Not the Participants I Was Looking For: BOT Attacks and Incentivized Recruitment Surveys

Contributing Author: Mary Leas PhD, RN, CCRN

The purpose of this article is to describe the author's experience utilizing a monetarily-incentivized online survey to recruit participants for a nursing research study and their experience detecting the many BOTs that overwhelmingly responded. Secondly, the author will offer survey development and respondent screening practices that may mitigate the negative impacts and risks that BOTs produce by fraudulently accessing surveys or research.

It is well known that recruiting specialty nursing populations for research can be challenging (Thompson & Patterson, 2025). The use of snowball sampling through social media-based professional nursing groups can help researchers to reach their desired populations and achieve rich data (Kirchherr & Charles, 2018). Facebook and LinkedIn are often used to recruit for health-related studies (Whitaker et al., 2017). Social media recruitment posts that include monetary incentivization have been recognized as valid tools for recruitment, retention, and attrition minimization (Largent et al., 2022). However, when posting financially-incentivized calls for research participation to social media-based professional groups, there are no assurances that the researcher will reliably contact their intended participant pool. On the contrary, researchers often make contact with BOTs (Harmon, 2025).

BOTs have been described in the literature as automated malicious agents, controlled by software, that emulate human responses, carry out tasks, respond to content, or complete surveys (Ng & Carley, 2025). BOTs continue to be an emerging threat to nursing research because they engage with surveys and mimic the responses of humans for financial or other gain. For these reasons, BOTs pose a risk to data integrity and validity (Harmon, 2025).

The author completed a research study last year exploring the phenomenon of moral distress in acute care nurse case managers. Participant recruitment occurred primarily through private listservs and public and private nursing case management groups on Facebook and LinkedIn. The standardized research recruitment post communicated that eligible participants would receive an Amazon gift card for completing the study interview. The author noticed almost immediately after posting the incentivized call for research participants online that the survey would be bombarded with large numbers of responses. Although initially delighted with the windfall of potential participants, the author stopped to analyze this phenomenon to protect the rigor of the study.

The author reviewed the survey responses and the data did not reflect the expected responses from nurse case managers. There was a shocking pattern of innumerous incomplete, low-quality, and/or illogical responses logged in the survey. Many differing and illogical responses were traced back to repetitious internet protocol (IP) addresses. Events such as these have been described in the literature as BOT attacks (Comachio et al., 2024, Harmon, 2025).

As a result of the BOT attack, the researcher paused recruitment while they reevaluated and redesigned their survey. First, the author added ReCAPTCHA (computer automated public Turing test to tell computers and humans apart) verification to the recruitment survey. ReCAPTCHA verification are tests embedded within surveys that can differentiate between human and computer responses by means of typing speed and IP address analysis, image challenges, and checkbox clicks (Ng et al., 2025; Webber-Ritchey et al., 2025). Additionally, the author added open answer questions, called trap questions, to the survey. Trap questions help researchers detect and exclude inappropriate data from survey participants who provide low quality responses (Harmon, 2025; Ng et al., 2025). For example, one trap question posed by the author was a request for potential participants to describe their case management role and responsibilities. An example of a low quality response to this specific question contained illogical information relating to bedside nursing without detail or context.

The redesigned recruitment survey was redeployed and participant responses were reviewed. The author ruled out participants who registered interest from any duplicate IP addresses. In internet-based surveys, multiple submissions originating from the same IP address is indicative of repeat responders, or BOTs, attempting to participate in a study. The inclusion of questionable participants threatens the validity of a study (Bowen et al., 2008; Walker et al., 2023). With the addition of these survey and data analysis improvements, the author was able to scrutinize the ReCAPTCHA verification data, consider the quality of each participant response against the study inclusion criteria, and review the IP address from which the response was received

before confirming the participant's study eligibility and scheduling the interview.

Additionally, despite the survey redesign, there were potential participants who could not be deemed eligible or ineligible based on the content or quality of their survey responses. In these cases, it is appropriate for a nurse researcher to use their discipline-specific expertise and knowledge to discern which participants are most likely representative of their target population (Ng et al., 2025). Therefore, the author contacted these participants via email to request additional information to confirm they met inclusion criteria before confirming their participation.

The author was able to identify potentially fraudulent participants and keep BOTs from infiltrating the study by pausing, redesigning, and redeploying the online survey. Online survey platforms such as Qualtrics have some built-in fraud detection capabilities (Qualtrics, n.d.). However, as a novice researcher, the author was not skilled at deploying their initial survey to minimize BOT responses and learning occurred through trial and error. The processes of ReCAPCHA verification, survey redesign, scrutiny of IP addresses, rigorous and systematic survey response screening, and inclusion clarification queries ruled out 119 out of 150 survey responses. These techniques are recognized in the literature as helpful for the maintenance of data integrity (Comachio et al., 2025; Harmon, 2025; Ng et al., 2025). The literature suggests that researchers should use a combination of strategies to protect their data and studies from BOT intrusion (Comachio et al., 2025; Ng et al., 2025). Despite ruling out a large number of potential participants, the author was able to recruit an adequate number of case manager perspectives to support their study.

This author would offer these additional best practices. When promoting a survey, it is recommended not to place the incentive messaging in a prominent place where it may be easily detected by BOTs. Artificial intelligence-powered BOTs can detect symbols and words that communicate a potential financial gain (Webber-Ritchey, 2025). Researchers should optimally deploy all BOT detection capabilities available within their online survey platform and design their surveys using multi-layered evidence bases strategies. Methodical survey response and eligibility screening should be completed. Lastly, any research study that includes financial incentives for participation should be designed with verification checks to confirm eligibility prior to distribution of incentives (Camachio et al., 2025; Harmon, 2025). The recommendations in this article include the strategies that the author found helpful. There are numerous literature-based resources available to nursing scientists to support disciplined online recruitment and data collection in the age of AI. As AI and machine learning continue to develop at a rapid pace, it is essential for nurse scientists to educate ourselves on BOT mitigation tactics. ■

References

Bowen, A. M., Daniel, C. M., Williams, M. L., & Baird, G. L. (2008). Identifying multiple submissions in internet research: Preserving data integrity. *AIDS and Behavior, 12*(6), 964–973. https://doi.org/10.1007/s10461-007-9352-2

Comachio, J., Poulsen, A., Bamgboje Ayodele, A., Tan, A. C., Ayre, J., Raeside, R., Roy, R., & O'Hagan, E. (2024). Identifying and counteracting fraudulent responses in online recruitment for health research: A scoping review. *BMJ Evidence-based Medicine, 30*(3), 173–182. https://doi.org/10.1136/bmjebm-2024-113170

Harmon, C. S. (2025). Best practices in mitigating the impact of BOT attacks in internet-mediated research. *CIN Computers Informatics Nursing, 43*(9), 1–5. https://doi.org/10.1097/cin.0000000000001332

Kirchherr, J., & Charles, K. (2018). Enhancing the sample diversity of snowball samples: Recommendations from a research project on anti-dam movements in Southeast Asia. *PLoS ONE, 13*(8), 1–17. https://doi.org/10.1371/journal.pone.0201710

Largent, E. A., Eriksen, W., Barg, F. K., Greysen, S. R., & Halpern, S. D. (2022). Participants' perspectives on payment for research participation: A qualitative study. *Ethics & Human Research, 44*(6), 14–22. https://doi.org/10.1002/eahr.500147

Ng, L. H. X., & Carley, K. M. (2025). A global comparison of social media BOT and human characteristics. Scientific Reports, 15(1), 1–19. https://doi.org/10.1038/s41598-025-96372-1

Ng, W., Erdembileg, S., Liu, J. C. J., Tucker, J. D., & Tan, R. K. J. (2025). Increasing rigor in online health surveys through the reduction of fraudulent data. *Journal of Medical Internet Research, 27*, 1–11. https://doi.org/10.2196/68092

Qualtrics. (n.d.). Fraud Detection. *Qualtrics.XM*. Retrieved February 14, 2026, from https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/

Thompson, H., & Patterson, C. (2025). Recruiting for research: incentives and integrity. Nurse Researcher., 33(3), 6–7. https://doi.org/10.7748/nr.33.3.6.s2

Walker, L. O., Murry, N., & Longoria, K. D. (2023). Improving data integrity and quality from online health surveys of women with infant children. *Nursing Research, 72*(5), 386–391. https://doi.org/10.1097/NNR.0000000000000671

Webber Ritchey, K. J., Ally, F., Galura, S., Buck, J., Brockway, C., Chipps, E., Ponder, T. N., Simonovich, S. D., Spurlark, R. S., Vancil, B., & Monturo, C. (2025). Identifying fraudulent responses and imposters in research recruitment of Subjects Through social media. JONA: *The Journal of Nursing Administration, 55*(7), 388–394. https://doi.org/10.1097/nna.0000000000001596

Whitaker, C., Stevelink, S. A. M., & Fear, N. T. (2017). The use of Facebook in recruiting participants for health research purposes: A systematic review. *Journal of Medical Internet Research, 19*(8), 1–11. https://doi.org/10.2196/jmir.7071