MCMASTER CHILD HEALTH CONFERENCE

Bot-ched Data: Dealing with Bots and Bad Actors in Online Autism Research

SAMANTHA RUTHERFORD [1], MACKENZIE SALT PHD[2]
[1] BACHELOR OF HEALTH SCIENCES (HONOURS), CHILD HEALTH SPECIALIZATION, MCMASTER UNIVERSITY
[2] OFFORD CENTRE FOR CHILD STUDIES, MCMASTER UNIVERSITY

BACKGROUND

There is a recent and dangerous threat to online research and data collection: bots and bad actors. Bots (artificial intelligence (AI)) and bad actors (human participants who do not truthfully complete surveys) are growing in their strength and numbers when it comes to infiltrating studies. In the field of autism research, these present additional barriers to an already underrepresented population. As these fraudulent participants continue to evolve past current methods which aim to combat them, it is imperative researchers consider all options of prevention, detection, and elimination, without compromising their survey's integrity or increasing participation barriers for valid participants.

OBJECTIVE

To synthesize current reviews of bot and bad actor prevention, detection, and elimination from online research surveys.

METHODS

A search of major databases was conducted for independent studies and reviews, resulting in 19 papers found to be most applicable. The literature was then summarized by what methods of bot and bad actor prevention, detection, and elimination were explored, how authors used each method, and the effectiveness of these.

RESULTS

The search resulted in 19 articles, 12 of which were independent studies which explained authors firsthand experiences dealing with bots and bad actors [1-12]. The remaining 7 were reviews which assessed common strategies for bot/bad actor prevention, detection, and elimination [13-19]. Of the independent studies, 2 focused on dealing with bad actors, 1 focused on bots, and 9 focused on both. For the reviews, none focused solely on bad actors, 1 focused on bots, and 6 discussed dealing with both.

Across these articles, 64 distinct methods were identified as strategies, however 11 of these were discussed most frequently.

(1) CAPTCHA

CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart". This tool can detect bots in research surveys by employing various methods such as image recognition tasks. While effective in combination with other measures against bots, it may not be foolproof, as bots are evolving to bypass CAPTCHAs [1,3,6-10,13-16].

(2) Email Screening
Email screening involves the verification of email addresses to authenticate research participants. While successful in identifying some fraudulent activities, it is susceptible to bots and bad actors using valid email addresses. Its efficacy is contingent upon the overall implementation of complementary measures [1,3,5, 11,15,16].

(3) IP Address Tracking
An IP address is a unique number which identifies any device accessing the internet. Tracking IP addresses can be useful to identify participants who attempt to complete surveys multiple times or used to block specific addresses. This method demonstrates moderate effectiveness by identifying repeat entries and geographic inconsistencies but faces limitations with VPNs (virtual private network; masks a user's IP address) and dynamic IP addressing (a temporary IP address which continually changes over time) [3-6,8,10-16,18].

(4) Consistency Checks
Consistency checks involve analyzing response coherence, for example, asking "how old are you" at the start of the survey and later "what year were you born". An inconsistency in responses to these can point towards fraudulent participation. While showing potential for detecting AI and bad actor responses, effectiveness is not consistently defined across articles [2,3,8,10,11,13,15,16].

(5) Timestamp Analysis
Examining survey completion times and response durations proves useful in detecting suspicious activity such as extremely rapid response times. Although, this may not account for atypical response times in human participants across diverse and inclusive study populations [1-3,6,11,13-15,17].

(6) Attention Checks
Attention checks request specific actions, such as leaving a question unanswered or selecting a particular answer option. These are shown to be moderately effective, though they may be incorrectly answered by valid respondents, emphasizing the need for integration with other strategies [3,7,8,10,12-15].

(7) Two-Step Opt-In
Two-step opt-in processes require multiple steps from participants before they may enter the study. For example, pre-screening potential participants followed by unique survey links sent to those deemed valid. This aims to limit public access compared to surveys posted on more public platforms. Effectiveness does vary based on other strategies used and potential link exposure by scammers [1,4,6,7,9,11,14,15].

(8) Collection of Contact Information
The collection of personal contact information including phone numbers and physical addresses is varied in its effectiveness, relying heavily on proper integration with other validation techniques to ensure participant authenticity [4,9,14,16,17].

(9) Clarifying Compensation Rules
Compensation is often an incentive for bot and bad actor infiltration. Clarifying compensation rules can prevent fraud by explaining compensation policies and only offering compensation post-data verification. Its direct impact on reducing bot responses is not explicitly quantified, though public compensation advertisements are noted to increase fraudulent participation [5,7,9,14-16].

(10) Domain Knowledge Assessment
Domain knowledge assessment is the evaluation of participants' knowledge related to survey content. For example, asking participants in an autism study to explain their lived experience. This method yields varied results as part of an anti-fraud strategy and it may pose challenges for certain populations [3,10,14].

(11) Interviews Pre- and Post-Data Collection
Interviews conducted pre- and post-data collection (i.e. prospectively or retrospectively), exhibit high efficacy in preventing bot participants and eliminating bot respondents. This strategy is also effective in deterring and detecting bad actors. However, interviews may deter eligible individuals and can remove anonymity [2,5,12,16].

CONCLUSIONS

Current strategies employed to tackle bots and bad actors in online autism research is a complex and nuanced landscape. A synthesis of 19 relevant studies revealed several distinct approaches. However, none of these methods are completely effective in isolation. This emphasizes the necessity to combine multiple strategies to enhance their overall efficacy.

Another recurring concern surfaces throughout the discussion: the imminent obsolescence of current strategies in the face of rapidly evolving AI capabilities. While these methods can have effective outcomes, the relentless progress of AI technologies poses a formidable challenge to their sustainability. Thus, it becomes evident that a dynamic and adaptable approach is needed. Researchers across disciplines must collaborate to find novel method combinations and novel strategies.

As the use of online questionnaires in all research—especially studies on autism and other underrepresented populations—continues to grow, it is increasingly important to keep participation barriers low while collecting valid data.

MCMASTER CHILD HEALTH CONFERENCE

QR Code to Full Research Poster:

1. Pozzar R, Hammer MJ, Underhill-Blazey M, Wright AA, Tulsky JA, Hong F, et al. Threats of Bots and Other Bad Actors to Data Quality Following Research Participant Recruitment Through Social Media: Cross-Sectional Questionnaire. Journal of Medical Internet Research. 2020 Oct 7;22(10):e23021.
2. Gonzalez JM, Grover K, Leblanc TW, Reeve BB. Did a bot eat your homework? An assessment of the potential impact of bad actors in online administration of preference surveys. PLOS ONE. 2023 Oct 5;18(10):e0287766.
3. King-Nyberg B, Thomson EF, Morris-Reade J, Borgen R, Taylor C. The Bot Toolbox: An Accidental Case Study on How to Eliminate Bots from Your Online Survey. Journal for Social Thought. 2023 Sep 18;7(1).
4. Godinho A, Schell C, Cunningham J. Out Damn Bot, Out: Recruiting Real People into Substance Use Studies on the Internet. Substance Abuse. 2019 Dec 10;41:1–3.
5. Pellicano E, Adams D, Crane L, Hollingue C, Allen C, Almendinger K, et al. Letter to the Editor: A possible threat to data integrity for online qualitative autism research. Autism. 2023 May 22;13623613231174543.
6. Wang J, Calderon G, Hager ER, Edwards LV, Berry AA, Liu Y, et al. Identifying and preventing fraudulent responses in online public health surveys: Lessons learned during the COVID-19 pandemic. PLOS Global Public Health. 2023 Aug 23;3(8).
7. Yarrish C, Groshon L, Mitchell J, Appelbaum A, Klock S, Winternitz T, et al. Finding the Signal in the Noise: Minimizing Responses From Bots and Inattentive Humans in Online Research. 2019 Oct 1;42:235.
8. Moss AJ, Rosenzweig C, Jaffe SN, Gautam R, Robinson J, LItman L. Bots or inattentive humans? Identifying sources of low-quality data in online platforms. 2021 Jun 11.
9. Bybee S, Cloyes K, Baucom B, Supiano K, Mooney K, Ellington L. Bots and nots: Safeguarding online survey research with underrepresented and diverse populations. Psychology & Sexuality. 2021 May 28;13.
10. Zhang Z, Zhu S, Mink J, Xiong A, Song L, Wang G. Beyond Bot Detection: Combating Fraudulent Online Survey Takers. Proceedings of the ACM Web Conference 2022. 2022 Apr 25;699–709.
11. Goodrich B, Fenton M, Penn J, Bovay J, Mountain T. Battling bots: Experiences and strategies to mitigate fraudulent responses in online surveys. Applied Economic Perspectives and Policy. 2023;45(2):762–84.
12. Kennedy C, Hatley N, Lau A, Mercer A, Keeter S, Ferno J, et al. Assessing the Risks to Online Polls From Bogus Respondents. Pew Research Center. 2020 Feb 18.
13. Kennedy R, Clifford S, Burleigh T, Waggoner PD, Jewell R, Winter NJG. The shape of and solutions to the MTurk quality crisis. Political Science Research and Methods. 2020;8(4):614–29. doi:10.1017/psrm.2020.6
14. Lawlor J, Thomas C, Guhin AT, Kenyon K, Lerner MD, Drahota A. Suspicious and fraudulent online survey participation: Introducing the REAL framework. Methodological Innovations. 2021;14(3).
15. Storozuk A, Ashley M, Delage V, Maloney EA. Got Bots? Practical Recommendations to Protect Online Survey Data from Bot Attacks. TQMP. 2020 May 1;16(5):472–81.
16. Teitcher JEF, Bockting WO, Bauermeister JA, Hoefer CJ, Miner MH, Klitzman RL. Detecting, Preventing, and Responding to "Fraudsters" in Internet Research: Ethics and Tradeoffs. J Law Med Ethics. 2015;43(1):116–33.
17. Pequegnat W, Rosser BRS, Bowen AM, Bull SS, DiClemente RJ, Bockting WO, et al. Conducting Internet-based HIV/STD prevention survey research: considerations in design and evaluation. AIDS Behav. 2007 Jul;11(4):505–21.
18. Reips UD, Buchanan T, Krantz J, Mcgraw K. Methodological challenges in the use of the internet for scientific research: ten solutions and recommendations. Studia Psychologica. 2016 Sep 20;14:139.
19. Hulland J, Miller J. "Keep on Turkin'"? J of the Acad Mark Sci. 2018 Sep 1;46(5):789–94.