# Canadian Oncology Nursing Journal

# Revue canadienne de soins infirmiers en oncologie

Volume 35, Issue 1 • Winter 2025
eISSN: 2368-8076

CANO ACIO
Canadian Association of Nurses in Oncology
Association canadienne des infirmières en oncologie

RESEARCH REFLECTION

# Battling the bots: Mitigating malicious responses in oncology nursing research

by Lorelei Newton, Claire Fullerton, Helen Monkman

Nursing research is vital to the creation and translation of evidence to inform practice, policy and guidelines. As researchers, we are also committed to upholding the integrity of nursing research, as well as supporting our research colleagues. In this spirit, we share our recent survey experience and thinking about a new threat to research integrity with troubling implications.

Chatbots, or computer programs that "simulate human conversation with an end user" (IBM, n.d.), now combine with artificial intelligence (e.g., machine learning) tools and large language models such as ChatGPT. These generative AI-powered chatbots (AI bots) scan information provided for informed consent preambles of surveys and complete closed questions (e.g., multiple-choice), as well as open-ended questions (e.g., text boxes). We define malicious responses as anonymous responses designed to exploit monetary incentives (Goodrich, et al. 2023) or provide ideological opposition (e.g., Haverkamp et al., 2023) that threatens data integrity.

Our survey project aimed to explore eHealth literacy and digital health information needs of older adult cancer survivors living in British Columbia (BC). We employed validated tools, as well as incorporated pilot study findings to ensure provincial context relevance. We consulted a statistician to ensure quality and to assist with data analysis. We employed CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) security offered by the approved institutional platform to mitigate malicious survey responses. After receiving ethics approval, the survey link was disseminated through trusted associations who, in turn, shared the link on their social media accounts. A draw for a gift card was offered as incentive.

When the survey closed, most of the 126 responses were anomalous. The statistician concluded, after reviewing data using current best practices to determine veracity, that only four responses were likely human generated. She based this conclusion on the following: very few internet protocols (IP) addresses were located in BC (with a majority either Eastern United States or other continents); multiple responses had identical start date and time (or differing by seconds only); an unusual number of participants selected the first option tick boxes for demographics, thus identifying as Hispanic females accessing care through the First Nations Health Authority with prostate cancer their primary diagnosis; and instead of calculating an answer, suspected non-human responses merely repeated a number offered in the question.

Best practices suggested to protect from AI bot malicious responses recommend a constellation of approaches. These items include ones such as: not including upfront description of the survey; more sophisticated CAPTCHAs; two-factor authentication; insert random unrelated questions periodically to filter responses (e.g., "provide an original joke"); speed analysis for survey completion; and limit access to certain groups or sources to ensure respondents are humans. Further investigation points to a perpetual cycle in which progressively complex AI bot detection solutions arise concurrently with increasingly sophisticated AI bot programming able to bypass those 'new' security measures (e.g., AI bots can now match predicted human speed or ignore honeypot questions[1]). Of note, the preponderance of such recommendations as those listed above are put forth by companies selling either survey platforms or access to survey participants (e.g., Amazon, Prolific, SurveyMonkey).

One proposed 'solution' to avoid survey preamble information is very concerning, particularly for oncology patients who may be quite vulnerable. We view it as having the potential to negatively impact human participant's informed consent process. In the uncertainty of the current AI bot infestation, research participants' right to informed consent must be held central. This is especially important considering the current emergence of for-profit companies offering access to a vetted participant pool. While we recognize that the advertising assures researchers (consumers) that the 'product' (human participants) will consist of access to legitimate adult participants who reside in democratic countries and are compensated fairly, we also note that there does not appear to be transparency regarding this claim. Thus, researchers will have to 'trust' that corporations, such as Amazon's Mechanical Turk (MTurk), are engaging in recruitment activities without coercion or violation of human rights. With this lack of transparency, how can scientific rigour in participant recruitment, equity, and

## AUTHOR NOTES

Lorelei Newton, PhD, RN (corresponding author), School of Nursing, University of Victoria

Claire Fullerton, BScN, RN, School of Nursing, University of Victoria

Helen Monkman, PhD, School of Health Information Science, University of Victoria

Conflicts of interest: The authors have no conflicts of interest to declare.

1 Honeypots are decoy questions embedded in a survey that are programmed to engage and deceive bot respondents (e.g., Storozuk et al., 2020). For example, inserting white text on a white background that a chatbot would answer but a human would not detect

representation be ensured? The devolution of research participation into a 'side gig' potentially exposes humans to exploitative corporate practices. In this way, buying access to survey participants could be seen as leveraging human vulnerabilities, such as having cancer, for economic gain. There is a real threat of scaling up inequities in our cancer systems, especially as the findings from surveys are used to inform best practice guidelines, policy and, indeed, often the direction of our democratic processes.

Fortunately, in Canada, ethical access to valid respondent pools does exist (e.g., https://www.yorku.ca/research/isr/). In our study, the human participants were most likely recruited through a similar non-profit pool (https://reachbc.ca/). Such hubs of not-for-profit access need to be supported and expanded as vital components of social infrastructure for researchers and the democratic structures we must trust. As we increasingly rely on AI tools for convenience and cost savings, we must also guard against being disconnected from the very people we wish to learn from through research. In the end, with the incredible advancements in technology, we must support practices that not only verify humanity, but validate it as well.

## REFERENCES


Amazon (n.d.). *Getting started with surveys on MTurk*. https://blog.mturk.com/getting-started-with-surveys-on-mturk-e2eea524c73

Amazon Mechanical Turk – Mturk (n.d.). Access a global, on-demand, 24x7 workforce. https://www.mturk.com/

Goodrich, B., Fenton, M., Penn, J., Bovay, J. & Mountain, T. (2023). Battling bots: Experiences and strategies to mitigate fraudulent responses in online surveys. *Applied Economic Perspectives and Policy, 45*(2), 762–784. https://doi.org/10.1002/aepp.13353

Haverkamp, A., Johnson, F., Bothwell, M., Driskill, Q., & Montfort, D. (2023). Attack helicopters and white supremacy: Interpreting malicious responses to an online questionnaire about transgender undergraduate engineering and computer science student experiences. *Bulletin of Applied Transgender Studies, 2*(1-2), 67-94. https://doi.org/10.57814/qd1y-9b22

IBM (n.d.). *What is a chatbot?* https://www.ibm.com/topics/chatbots

Prolific (n.d.). *How to improve your data quality from online research*. https://www.prolific.com/resources/how-to-improve-your-data-quality

Storozuk, A., Ashley, M., Delage, V., Maloney, E. (2020) Got bots? Practical recommendations to protect online survey data from bot attacks. *The Quantitative Methods for Psychology, 16*(5), 472-481. https://doi.org/10.20982/tqmp.16.5.p472

SurveyMonkey (n.d.). *How can you outsmart a bot survey respondent? Here's what we learned from building one ourselves*. https://www.surveymonkey.com/curiosity/outsmart-bot-survey-respondent/