Safeguarding Online Studies Against Bots: Information, Tips, and Guidance

Any researcher planning to conduct any form of online data collection, especially via online surveys, should take precautions against "bots". Bots are automated computer programs that are capable of independent functioning and the ability to emulate human responses. They are created by bad actors often looking to take advantage of research compensation or skew the results of studies.

Bots pose as eligible participants and repeatedly submit responses at much faster rates than actual human respondents, capable of making several hundred submissions within minutes. Bots can be programmed to give a normal answer distribution across responses and use language from the survey to craft open-ended responses to elicit multiple payments from the study team in any studies with compensation. They can also be programmed to skew results by selecting specific options or writing specific written responses creating a large volume of submissions with data that may be biased, unreliable, or invalid.

While bot activity will not occur on all online surveys or forms, any studies offering any type of compensation (e.g. gift cards, completion tokens, survey credit, etc…) are more likely to be targeted. Study teams have reported bot activity on surveys listed on frequently used research crowdsourcing sites such as MTurk and Prolific (among others). Researchers should be mindful if the link for the online survey is publicly listed. Bot scripts are ever evolving and creators of bots may adapt to safeguards that study teams have in place. Multiple approaches may be needed and constant vigilance from study teams monitoring incoming survey responses is strongly encouraged.

See below for tips and guidelines for study teams conducting online research. This is NOT an exhaustive list of all the types of safeguards but is simply a starting point for study teams. REDCap, Qualtrics, and various other survey hosting sites all have different options available – *study teams should review all the fraud prevention tools offered to them by the survey site*. Not all options may be relevant to every study. When building the survey online:

- Enable **CAPTCHAs** and **reCAPTCHA** - the most basic level of security which involve asking users to identify letters or numbers that have been distorted or to identify basic images. This may be a pass/fail and those that do not pass are usually unable to either start or complete the survey.
- Add **challenge questions/attention checks** throughout the survey to help spot bots or fraudulent responses.

        - Multiple attention-check questions such as "*Pick the word that rhymes with dog*" or "*To answer this question, please choose D*." or "*Who would drive a fire truck*?"
        - **Cross question validation** - Similar questions at different points in the survey to check for consistency. They do not have to be related to the survey topic itself; it is just to help detect automated responses.
            - E.g., "*What is your favorite color*?" & several questions later "*Earlier in the survey, what did you say was your favorite color*?"
        - Consider asking the **screener questions** at the beginning and again at the end of the survey for consistency.
    - Add **honeypot questions**, hidden questions that a human wouldn't see but a bot will see and answer. The content of the question is unimportant as the purpose is to identify a response where none should exist.
    - Ask **open-ended questions** to assess engagement.
    - If possible, **randomize** question order and response option order.
    - If recruiting multiple groups or on different platforms, add a **unique identifier to the end of the URL** to create unique links for each group.
        - E.g., If the study is recruiting from Reddit and Facebook, set up each post on each platform to have a unique end identifier. If one gets hacked, only the affected one needs to be shut down.
    - Depending on the identifiability of the data being collected, consider **IP filtering** (blocking repeated attempts from the same IP address) or turning on **GeoIP** (restricting the survey to a certain region of the world). ***IP addresses are considered personal identifiers; the collection of IP addresses means that the dataset is not anonymous.***
    - ***Add a response limit or quota to prevent over enrollment. The quota must match your IRB-approved number of participants and should align with your project budget.***
- When reviewing the surveys:
    - Review the attention check, validation, and honeypot questions.
    - Review answers for consistency.
    - Identify if there are patterns in survey responses (e.g., only A is selected for every answer).
    - Review for duplicate open-ended answers over multiple surveys.
    - Review for incoherent/nonsensical open-ended answers. Please note that human participants can provide answers that the study team might not expect that may not be fraudulent.
    - Check **time stamps.**
        - Are there clusters of submissions at the same or similar times?

        - Are there patterns of any sort – an influx of submissions at a similar time daily?
        - Are surveys being completed in an unrealistic timeframe?
- On study documents:
    - **Protocol** – Provide information about what controls and measures are taken regarding trying to mitigate bot infiltration as well as clear procedures for handling bot activity and fraudulent data:
        - How is suspicious activity defined by the study team?
            - E.g., answering 2/3 attention check questions incorrectly? Completed the survey in <1 minute? Responding to honeypot questions? Multiple surveys with the same open-ended answers? Impossible data values?
        - What will study teams do with surveys determined to be fraudulent?
        - If there is compensation involved, does the study team have enough time to review the surveys prior to providing compensation?
        - Prospectively create a data-cleaning protocol in your IRB protocol for identification of bots and fraudulent responses.
    - **Consent form** - Ensure that your consent form contains the SBU boilerplate bot language included in the latest version of the online consent form found in the myResearch library.
    - **Recruitment material** –
        - Refrain from posting specific compensation amounts in any fliers or postings about the study. Avoid using symbols like $, €, or £ in the public-facing survey details. The total compensation must be stated in the consent form.
        - If posting to social media, consider posting recruitment information as images to avoid bot scraping and auto-filling.
        - Consider using a compensation raffle.
        - Consider using a public link for a screening survey to verify eligibility and detect bots before they affect your data.

Resources and Further Reading

Please reach out to the Office of Research Compliance if you have questions or if you are responding to a bot attack on your online survey. Stony Brook University IT may be able to assist.

Goodrich, B., Fenton, M., Penn, J., Bovay, J., and 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

Griffin, M., Martino, R.J., LoSchiavo, C., Comer-Carruthers, C., Krause, K.D., Stults, C.B., Halkitis, P.N. (2022). “Ensuring survey research data integrity in the era of internet bots.” *Qual Quant* **56**, 2841–2852. https://doi.org/10.1007/s11135-021-01252-1

Kennedy R, Clifford S, Burleigh T, Waggoner PD, Jewell R, Winter NJG. (2020). “The shape of and solutions to the MTurk quality crisis.” *Political Science Research and Methods* 8, 614–629. https://doi.org/10.1017/psrm.2020.6

Lawlor, Jennifer & Thomas, Carl & Guhin, Andrew & Kenyon, Kendra & Lerner, Matthew & Drahota, Amy. (2021). “Suspicious and fraudulent online survey participation: Introducing the REAL framework.” *Methodological Innovations*. 14. 205979912110504. https://doi.org/10.1177/20597991211050467

Pozzar R, Hammer MJ, Underhill-Blazey M, Wright AA, Tulsky JA, Hong F, Gundersen DA, Berry DL. 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.

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

Teitcher, J. E., Bockting, W. O., Bauermeister, J. A., Hoefer, C. J., Miner, M. H., & Klitzman, R. L. (2015). “Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs.” *The Journal of law, medicine & ethics : a journal of the American Society of Law, Medicine & Ethics*, *43*(1), 116–133. https://doi.org/10.1111/jlme.12200

https://behavioralscientist.org/how-to-battle-the-bots-wrecking-your-online-study/

https://www.psychstudio.com/articles/bots-randoms-satisficing/