Facebooks owners and executives created third party fake like and traffic networks to rig elections

- Facebook’s charges that all of the fake traffic and likes on Facebook are “Russian’s” and “Indian Rogue Programmers” is Bullshit! Facebook knew it was fake since Obama ran for office!

- Mark Zuckerberg, David Plouffe and all of the senior Facbook executives knew the traffic and likes system was fake since before 2006 and THEY ENCOURAGED IT TO RIG VOTES for Obama and Clinton!

- Facebook/Fakebook is a fraud manifested for political control as weaponized information

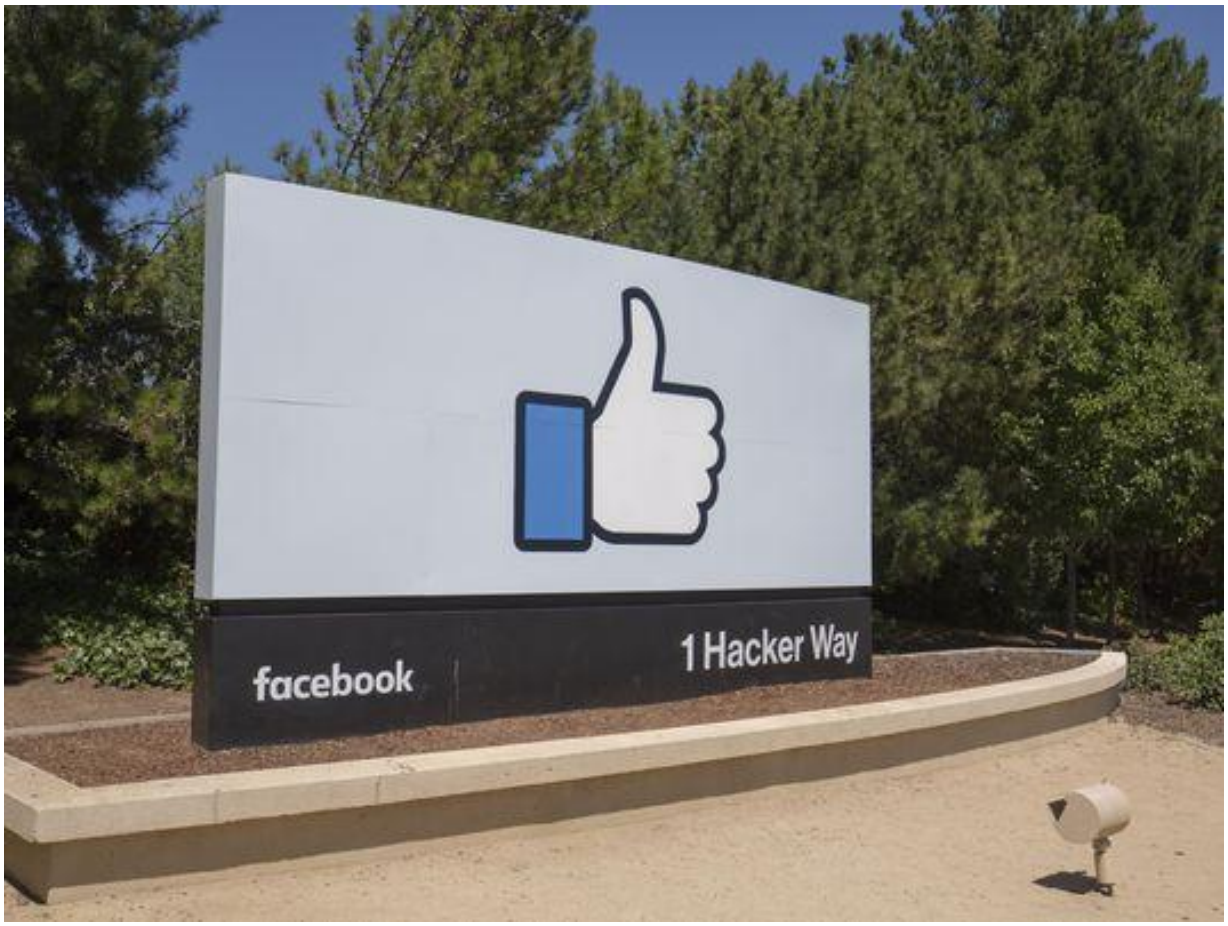
- Facebook allows fake traffic and fake likes as long as they are FOR the DNC!

Fake Facebook 'like' networks exploited code flaw to create millions of bogus 'likes'

Elizabeth Weise, USATODAY

-

A new study from the University of Iowa finds that scam artists are exploiting gaps in Facebook security to give some posts thousands of fake "likes." Buzz60

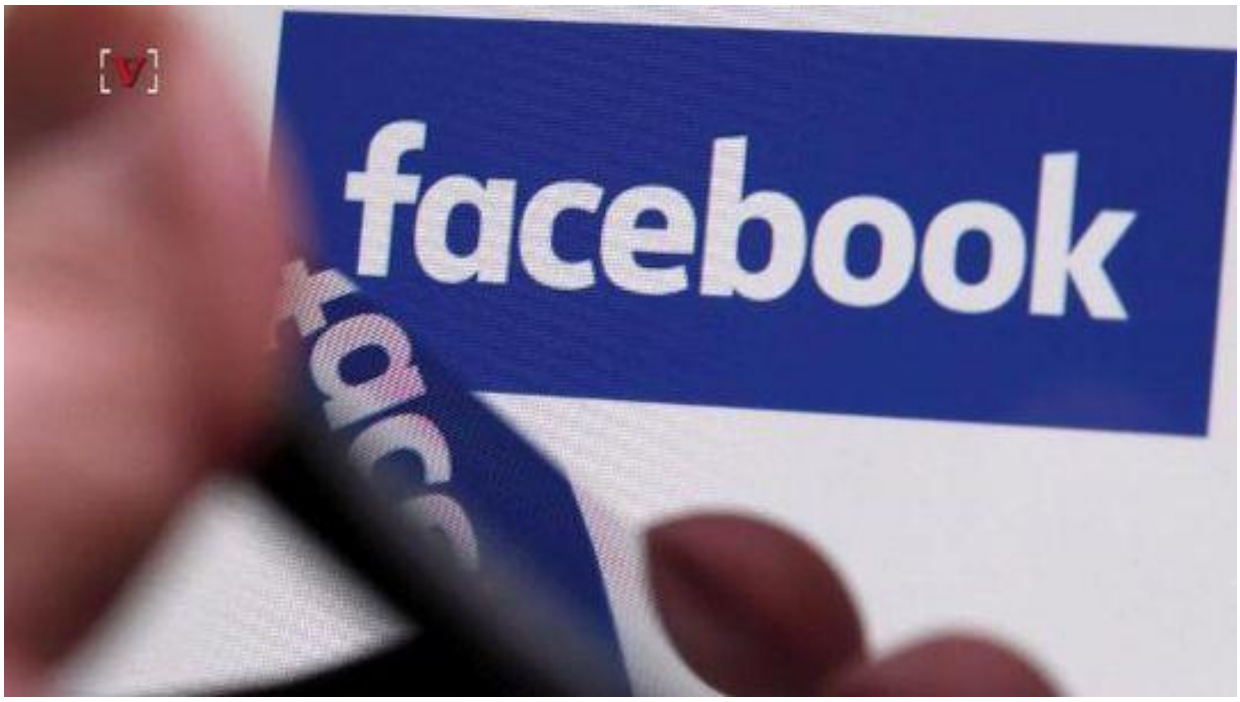


(Photo: Martin E. Klimek, USA TODAY)

1339 CONNECTTWEET 42 LINKEDIN 14 COMMENTEMAILMORE

SAN FRANCISCO — A thriving ecosystem of websites that allow users to automatically generate millions of fake "likes" and comments on Facebook has been documented by researchers at the University of Iowa.

Working with a computer scientist at Facebook and one in Lahore, Pakistan, the team found more than 50 sites offering free, fake "likes" for users' posts in exchange for access to their accounts, which were used to falsely "like" other sites in turn.



The top Democrat in the Senate who’s looking into Russian election interference is going after Facebook. Veuer's Nick Cardona (@nickcardona93) has that story. Buzz60

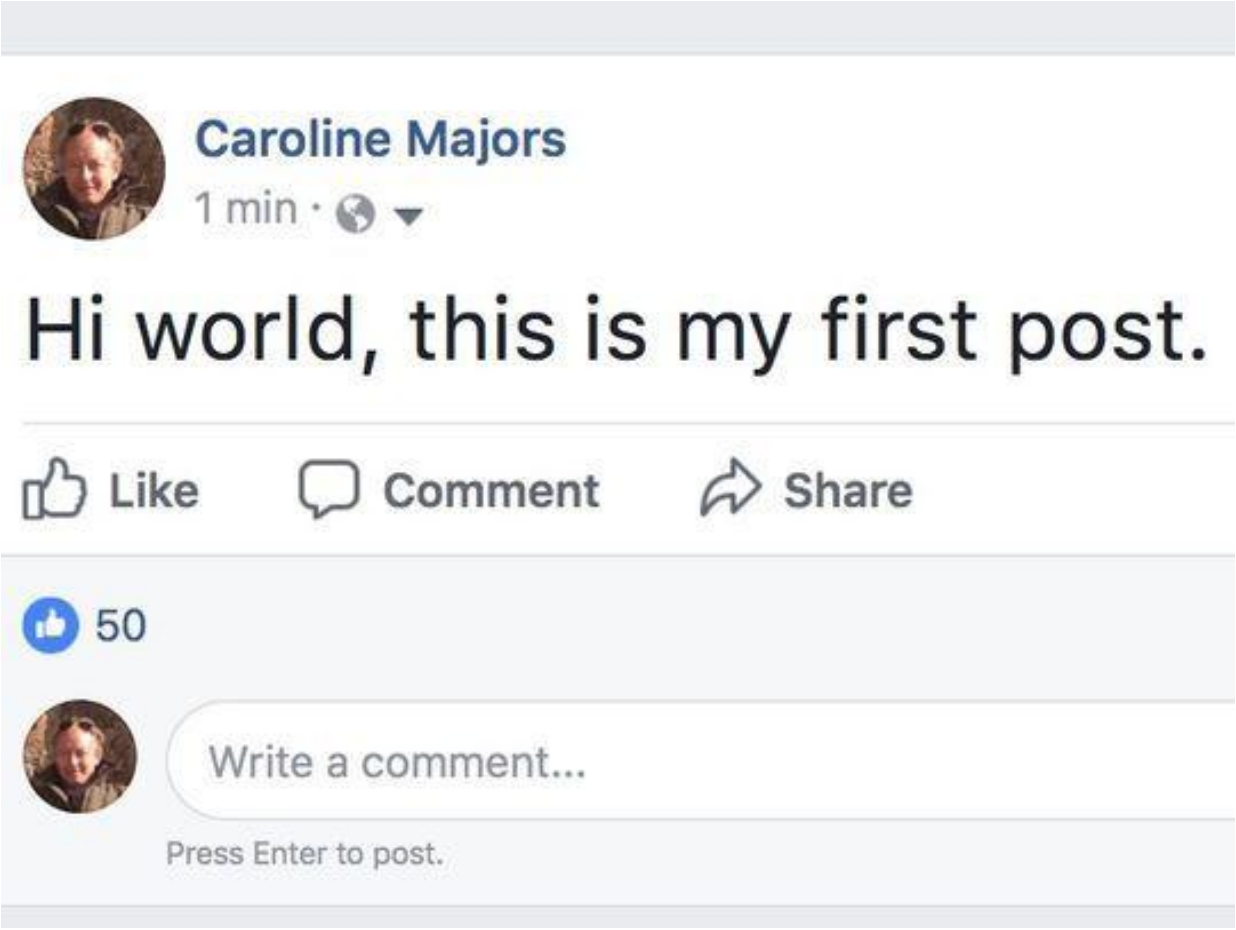
The scientists found that these “collusion networks” run by spammers have managed to harness the power of one million Facebook accounts, producing as many as 100 million fake "likes" on the systems between 2015 and 2016.

A large number of “likes” can push a posting up in Facebook’s algorithm, making it more likely the post will be seen by more people and also making it seem more legitimate.

Quid-pro-quo sites that give users points for liking a post in exchange for getting their own posts liked have long existed, violating Facebook's terms of service.

The researchers found that this activity has now been turbocharged because scam artists found a loophole to exploit code Facebook uses to allow third-

party applications such as iMovie and Spotify to access a user's Facebook account, automating a process that formerly was manual and involved many fewer likes.



Researchers at Facebook and the University of Iowa found thriving ecosystem of sites that allow members to get fake likes on their Facebook posts in exchange for turning over control of their account to the site. USA TODAY was able to get 50 likes on a post in under 1 minute using one of the reputation fraud sites. (Photo: Elizabeth Weise)

"When you become part of this network, you can say 'Give me likes on this post and as soon as you request it, you get thousands of likes on a specific post," said Zubair Shafiq, a professor of computer science at the University of Iowa in Iowa City who documented the automated networks.

Facebook said it had addressed the activity described in the research and was no longer seeing it on its platform. It is also investigating different techniques that could be used to generate inauthentic "likes" in smaller volumes and said it will take the appropriate action to help ensure that connections and activity on its service are authentic.

However at least some similar techniques still function as USA TODAY was able to join one of the networks and get 50 likes on a post to a newly-created Facebook page within one minute.

The services operate outside of the United States but hide their locations. They also disguise the fact that people who use them are engaged in activity prohibited by Facebook.

More: Facebook finds Russian ads that sought to sow division during U.S. election

More: 'It's hurt my wallet' — How one fake news publisher is faring after Facebook crackdown

More: Facebook breaks up fake account ring targeting publisher pages

More: USA TODAY asks FBI to probe rise in fake Facebook followers

Their business model is basic: They make their money by posting ads on their sites and also selling "premium" services that allow users to get even more "likes" than they allow their regular users. Some also allow users to create fake comments that can be added to the post of their choice.

The sites operate openly, and researchers found them by entering a Google search for phrases such as "Page Liker." Among the 50 so-called collusion networks listed researchers listed was djliker.com, which described itself as "a social marketing system that will increase likes, comments and increase visits to pages."

Another claims it was set up by Indonesian students, though the contact email address given doesn't work. They offer easy-to-follow instructions

and even how-to videos to walk users through signing up.

A paper outlining the research was first posted Wednesday and will be presented at the Association for Computing Machinery Internet Measurement Conference in London in November. One of the authors is Nektarios Leontiadis, a threat research scientist at Facebook.

The networks identified by these researchers do not appear to be linked to another, extensive Facebook scam involving fraudulent "likes" that Facebook said it had disrupted in April. That operation targeted popular publishers' pages with false "likes" in an attempt to gain more Facebook friends. Facebook purged millions of fake accounts connected to that scam from USA TODAY, one of the primary targets, and others.

In the Facebook hacking scam detected by the Iowa researcher, users are knowingly entering into a agreement to falsely obtain "likes." But they may not realize what they're giving up.

“Users think it’s relatively benign, but actually they’re handing over full control of their Facebook account,” said Shafiq.

“They can also access all the information that’s available on your profile, see your posts, get your friends list, even read your private messages. We can't tell if this information is being collected and sold to others,” he said.