

Guide 1: Understanding Bots — What NGOs Need to Know

BOTS.NGO

Executive Summary

Bots — automated software programs that perform tasks at speed and scale that no human team could replicate — are now embedded in nearly every digital environment that civil society organizations inhabit. As of recent estimates, 62 percent of all internet traffic is generated not by humans but by programs acting autonomously: analyzing information, spreading messages, finding vulnerabilities, and interacting with users. Up to 48 million Twitter/X accounts are estimated to be bots. And the sophistication of these automated agents is increasing rapidly: modern AI-powered bots can generate human-like text, hold coherent conversations, and create realistic personas that are increasingly difficult to detect and distinguish from real human accounts.

For NGOs, this reality cuts in two directions. On one hand, bots and automation tools offer extraordinary opportunities: helping citizens register to vote, contact elected officials, translate content for global audiences, respond to supporter inquiries 24 hours a day, monitor legislation and media, and analyze large data sets that would overwhelm any human team. On the other hand, bots pose significant risks: they are used by political operatives and foreign governments to spread misinformation, manufacture the appearance of grassroots support (astroturfing), flood regulatory processes with fake public comments, and amplify harassment campaigns against civil society organizations and their staff.

This guide provides NGO leaders, communications staff, technology managers, and campaign teams with a comprehensive grounding in what bots are, how they work, what opportunities they create, and what risks they pose. It is the foundation for Guides 2 and 3, which cover how to deploy bots responsibly and how to protect your organization from malicious bot activity. The guide synthesizes research from the Stanford Social Innovation Review, the Ford Foundation, the Brennan Center, NIH, and leading civil society technology practitioners.

Key takeaway: Bots are neither good nor bad — they are powerful. NGOs that understand them can leverage their benefits while protecting against their harms. NGOs that ignore them are already operating in a bot-influenced environment without the knowledge to navigate it safely.

Evidence Table: Key Findings, Strength, and NGO Implications

Key Finding	Evidence Strength	NGO Implications
62% of all internet traffic is generated by bots and automated programs, not human users.	Moderate — widely cited estimate from digital security research	NGOs are operating in a bot-saturated environment whether they choose to or not. Understanding this is baseline knowledge for any digital strategist.
During the 2016 U.S. election, just 6% of Twitter accounts — likely bots — were responsible for spreading 31% of the low-credibility information on the platform.	Strong — Indiana University research, widely replicated	Misinformation spread by bots directly threatens the information environments NGOs depend on for public engagement and policy influence. Build media literacy into all communications work.
In 2017, bots flooded the FCC with more than 1 million fake public comments opposing net neutrality, subverting the regulatory process.	Strong — Brennan Center documentation; FCC investigation	NGOs using regulatory comment processes must be aware that these systems are vulnerable to bot-flooding. Advocate for transparency and verification requirements in regulatory comment systems.
AI-powered bots can generate human-like text and realistic personas that are increasingly difficult to detect.	Strong — RAND research (2025); BBC reporting (2026); academic literature	The "is this a human?" question is no longer reliably answerable. NGOs must develop detection heuristics and maintain skepticism about apparent grassroots activity that emerges suddenly and at scale.
Early adopter NGOs have used bots to automate civic engagement — helping citizens register to vote, contact elected officials, and translate content at scale.	Strong — SSIR (2018); Ford Foundation; multiple practitioner case studies	Legitimate NGO use of bots for civic engagement is well-established and effective. The question is not whether to use automation, but how to do so ethically and transparently.
Swarms of AI bots can measurably shift people's beliefs and political opinions through repeated, coordinated exposure to particular narratives.	Emerging — The Conversation (2026); academic research on synthetic consensus	NGOs working on public opinion change must understand that bot-generated "synthetic consensus" can make fringe positions appear mainstream, undermining authentic advocacy efforts.
Not all automation is malicious — outright bans on bots are neither practical nor desirable, and would eliminate many socially valuable applications.	Strong — Policy Options analysis; SSIR	Advocate for transparency and accountability frameworks, not blanket bans. Support disclosure requirements and platform verification systems that distinguish legitimate from malicious bots.

Step-by-Step Framework

Step 1: Build Organizational Literacy About Bots

The most important first step for any NGO is ensuring that key staff — particularly in communications, campaigns, technology, and leadership — have a working understanding of what bots are and how they operate. This does not require technical expertise; it requires conceptual clarity about the different types of bots, their capabilities, and the environments in which they operate.

There are three broad categories of bots relevant to NGO work. First, beneficial automation tools: software programs that perform repetitive or scalable tasks on behalf of the NGO, such as email marketing automation, social media scheduling, chatbots on the NGO's website, voter registration tools, or legislative monitoring alerts. Second, neutral or ambiguous bots: programs that operate in digital spaces where the NGO is active but are not specifically targeting the NGO — social media algorithms, search engine crawlers, and content aggregators. Third, adversarial bots: programs operated by bad actors to spread misinformation, manufacture false consensus, amplify harassment, or flood regulatory and comment systems with inauthentic activity. NGOs need to understand all three categories to navigate their digital environment effectively.

Step 2: Map Your Digital Ecosystem for Bot Exposure

Conduct a simple audit of all the digital spaces where your NGO operates or relies on for information. For each space, assess: How bot-saturated is this environment? Which types of bot activity pose the greatest risk to our work? What beneficial automation tools are we already using, and are they operating with appropriate human oversight?

Social media platforms are the most obvious bot-saturated environment, but they are not the only one. Email inboxes are targets for bot-generated spam and phishing. Regulatory comment systems (as the FCC case demonstrated) are targets for bot-flooding. Petition platforms can be gamed by bots to manufacture apparent support. Media monitoring tools can be fooled by bot-generated content that appears to be organic coverage. Website analytics can be distorted by bot traffic. Map each of these exposure points and assess the current risk level.

Step 3: Understand the Specific Risks to Civil Society

Civil society organizations face a distinctive risk profile from adversarial bots that differs from the risks facing businesses or governments. First, NGOs are particularly vulnerable to coordinated bot harassment campaigns: when an NGO takes a controversial position on a politically charged issue, it may become the target of bot-amplified harassment against its staff, flooding their inboxes and social media accounts with abuse and making normal work impossible. Second, NGOs working on politically sensitive issues are vulnerable to disinformation campaigns in which bot networks spread false narratives about the organization's work, funding, or motives — narratives that can spread faster than the NGO can respond. Third, NGOs that rely on regulatory processes, public comment periods, or consultative procedures are vulnerable to bot-flooding that drowns out authentic civil society voices.

Understanding these specific risk vectors is essential before building defensive strategies. Not all NGOs face the same risks: an animal rights organization working on corporate campaigns faces different bot risks than a democracy organization working on voter registration, which faces different risks than a human rights organization working in a politically repressive country.

Step 4: Distinguish Legitimate from Malicious Automation

One of the most important conceptual distinctions in the bot landscape is between transparent, human-authorized automation and deceptive, covert automation. NGOs themselves use automation tools all the time — email marketing systems, social media schedulers, website chatbots, legislative tracking services. These are legitimate automation tools because: (1) they are authorized by the organization; (2) their automated nature is either disclosed or widely understood; and (3) they do not deceive users about whether they are interacting with a human or a program.

Malicious bots, by contrast, typically involve deception: fake personas, hidden operators, and manufactured authenticity. The distinction matters because it means the answer to bot misuse is not to ban all automation, but to require transparency, accountability, and human authorization. NGOs should advocate for disclosure requirements — platforms requiring bots to be labeled as bots — and should model those practices in their own use of automation tools.

Step 5: Develop a Bot Policy for Your Organization

Every NGO should have a written policy governing its own use of automation tools. This policy does not need to be long or technically complex, but it should address: Which automation tools does the organization use and for what purposes? What disclosure practices apply — do we tell users when they are interacting with a bot? What human oversight exists over automated systems — who is responsible for monitoring and correcting bot behavior? What are the ethical limits on our use of automation — what would we never use a bot for, regardless of effectiveness? How does the policy apply to campaign partners and vendors who act on our behalf?

The National Eating Disorders Association's experience in 2023 — when its AI chatbot gave harmful advice to people seeking help with eating disorders, forcing a rapid shutdown and generating significant reputational damage — illustrates what happens when automation tools are deployed without adequate policy, oversight, and testing. A written policy, reviewed annually and enforced through vendor contracts and staff training, is the first line of defense.

Step 6: Build Detection and Response Capacity

Regardless of whether your NGO uses bots itself, you need the capacity to detect when adversarial bots are targeting your organization or distorting the information environments in which you operate. Basic detection capacity includes: monitoring for sudden spikes in social media mentions or hashtag activity (often a sign of bot amplification); being aware of coordinated posting patterns (many accounts posting the same message within minutes of each other); checking the account age and activity history of accounts engaging with your content; and using tools like Botometer, which scores Twitter/X accounts on their likelihood of being automated.

Response capacity includes: having a communications plan for bot-amplified harassment or disinformation campaigns; maintaining relationships with platform trust-and-safety teams

who can respond to reports of coordinated inauthentic activity; and having a designated staff member with responsibility for monitoring and escalating bot-related incidents. The most important principle: do not respond to bot-amplified harassment by engaging with each individual bot account — this amplifies rather than suppresses the campaign. Instead, respond through authentic channels (your own media, partner networks, direct supporter communication) and report the coordinated activity to the platform.

Step 7: Engage Policy and Advocacy on Bot Governance

NGOs have a direct stake in how bots are governed, both as organizations that are affected by bot activity and as representatives of civil society interests in public policy spaces. Across democracies, governments are grappling with how to regulate bots: requiring disclosure, imposing liability for bot-generated harms, creating verification requirements for high-volume automated accounts, and protecting regulatory processes from bot-flooding.

Engage in these policy debates actively. Advocate for transparency and disclosure requirements, not blanket bans. Support platform accountability measures that require social media companies to enforce their terms of service against coordinated inauthentic activity. Push for the protection of regulatory comment processes through verification requirements that preserve the voice of authentic civil society while shutting out bot-generated fake comments. NGOs' credibility in these debates depends on their own transparent and ethical use of automation tools — practice what you advocate.

Tools & Templates

Bot Exposure Audit Template: A spreadsheet listing all digital platforms and systems the NGO uses, with columns for: bot activity level (low/medium/high), type of bot risk (misinformation, harassment, comment flooding, analytics distortion), current detection capacity, and priority for additional protection.

Organizational Bot Policy Template: A one-to-two page policy document covering: approved automation tools and their purposes, disclosure practices, human oversight requirements, ethical limits, and vendor/partner compliance requirements. Reviewed annually.

Bot Detection Checklist: A quick-reference card for communications and campaign staff listing the key indicators of bot activity: sudden follower spikes, coordinated posting patterns, low-age accounts, repetitive content, fake profile indicators. Post near workstations.

Incident Response Plan: A pre-written plan specifying: who to notify when bot-amplified harassment or disinformation is detected, what actions to take (reporting, authentic response, platform escalation), and what to avoid (don't engage with individual bots, don't escalate the bot's narrative).

Vendor Bot Assessment Questionnaire: A short questionnaire for any vendor or partner deploying automation tools on the NGO's behalf. Questions: What automated tasks does your tool perform? Does it disclose its automated nature to users? What data does it collect? What human oversight is in place? How are errors identified and corrected?

Staff Bot Literacy Training Module: A 45-minute facilitated session (or slide deck for async delivery) covering: what bots are, the three categories relevant to NGO work, real case examples of both beneficial and harmful bot activity, and how to use the detection checklist.

Case Vignettes

Vignette 1: The FCC Net Neutrality Bot Flood (2017)

In 2017, during a Federal Communications Commission (FCC) public comment period on net neutrality rules, bots flooded the agency with more than 1 million fake comments — nearly all from fake constituents calling for the repeal of net neutrality protections. The campaign was discovered only because hundreds of thousands of comments were uncannily similar, revealing the automated origin. But the discovery came too late to prevent the comments from initially being treated as authentic public input.

The case has direct relevance to NGOs that participate in regulatory comment processes and depend on those processes to give civil society a voice in policy decisions. If bot-generated fake comments can drown out authentic civil society submissions, the entire regulatory consultation process — which NGOs depend on as a legitimate channel for influencing policy — is undermined. The Brennan Center has since documented that, as AI tools grow more sophisticated, the problem of bot-generated fake regulatory comments is becoming harder to detect and more difficult to attribute.

Lessons learned: (1) Regulatory comment processes are vulnerable to bot-flooding and cannot be assumed to accurately represent public opinion. (2) Advocate for verification requirements in regulatory processes. (3) When submitting formal comments, use your organization's letterhead, provide verifiable organizational details, and make your submission as distinctive and substantive as possible — the opposite of what bots produce.

Vignette 2: Charity:Water's "Walk with Yeshi" AI Chatbot Campaign

Charity:water, a U.S.-based organization advocating globally for clean drinking water, developed an AI chatbot for their fundraising campaign "Walk with Yeshi" — a chatbot that told the story of Yeshi, a young woman from Ethiopia, through Facebook Messenger, incorporating conversation, geolocation, and multimedia content. Through sophisticated storytelling, many people were emotionally engaged and supported the campaign, with funds raised helping build over 100 wells.

The case illustrates the potential of transparent, mission-aligned automation to create meaningful human connection and real-world impact — the opposite of the deceptive bot activity discussed in Vignette 1. The key differences: the automation was authorized by the organization, served the mission directly, created genuine value for users, and involved human oversight throughout. The chatbot's automated nature was not hidden; it was part of the creative concept.

Lessons learned: (1) Transparent, mission-aligned automation can create genuine human connection and measurable impact. (2) The ethical line is between automation that serves

users with their knowledge and authorization versus automation that deceives users. (3) This level of chatbot sophistication requires significant technical expertise or budget — be realistic about your organization's capacity before attempting complex conversational AI campaigns.

Metrics & KPIs

Metric	What It Measures	How to Track
Bot exposure audit completion	Whether all digital platforms have been assessed for bot risk	Annual audit completion date; audit document
Organizational bot policy adoption	Whether a written policy exists and is current	Policy document version date; staff acknowledgment
Bot detection incidents identified	Number of bot-related incidents detected (adversarial activity)	Incident log maintained by communications team
Staff bot literacy completion rate	Percentage of relevant staff who have completed training	Training attendance records
Vendor compliance rate	Percentage of automation vendors who have completed the assessment questionnaire	Procurement records
Regulatory comment process engagement	Whether the NGO actively engages in relevant regulatory processes with substantive submissions	Activity log
Platform trust-and-safety reports filed	Engagement with platform reporting systems for coordinated inauthentic activity	Incident log

Risks & Mitigations

Risk: Beneficial automation tools causing harm through inadequate oversight. The National Eating Disorders Association experience (2023) shows that AI chatbots deployed without adequate oversight can cause direct harm and serious reputational damage.

Mitigation: Implement the vendor bot assessment questionnaire for all automation tools. Require human oversight protocols. Pilot all chatbots with staff before public deployment. Maintain easy escalation pathways to human staff.

Risk: NGO's own automation tools being perceived as astroturfing. If an NGO uses automation to amplify its message in ways that obscure the automated origin, it risks being accused of the same deceptive practices it opposes.

Mitigation: Disclose automation use. Be transparent about which elements of your digital presence are automated. Build a reputation for authentic engagement that makes your organization's voice credible.

Risk: Bot-amplified harassment overwhelming staff capacity. Coordinated harassment campaigns targeting staff (particularly women and people of color) can make normal work impossible and cause serious personal harm.

Mitigation: Develop an incident response plan before any incident occurs. Train all staff on

how to recognize and report coordinated harassment. Build relationships with platform trust-and-safety teams. Prepare organizational support protocols for targeted staff.

Risk: Synthetic consensus distorting your organization's strategic decisions. If your organization monitors social media to understand public opinion, bot-generated synthetic consensus can make fringe positions appear mainstream — leading to strategic miscalibration. **Mitigation:** Develop protocols for distinguishing bot-amplified content from authentic public opinion. Use multiple sources of public opinion data, not only social media monitoring. Maintain healthy skepticism about sudden apparent shifts in public discourse.

Implementation Checklist

- ☐ Complete bot exposure audit across all digital platforms
- ☐ Develop and adopt organizational bot policy
- ☐ Train all relevant staff using the bot literacy training module
- ☐ Complete vendor bot assessment questionnaire for all current automation vendors
- ☐ Set up bot detection monitoring (Botometer or equivalent for social media)
- ☐ Develop incident response plan for bot-amplified harassment or disinformation
- ☐ Establish relationship with platform trust-and-safety contacts
- ☐ Review regulatory comment processes for bot-flooding vulnerability
- ☐ Advocate for bot disclosure and transparency in at least one relevant policy forum
- ☐ Schedule annual bot policy review and audit refresh

Glossary

Bot: A software program that automates tasks on the internet, from helpful automation (scheduling, monitoring, customer service) to malicious activity (spreading misinformation, manufacturing false consensus). Short for "robot."

Chatbot: A bot designed to conduct text- or voice-based conversations with users, simulating human interaction. Used by NGOs for donor FAQ, information provision, and campaign storytelling. Can cause harm if deployed without adequate oversight.

Astroturfing: The use of bots or coordinated inauthentic accounts to manufacture the appearance of genuine grassroots support for a position or cause. Named for the artificial grass brand Astroturf.

Coordinated inauthentic behavior (CIB): A term used by social media platforms to describe organized efforts to manipulate public discourse using fake or compromised accounts, often bot-driven. Facebook/Meta has used CIB as a key enforcement standard.

Synthetic consensus: The manufactured appearance of widespread agreement with a particular position, created by bot networks posting the same message from many accounts. Can shift genuine public opinion by making fringe positions seem mainstream.

Bot farm: An organized network of computers or mobile devices running bot software, often operated by state actors, political operatives, or criminal groups for the purpose of social media manipulation.

Botometer: A tool developed by Indiana University that analyzes Twitter/X accounts and scores them on the likelihood that they are automated bots.

AI-powered bot: A bot using machine learning and natural language processing to generate human-like responses that are difficult to distinguish from authentic human communication.

Disclosure: The practice of clearly indicating to users when they are interacting with an automated system rather than a human. The ethical foundation of legitimate bot use.

Human-centered automation: An approach to automation, articulated by technology consultants including Beth Kanter, in which automated systems are designed to augment human capacity rather than replace human judgment, with clear human oversight and escalation pathways.

Agentic AI: A class of AI systems that can take autonomous actions on behalf of an organization — browsing the web, filing forms, sending messages — with minimal human oversight for each action. An emerging area of NGO technology adoption requiring careful governance.

References

1. Stanford Social Innovation Review. (2018). Leveraging the Power of Bots for Civil Society. ssir.org
2. Ford Foundation. (2026). Why You Should Care About Bots If You Care About Social Justice. fordfoundation.org
3. Brennan Center for Justice. (2023). Artificial Intelligence, Participatory Democracy, and Responsive Government. brennancenter.org
4. Alliance for Peacebuilding / Toda Peace Institute. (2018). Civil Society in the Age of Automation. toda.org
5. Kanter, B. & Fine, A. (2020). The Smart Nonprofit: Staying Human-Centered in an Automated World.
6. The Conversation. (2026). Swarms of AI Bots Can Sway People's Beliefs — Threatening Democracy. theconversation.com
7. PMC / NIH. (2021). Bots and Misinformation Spread on Social Media. pmc.ncbi.nlm.nih.gov
8. BBC World Service. (2026). How Bots Manipulate Social Media. bbc.com
9. Policy Options (IRPP). (2025). Minimize Harmfulness of Bots, But Don't Ban Them. policyoptions.irpp.org
10. FundraisingBox. (2025). 3 Examples: Fundraising Campaigns with AI. fundraisingbox.com
11. ThinkPic. (2025). How to Use A.I. Effectively and Protect Your Organization's Reputation and Values. thinkpic.org

12. Constructive. (2025). Ethical AI: 9 Resources and Best Practices for Nonprofits.
constructive.co