explained the attack in a blog post, saying it was caused by cross-site scripting (XSS), which involves placing code from an untrusted website into another one.

"In this case, users submitted javascript code as plain text into a tweet

that could be executed in the browser of another user," he said.

Lord said Twitter had patched up a similar issue last month but it resurfaced as the result of a recent site update.

He said the initial attack involved pop-up boxes which appeared when a Twitter user hovered over an infected link with their mouse.

"Other users took this one step further and added code that caused people to retweet the original tweet without their knowledge," he said.

Lord stressed there was no need for Twitter users to change passwords "because user account information was not compromised through this exploit."

"We apologize to those who may have encountered it," he said.

Graham Cluley of computer security firm Sophos said that in Sarah Brown's case her Twitter page tried to redirect visitors to a porn site in Japan.

Cluley said the hackers behind the attacks exploited the security hole "for fun and games."

"But there is obviously the potential for cybercriminals to redirect users to third-party websites containing malicious code, or for spam advertising pop-ups to be displayed," he said.

Gibbs, the White House spokesman, told reporters the incident had not made him reconsider using Twitter.

"From time to time, I have no doubt that there will be those that want to gum up the system and things like that," he said. "I don't hesitate to

continue to use it."

Without technology "we'd all be writing on -- yes, parchment, or we'd be sending letters in the mail as press releases, which we used to do not too long ago," he said. "So, it's the vagaries of doing business."

Twitter, which allows users to pepper one another with messages of 140 characters or less, has over 145 million registered users firing off more than 90 million tweets a day, co-founder Evan Williams said recently.

Twitter unveiled a major redesign of its website a week ago that is being slowly rolled out to users of the service across the globe. The company said the attack was not connected to Twitter's revamp.

(c) 2010 AFP