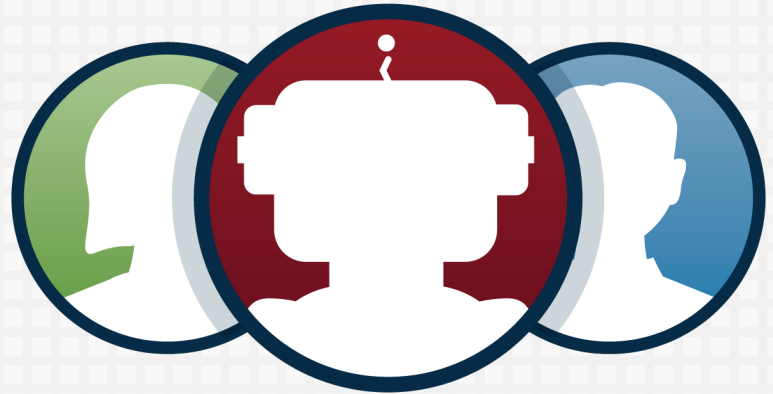# SOCIAL MEDIA BOTS

Social Media Bots are automated programs that simulate human engagement on social media platforms. As they become more prevalent and better at mimicking human behavior, the potential impacts — helpful and harmful — expand. Visit CISA.gov/MDM to learn more.

Social Media Bots use artificial intelligence, big data analytics, and other programs or databases to masquerade as legitimate users on social media. They vary depending on their function and capability: Some are helpful, like chat bots and automated notifications, but some can be used to manipulate real users. When misused, Bots can amplify disinformation and distort our perception of what's important, polluting or even shutting down online conversations.

Recognizing Bot behavior can help us respond to their attacks.

Common Attacks

Click/Like Farming
Bots inflate an account's popularity by liking or reposting its content.

Hashtag Hijacking
Bots attack an audience by leveraging the group's hashtags (e.g., using spam or malicious links).

Repost Network
Coordinated Bots ("botnet") instantly repost content from a "parent" Bot.

Sleepers
Bots wake up from long periods of dormancy to launch thousands of posts or retweets in a short time.

Astroturfing
Bots share coordinated content to give a false impression of genuine grassroots support for or opposition to an issue.

Raids
Bots swarm and overwhelm targeted accounts with spam.

Bots can be recognized by their interactions with each other and with real users. They often display:
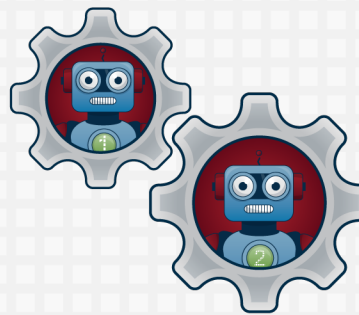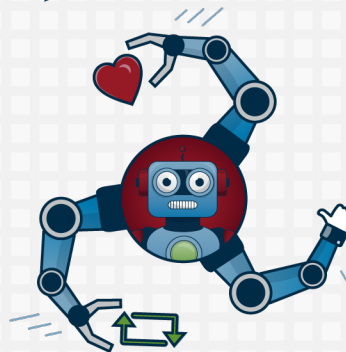
Coordinated Actions
Bots often act together, sharing similar content around the same time or frequently re-sharing each other's posts.

Repetitive and Specific Postings
Bots often post identical content and use emoticons and punctuation in more regular patterns compared to real users.

High Levels of Activity
Bots often have higher levels of activity compared to normal social media behavior, posting frequently and often sharing content without an opinion.

SOCIAL MEDIA BOTS

Social Media Bot capabilities have evolved from assisting with simple online tasks to engaging in more complex behaviors imitating human users, which bad actors use to manipulate our online interactions. Visit CISA.gov/MDM to learn more.

Social Media Bots are increasingly integrated into many of our online activities, sometimes without us even knowing. Bots vary in their functions and capabilities: Some help automate simple tasks, while more advanced Bots use artificial intelligence, big data analytics, and other programs to mimic human users. Bad actors sometimes employ Bots as part of coordinated efforts to manipulate human users.

Understanding different Bot uses can help us recognize attempts to manipulate.

Helpful Bots support:

Notifications
Automatically post an update when a trigger event occurs

Entertainment
Generate humorous content or aggregate news

Searches
Enable key word searches and detect dangerous activity

Commerce
Provide customer care or schedule posts for brands

Harmful Bots manipulate:

Popularity
Inflate follower counts and share posts to boost perception of influence

Harassment
Overwhelm or ruin reputations of targeted accounts to the point of deactivation

Scams
Phish for personal data or promote a product

Information Operations
Spread propaganda to limit free speech and manipulate democratic processes

Bad actors seeking to manipulate users on social media often employ different types of Bots as well as trolls to spread inauthentic content:

Automated Bots run purely on programming language executed without human management. They can be purchased to do simple actions and to give the impression of influence.

Semi-automated Bots allow a user to program a set of parameters but require human management, like fake accounts. These "cyborgs" are better at evading detection.

Trolls are human users, often with obscured identities, who seek to create division online. Bad actors may employ Bots in coordination with trolls.

SOCIAL MEDIA BOTS

Social Media Bots support coordinated inauthentic behavior by bad actors and threaten our ability to have important democratic discussions. Visit CISA.gov/MDM to learn more.

Social Media Bots are often one part of larger inauthentic efforts through which accounts, both human-run and automated, work in coordination to mislead people. By purchasing or setting up their own Bots, bad actors can amplify their efforts to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation.

Knowing how Bots support inauthentic activity can help us mitigate their attacks.
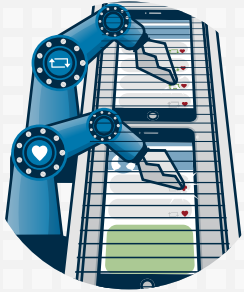
Click/Like Farming
Bots inflate popularity by liking or reposting content. The perception of influence online can translate to actual influence and distort what really matters.
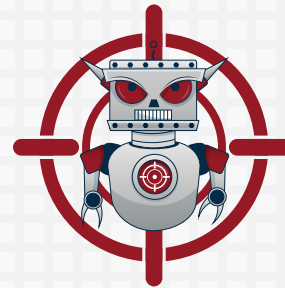
Astroturfing
Bots share coordinated content to give a false impression that there is genuine grassroots support for or opposition to an issue, making it seem more important than it is.
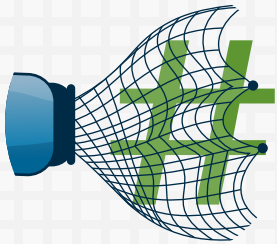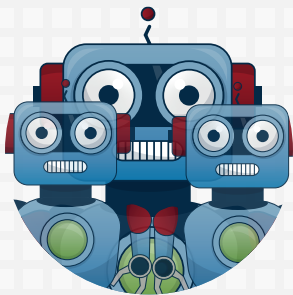
Hashtag Hijacking
Bots attack an audience by leveraging the group's hashtags (e.g., using spam or malicious links), silencing opposing opinions and chilling open discussion.
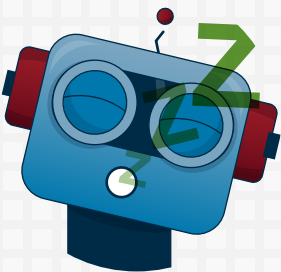
Raids
Bots swarm and overwhelm targeted accounts with spam, harassing the user and silencing opposing opinions.

Repost Network
Coordinated Bots ("botnet") instantly repost content from a "parent" Bot, flooding social media with inauthentic content that can influence public opinion and undermine facts.

As social media becomes increasingly important for connecting with each other, Bot attacks help bad actors disrupt democracy by polluting online conversations about the issues.

Undermine trust in institutions by overwhelming facts with falsehoods.

Influence our priorities by manipulating organic discussions.

Polarize us into more extreme positions that prevent healthy dialogue.

Sleepers
Bots wake up from long periods of dormancy to launch thousands of posts in a short time. The surge in attention to an issue can generate a false sense of urgency.

Suppress participation by silencing different opinions.

SOCIAL MEDIA BOTS

Although Social Media Bots try to imitate human users, some characteristics *may* be indicators of inauthentic behavior. Recognizing inauthentic behavior can increase resilience to manipulation. Visit CISA.gov/MDM to learn more.

How to Spot a Bot

1. Profile Image
May be stolen from real users, AI-generated, or a cartoon, sometimes detectable by reverse image searching.

2. Username
Contains suspicious numbers and/or irregular capitalization.

3. Bio
Contains divisive content that appeals to a target group but contains little personal information.

4. Creation Date
Account was created recently or only became active recently after a period of dormancy.

5. Followed Accounts
Account follows a high number of other accounts to build a following and may be followed by an almost identical, high number of accounts (e.g., follow for follow).

Pineapple Pizza 16
@JefniTeehooMei0973
Loves dogs, sports, and exposing the #TruthAbouttheOtherSide
USA · Joined last week
267 FOLLOWERS | 283 FOLLOWING

Pineapple Fan 22
@
Watch this video exposing the truth!

PINEAPPLE BELONGS ON PIZZA

People for Pineapple Pizza
@
how #theotherside makes me feel

Pineapple Pizza 16
@JefniTeehooMei0973
Другая сторона плохая, и ей не следует доверять. Раскройте правду! Другая сторона плохая.

↓ 50+ POSTS FROM PAST HOUR ↓

6. Coordinated Network
Frequently reposts from other suspicious accounts or shares similar content in coordination with other suspicious accounts.

7. Sharing
Reposts most content from other users rather than creating original posts, often sharing without stating an opinion.

8. Viral Content
Shares content that elicits an emotional response and is easily reposted, like memes and GIFs; spams targeted hashtags; or uses emoticons and punctuation in notable patterns.

9. Erratic Behavior
Shares content about many unrelated topics or changes interests and behavior suddenly, such as randomly posting in a new language.

10. Hyperactive
Shares a large amount of content, sometimes nonstop around the clock or spiking at certain times.