Northeastern University
Human Research

Guidance: Preventing Bots and Fraudulent Responses in Online Studies

Overview

Recruiting participants through online platforms offers efficiency and broad reach, but it also increases the risk of fraudulent survey responses. Online surveys are vulnerable to two related threats. The first is bots: automated programs designed to rapidly complete surveys, often to obtain participant compensation. The second is human bad actors: real people who submit faked responses, misrepresent their eligibility, complete a study multiple times under different identities, or participate from outside the intended population to collect compensation. Both threats are often financially motivated, and a common warning sign of either is an unusually high volume of responses within a short period of time.

Fraudulent responses undermine data integrity, may render datasets unusable, and can require substantial time and resources to identify and remove. They also complicate participant compensation. As bad actors become more sophisticated—capable of generating realistic response patterns and open-ended answers—distinguishing authentic participants from fraudulent ones is more challenging.

Given the prolific use of online research and recruitment, researchers conducting online studies must remain vigilant and proactive. Preventing bot and other fraudulent responses often requires multiple strategies. The guidance below outlines practical considerations to help researchers protect data quality and maintain regulatory compliance when conducting online human subjects research.

Common signs:

1. Receiving many responses in a very short period of time. Researchers often receive dozens or hundreds of responses in a very short period of time at set intervals.

2. Receiving responses with an impossible completion time. Bots and bad actors who skip reading questions often complete surveys in timeframes that are not humanly possible.

3. Receiving responses that seem to have very similar email addresses. Some researchers report that some fraudulent participants will use free email addresses like Google and have minor variations of the same email address. Often, this will take the format of name+randomtest@gmail.com.

4. Receiving data or responses that don't make sense. Researchers will notice data patterns that are extremely unlikely in individual responses such as one depression inventory's responses being very different from a parallel instrument.

5. Use of VPN to change IP addresses between responses. Most bad actors use VPN and submit multiple responses from different IP addresses this way. Because of this, you might not be able to use IP address as a reliable way to flag bad actors.

Tips to mitigate bad actors:

1. Be cautious with public links that advertise compensation. Posting links on public websites with compensation tends to attract bad actors.

- Recruit through trusted organizations or networks.
- Use a public screening survey that is reviewed manually, then send personalized links to eligible participants.
- Ask interested individuals to contact you directly for survey links.
- If a public link is used, monitor responses closely and close the survey if bad actor activity is suspected.

2. Carefully consider compensation. Bad actors almost always seek out studies with compensation.

- Consider non-monetary incentives or emphasize the study's importance (without overstating benefits).
- Exclude compensation details from advertisements; include them in the consent form instead.
- If participants are compensated, clearly state what will disqualify them from payment in the exempt info sheet or consent form.
- Consider disqualification criteria carefully. Thresholds meant to catch bad actors may result in real responses being rejected which can impact equitable subject selection or skew your sample.

3. Design surveys to detect fraud.

- Include attention-check questions.
- Add open-ended items.
- Use duplicate or consistency-check questions.
- Use a pre-screening survey or embedded eligibility checks to exclude ineligible participants and filter out bad actors.

4. Use built-in survey protections.

- Enable fraud-detection tools (e.g., Qualtrics features- see links below).
- Use CAPTCHA/reCAPTCHA verification.
- Collect timestamps to flag unusually fast completion times.
- Collect IP addresses to detect duplicate or out-of-region responses (note: IPs are identifiers).
- Set response limits to reduce over-enrollment, recognizing this is not foolproof.
- Note that, as bad actors become increasingly more sophisticated, many of the options above become less useful.

5. Plan for managing fraudulent responses.

- Plan how you will handle fraudulent responses when designing your study.
- Specify in advance what will count as a fraudulent or low-quality response (e.g., failed attention checks, impossible response patterns, duplicate identifiers).
- Clearly state in the consent form when compensation may be withheld or participation ended.
- Monitor survey data regularly and act quickly if suspicious patterns emerge.
- Recognize that fraud-prevention measures, compensation conditions, and any identifiers collected to detect fraud should be described in your IRB submission. Adding these measures mid-study may require an amendment.

Responding to Bad Actors After a Study Goes Live:

Most researchers first discover the bad actor problem after a survey goes live, and they have multiple responses. The worst-case scenario is that a study has been completed, has already compensated participants, and the responses are heavily contaminated with bad or garbage data. The goal is to contain the damage, prevent further harm, preserve what data you can, and meet your regulatory obligations and commitments to your participants.

1. Pause the Study. This might include deactivating public links or removing recruitment posts. Participants who responded via email/etc can be told that you are pausing enrollment for technical reasons. You can then reach out to our office to discuss how to move forward.

2. Assess the Damage. How much of the dataset is usable, and what needs to be discarded? Distinguish between responses that are almost certainly fraudulent (impossible completion times, duplicate identifiers, coordinated bursts of near-identical submissions), responses that are suspicious but ambiguous, and responses that appear legitimate. Document the indicators you are relying on.

3. Handle Compensation Decisions Carefully. Wrongly withholding compensation from a real participant is both an ethical harm and a potential source of valid complaints. If your consent forms specified conditions for compensation, follow them. If they didn't, you may need to compensate all participants. You can consult with the IRB if you feel you are unable to do so.

4. Contact our Office. We can help determine how you should react, handle communication, handle reporting requirements, or other next steps. Every instance and situation is different.

References and Resources:

- University of Wisconsin, Milwaukee-IRB Tip Sheet on Preventing Fraudulent Responses and Bots in Online Studies
- UCLA Research Administration Human Research Protection Program Tip Sheet: Online Survey Protection Considerations
- University of Maine-Guidance on Preventing Bots and Fraudulent Responses in Online Surveys
- Columbia University, Teachers College: Bots and Online Human Subjects Research

- Behavioral Scientist: "How to Battle the Bots Wrecking Your Online Study"
- NIH, National Library of Medicine: "Detecting, Preventing, and Responding to "Fraudsters" in Internet Research: Ethics and Tradeoffs"
- **Qualtrics**: Fraud Detection; Response Quality; and Survey Protection
- **Amazon Mechanical Turk (MTurk)**: Acceptable Use Policy
- **Prolific:** Bots and Data Quality on Crowdsourcing Platforms
- **Survey Monkey**: Filtering Survey Results