

Why buy social bots? For 'illusion of popularity,' researcher says

January 30 2018, by Allie Nicodemo



Credit: Northeastern University

On Saturday, the *New York Times* published an article detailing its investigation into Devumi, a company that sells Twitter followers to celebrities, influencers, and anyone else willing to pay for online

popularity. The purchased followers are automated social bots—fake Twitter accounts that exist solely to boost a user's follower count or perform simple tasks like retweeting. The Times reported that about 55,000 of these bots were found to be using photos stolen from the profiles of real people.

Twitter recently confirmed that more than 3,800 Russian troll accounts were created and deployed during the 2016 U.S. presidential election to confuse and mislead voters. As the influence of social bots becomes more apparent, Congress and consumers alike are calling for increased oversight.

Onur Varol, a postdoctoral research associate at Northeastern's Center for Complex Network Research, has been studying the problem of social bots for several years. His research, which was cited in the Times article, found that between 9 and 15 percent of active Twitter accounts are bots. Varol even created a platform—Botometer—that analyzes Twitter accounts and scores them based upon how likely they are to be bots. Here, Varol explains why social bots have become so prominent and why Twitter isn't doing more to combat them.

The *New York Times* article pointed out that Twitter, unlike most online platforms, doesn't require new users to complete a spam test before signing up. Why do you think that is?

I think it's a probably a platform design choice. They don't want to dismay people from using the platform, so they try to make it as easy and user-friendly as possible. At some point early on, Twitter made those choices and now it's harder for them to roll back. There is email validation, which can be easily bypassed, and then recently there is mobile phone validation. But even those mobile activations can be easily dealt with by, say, creating a Google Voice number to receive confirmation SMS during account creation.

If social bots are fake, does buying them really help people grow their online influence? After all, the purchased followers aren't real people.

The point is not to expect anything from the bot accounts. Bots accessible to regular users for purchase are not very sophisticated. The simple bot accounts might not help users directly to be more influential or visible, but they create a cognitive bias. If I see that you have 100 [followers](#) compared with 1,000 followers, it makes a difference. If I see you have 1,000 followers, I might think, 'Okay, this person is sharing something really interesting. One thousand people followed her, so I should follow her, too.' But if I see you only have 100 followers, I might think, 'Maybe this [account](#) is not worth following.'

I think those numbers are creating the illusion of popularity. This is just one of the cognitive biases affect our judgement on accounts value or usefulness. Similarly, if your tweet is favorited or retweeted by 50 bots, a real human will look at it and say, '50 people liked it, so maybe I should also share with my network so others can like the content.'

Is purchasing followers against Twitter's rules and regulations? If so, how are Devumi and its customers getting away with it?

According to Twitter's terms of service and developer agreements, the large-scale purchasing activities shouldn't be allowed. As a result of the Times article, the New York attorney general started an investigation of Devumi for impersonation and deception, which are illegal under the state's law. But the problem with these accounts is they are not really active—they just boost followers. They give visibility but they don't really act. If you look at most of the fake accounts, they either haven't

tweeted yet or they replicate other real human beings' existing accounts.

Why isn't Twitter doing more to regulate the use of social bots?

It's hard to say. I think Twitter could easily identify and deactivate bots. They have much more information and insight about user behavior, and they have better data about tweet deletions or profile changes. Practically, it's a relatively easy task for them to do.

I think the only reason Twitter is not proactive on addressing social bots is that if they say, 'On our platform, 15 percent of the accounts are bots,' that looks really bad for their investors. Their business plan relies on advertisement, they charge their customers based on the number of impressions, or the number of people who will see the ad.

I think there will eventually be more tools like Botometer to succeed in this arms-race with bot creators. Then the platforms will become more aware of the public's response to exceeding number of bots wandering in their platform and engaging randomly with their followers. If people start finding that significant fraction of their followers are fake, maybe Twitter will promise to take action. Otherwise, they won't invest on deleting accounts because it doesn't have direct effect and what they promise to their followers is more followers, more engagement, and larger networks, so they don't want to pay attention. Instead, they assume these are genuine interactions. Luckily, we have been observing more Twitter users have become aware of social bot problems and engaging with research community to help them improve their tools by providing feedback, reporting bot accounts, and using browser plug-ins and tools like Botometer to analyze their own followers.

Provided by Northeastern University

Citation: Why buy social bots? For 'illusion of popularity,' researcher says (2018, January 30)
retrieved 9 April 2024 from <https://phys.org/news/2018-01-social-bots-illusion-popularity.html>

<p>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.</p>
--