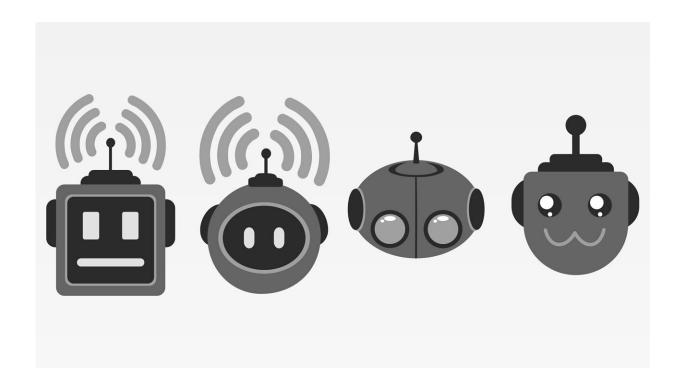


Election disinformation: How AI-powered bots work and how you can protect yourself from their influence

April 10 2024, by Nick Hajli



Credit: Pixabay/CC0 Public Domain

Social media platforms have become more than mere tools for



communication. They've evolved into bustling arenas where truth and falsehood collide. Among these platforms, X stands out as a <u>prominent battleground</u>. It's a place where disinformation campaigns thrive, perpetuated by armies of AI-powered bots programmed to sway public opinion and manipulate narratives.

AI-powered bots are automated accounts that are designed to mimic human behavior. Bots on social media, chat platforms and conversational AI are integral to modern life. They are needed to make AI applications run effectively, for example.

But some bots are crafted with <u>malicious intent</u>. Shockingly, bots constitute a significant portion of X's user base. In 2017 <u>it was estimated</u> that there were approximately 23 million social bots accounting for 8.5% of total users. More than two-thirds of tweets <u>originated from these</u> <u>automated accounts</u>, amplifying the reach of disinformation and muddying the waters of public discourse.

How bots work

Social influence is now a commodity that can be acquired by purchasing bots. Companies sell fake followers to artificially boost the popularity of accounts. These followers are available at remarkably low prices, with many celebrities among the purchasers.

In the course of our research, for example, colleagues and I detected a bot that had posted 100 tweets offering followers for sale.

Using AI methodologies and a <u>theoretical approach</u> called <u>actor-network</u> <u>theory</u>, my colleagues and I dissected how malicious social bots manipulate social media, influencing what people think and how they act



with alarming efficacy. We can tell if fake news was generated by a human or a bot with an accuracy rate of 79.7%. It is crucial to comprehend how both humans and AI disseminate disinformation in order to grasp the ways in which humans leverage AI for spreading misinformation.

To take one example, we examined the activity of an account named "True Trumpers" on Twitter.

The account was established in August 2017, has no followers and no profile picture, but had, at the time of the research, posted 4,423 tweets. These included a series of entirely fabricated stories. It's worth noting that this bot originated from an eastern European country.

Research such as this influenced X to restrict the activities of social bots. In response to the threat of social media manipulation, X has implemented temporary reading limits to curb data scraping and manipulation. Verified accounts have been limited to reading 6,000 posts a day, while unverified accounts can read 600 a day. This is a new update, so we don't yet know if it has been effective.

Can we protect ourselves?

However, the onus ultimately falls on users to exercise caution and discern truth from falsehood, particularly during election periods. By critically evaluating information and checking sources, users can play a part in protecting the integrity of democratic processes from the onslaught of bots and disinformation campaigns on X. Every user is, in fact, a frontline defender of truth and democracy. Vigilance, <u>critical</u> thinking, and a healthy dose of skepticism are essential armor.

With social media, it's important for users to understand the strategies employed by malicious accounts.



Malicious actors often use networks of bots to amplify false narratives, manipulate trends and swiftly disseminate misinformation. Users should exercise caution when encountering accounts exhibiting suspicious behavior, such as excessive posting or repetitive messaging.

Disinformation is also frequently propagated through dedicated <u>fake</u> <u>news</u> websites. These are designed to imitate credible news sources. Users are advised to verify the authenticity of news sources by cross-referencing information with reputable sources and consulting fact-checking organizations.

Self awareness is another form of protection, especially from social engineering tactics. Psychological manipulation is often deployed to deceive users into believing falsehoods or engaging in certain actions. Users should maintain vigilance and critically assess the content they encounter, particularly during periods of heightened sensitivity such as elections.

By staying informed, engaging in civil discourse and advocating for transparency and accountability, we can collectively shape a digital ecosystem that fosters trust, transparency and informed decision-making.

This article is republished from <u>The Conversation</u> under a Creative Commons license. Read the <u>original article</u>.

Provided by The Conversation

Citation: Election disinformation: How AI-powered bots work and how you can protect yourself



from their influence (2024, April 10) retrieved 21 May 2024 from https://phys.org/news/2024-04-election-disinformation-ai-powered-bots.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.