IRB Guidance on Preventing Fraudulent Responses and Bots in Online Studies*

Updated: 03/12/26

IRB's have 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.

To prevent bots and other types of fraudulent activity, 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.

- **Avoid posting links to social media** & other open web platforms!
- Use other methods for recruitment. For example, **work with a relevant organization** to help distribute your survey to their members (and make sure they do NOT post it on a public website!).
- **Include 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.
- **Do NOT use the words "paid," "survey," or "study" in the survey URLs!**

Bots look for these key words. (For example, use “redcap.link/example” rather than “redcap.link/examplesurvey”).

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

- **If possible, do NOT provide monetary compensation** for online survey completion.
- **Do NOT list the compensation in the online advertisement (e.g., email, flyer)** if monetary compensation is provided. The compensation only needs to be stated in the informed consent form.

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

- Include **attention check questions** to promote respondent attentiveness and reduce automated responses.
- Include **open-ended response questions** (to flag nonsensical or irrelevant content)
- Include **duplicate questions** at multiple points to ensure consistency in responses, or ask the same question more than once.
- Add **false/impossible response options** (such as a selection for “TV ad” when recruitment never occurred through TV ads) to flag suspicious responses.
- **Deploy cross-survey validation** (e.g., ask the same question on an eligibility screener and survey to compare responses for consistency across forms)

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).
- Look for **batches** of concurrent survey start & end times.
- **Enable time zone checks** to ensure respondent’s computer is in the target time zone, if applicable.
- **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 are not 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 are not 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 is not 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 will not 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.
- Use **videoconference or phone verification** for those deemed eligible.

Resources

https://uwm.edu/irb/wp-content/uploads/sites/127/2024/01/Tip-Sheet-on-Preventing-Bots.pdf

Identifying and preventing fraudulent responses in online public health surveys: Lessons learned during the COVID-19 pandemic

Wang J, Calderon G, Hager ER, Edwards LV, Berry AA, et al. (2023) Identifying and preventing fraudulent responses in online public health surveys: Lessons learned during the COVID-19 pandemic. PLOS Global Public Health 3(8): e0001452. https://doi.org/10.1371/journal.pgph.0001452

*We thank the **University of Wisconsin Milwaukee Institutional Review Board (IRB)** for sharing their "Tip Sheet on Preventing Fraudulent Responses and Bots in Online Studies" for our use in creating this document.