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

September 9 2017, by Elizabeth Weise, Usa Today

A new AI tool created to help identify certain kinds of substance abuse based on a homeless youth's Facebook posts could provide homeless shelters with vital information to incorporate into each individual's case management plan. Credit: CC0 Public Domain

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 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.

"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 told USA Today that the security flaw that made it possible for these sites to exploit users' accounts had been closed. However on Thursday, 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.

Facebook did not immediately respond to a request for comment.

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.

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.

©2017 USA Today
Distributed by Tribune Content Agency, LLC.

Citation: Fake Facebook 'like' networks exploited code flaw to create millions of bogus 'likes' (2017, September 9) retrieved 25 April 2024 from https://phys.org/news/2017-09-fake-facebook-networks-exploited-code.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.