MANAGING PARTICIPANTS (AND BOTS) FALSIFYING THEIR IDENTITY IN RESEARCH

The purpose of this document is to provide guidance on ethically acceptable strategies to prevent participants' misrepresenting their eligibility for participation in research and non-participant 'bot' responses to survey research or other types of online engagement in research. Your study may be the target of participant misrepresentation if you notice one or more of the following signs:

- Participant claiming to be from a required geographic area who cannot provide appropriate contact information, or who changes contact information once participation begins.
- Evidence emerges that an individual (IP Address) has enrolled multiple times under different names.
- Requests that a scheduled online interview be replaced with a text-based chat.
- Illogical or inconsistent responses provided to questions posed.
- Multiple participants communicating using the same messaging or who provide unusually brief or vague responses to questions or who complete surveys far faster than is plausible.
- Unusual interest in monetary incentives.
- Receiving a high number of responses in a short period of time.
- Multiple email addresses formatted similarly or that are from unknown email domains.

When a research participant's identity is called into question, the integrity of the data and the data of other participants is also called into question. Valuable research time is lost and there is the chance of monetary loss if incentive/remuneration is provided to falsified participants. Social media recruitment and online participation options may increase the likelihood of fraudulent participation.

How to Create Secure Online Surveys
It is becoming more common to encounter "bot-like" response behavior in online surveys. Bots can be difficult to identify but being watchful for anomalies such as those listed above may help. Advanced Research Computing (ARC) recommends the following practices when using online surveys:
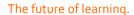
- Avoid sharing survey links on publicly accessible platforms (such as social media) unless your aim is to generate a very large number of responses.
- Where possible, limit the number of responses a single participant can submit, as well as time to complete the survey.
- If survey access is shared via email, configure the survey link to only allow invited participants to access the survey and ensure the link is set to expire after a specified amount of time.

Mitigation Strategies related to incentives/remuneration and validating identity
There are multiple reasons why participants may misrepresent their identities, including malicious intent to corrupt data, however the offer of incentives/remuneration seems to be the most common reason. The suggested strategies below focus on changing how identities are validated, and how incentives/remuneration is offered. While these strategies cannot guarantee that participants don't continue to falsify their identities, they may hopefully dissuade some and allow for early detection of others. Keep in mind that these strategies will need to be outlined in the recruitment and/or consent materials so that invited participants have the information necessary to make an informed choice about whether they choose to participate in the research.

1. When seeking Canadian participants only, avoid using gift cards that have worldwide usage (i.e. use gift cards from a Canadian retailer) and include a statement that incentives/remuneration will be in the form of **Canadian** gift cards on your consent documents.
2. Include screening questions and/or embed questions about participant's demographic information to confirm eligibility, whereby those who do not answer correctly are removed.
3. When conducting online interviews or focus groups, ask that participants begin the session with their video turned on (so the interviewer can verify identifying details), but do not record or document these identifying details; just note that the participant has been verified (to minimize the risk of documenting or retaining personally identifiable information). For focus groups in particular, ensure you have a "waiting room" set up that allows for this verification to occur in private before participants join the group. Describe in the consent form how identity will be verified (e.g. by asking to see a piece of photo identification (without recording) or through informal facial recognition (to mitigate repeat participation).
4. In studies where geographic location is an inclusion criterion, deliver gift cards/remuneration by mail and collect their mailing address. This information should be stored separately from participant data and destroyed after the issuance of the remuneration/incentive.
5. Whenever possible, limit the number of responses a participant can submit and limit the timeframe that a survey is active.
6. Ensure the survey link is configured to only allow invited participants (i.e. email address) to access the survey and set the link to expire after a specific time period.
7. Use a captcha program that protects websites against bots. The University's instance of REDCap has this feature built in that can easily be added to public surveys REDCap | Research | Athabasca University
8. When using online interview or focus group methods, communicate your plan for dealing with possible participant misrepresentation in the consent form. For example, "Due to the increase in participants misrepresenting their eligibility to participate in research, we will ask you to confirm your eligibility before the [interview]/[focus group] begins. We will ask you to turn on your video and show us a piece of photo identification (like your driver's license). We will not record or document this information in the study records; it will only be used to confirm your eligibility. If you do not wish to proceed in this way, you will not be included in the study and will not receive any incentive/remuneration." OR "Participants will be asked to pass a short pre-screening questionnaire to confirm

eligibility to participate in the study. If you do not pass, you will not be included in the study and will not be compensated."

9. Provide your research team with information about the possibility of participants falsifying their identity and instructions for discontinuing engagement with a participant and discarding data if necessary.

Whatever pre-screening or mitigation strategies a researcher chooses to put in place, all constraints placed on participants to quality for participation in a research study must be disclosed during recruitment and consent. Be mindful to avoid using requirements that might create stigma, cause distress or place an undue burden on a population (e.g. be careful to avoid disqualifying those who might struggle with technology due to health or other issues).

Adapted from:
Office of Research Services. (2023). *Participants (and Bots) Falsifying Their Identity.* University of British Columbia.

Research Ethics. (2023). *Participant Misrepresentation in Research: Ethically Acceptable Mitigation Strategies.* Dalhousie University.