Tip Sheet on Preventing Fraudulent Responses and Bots in Online Studies

The IRB office has seen an uptick in the use of online platforms, including social media, to advertise and recruit research participants. Unfortunately, online platforms are susceptible to fraudulent survey responses. Online surveys advertised on social media are especially vulnerable to bots (that is, impersonator computer programs that will automatically complete an online survey). For example, researchers may post a social media advertisement with an online survey link and receive an unusually high number of responses in a short time (hundreds of responses in a few hours!). Often, bots will take the survey to earn the study's incentive / compensation.

Data integrity is lost when surveys experience bot attacks and fraudulent responses. The data may be unusable, or the researcher may need to invest significant efforts to sort through the data for authentic responses. Filtering through data to find "real" participants can also cause problems for distributing participant compensation. Additionally, due to the high volume of bot responses, researchers might exceed their IRB-approved number of participants, resulting in a protocol deviation.

To prevent bots and other types of fraudulent activity, please consider the following tips when designing and implementing online research. Not all options will be applicable for every study. Preventing fraud is a complex issue, so you may need to implement multiple strategies.

Tip #1: Exercise caution when posting a survey link on a publicly available website (especially social media sites). This means that the survey will be open to anyone – including bots.

Alternatives:

- Use other methods for recruitment. For example, work with a relevant organization to help distribute your survey to their members.
- Use a public link for a screening survey, so you can verify eligibility and detect bots. Send a personalized main survey link to eligible participants.
- Ask interested individuals to contact you directly.

If you use a public survey (not usually recommended), monitor it closely! Check the responses as soon as it is publicly posted. Close the survey if you suspect bots.

Tip #2: Carefully consider study incentives / compensation. Surveys with monetary compensation seem to attract the most bots.

Alternatives:

- Don’t provide monetary compensation for survey completion. Highlight the importance of the study or other benefits of participation (but please do not exaggerate benefits or make promises about something that hasn’t been tested).
- Don’t include compensation in the online advertisement. The compensation can still be added to the consent form.

Tip #3: Design your survey to detect bots and fraudulent responses.

- Include attention check questions.
- Include open-ended response questions.
- Include duplicate questions.

Tip #4: Use survey features to detect bots.

- Use fraud detection features offered by Qualtrics.
- Use CAPTCHA verification.
- Collect timestamps (allows you to determine how quickly the survey was taken).
- Collect IP addresses (allows you to determine where the survey was taken and if it was taken multiple times by the same respondent). *Note: IP addresses are considered identifiers, so datasets with IP addresses aren’t considered anonymous.*
- To prevent over-enrollment (which often occurs when there is a high volume of bot responses), set a limit on the number of survey responses. However, please note that setting a quota in Qualtrics is not a perfect system. Responses aren’t recorded until the surveys are completed, so if multiple participants / bots are taking the survey at the same time, the limit will be exceeded. Relying solely on this strategy isn’t recommended.

Tip #5: Have a plan to manage bots / fraudulent responses.

- In the consent form, include the conditions under which someone will not be paid and/or will be withdrawn from the study. Examples: Participants won’t receive compensation if they fail multiple attention check questions / complete the survey in under two minutes / have an IP address that is outside the United States.
- Monitor your survey responses on a routine basis.

Resources

These tips are mostly based on the IRB office’s experiences and strategies that we have seen implemented, as well as other suggestions in the resources below. There are additional recommendations in these resources that may be helpful:

- Ensuring survey research data integrity in the era of internet bots
- How to Battle the Bots Wrecking Your Online Study

- Threats of Bots and Other Bad Actors to Data Quality Following Research Participant Recruitment Through Social Media: Cross-Sectional Questionnaire
- Got Bots? Practical Recommendations to Protect Online Survey Data from Bot Attacks
- Detecting, Preventing, and Responding to “Fraudsters” in Internet Research: Ethics and Tradeoffs
- UCLA Research Administration Human Research Protection Program Tip Sheet: Online Survey Protection Considerations
- How to Stop Bots From Ruining Your Survey