

Guidance – Preventing Fraud in Human Subjects Survey Research

General Description

This guidance is written to help researchers protect their data and reduce the risk of financial loss, fraud or bad survey responses when collecting survey data from research participants.

Considerations & Best Practices

General / Survey Design

- Survey Instrument selection – UNLV offers [Qualtrics XM survey](#) instrument is a key step in the design and deployment of a secure and effective survey. Use of other platforms risks security as well as data ownership and control by the P.I. and UNLV. Recommended survey platforms include [REDCap](#) and Qualtrics.
- Within Qualtrics, implement Security Scan Monitor which prevents email scanners from inadvertently starting a survey session.
- Implement Qualtrics Expert Review functionality to help ensure that surveys collect data of the highest quality.
- Remove the use of a back button to prevent retaking of survey.
- Perform periodic web-browser searches for the survey URL to identify if it has been republished.
- Design the survey with random answer choices, skip patterning, and selection of default answers.

Recruitment Strategies

- **Consider not offering monetary compensation**
- **recruit from a known group or organization (e.g. specific groups on social media, members of a particular organization like a university subject pool)**
- **Include a screener asking creative questions that verify the person as a member of the specific population before they can attempt the survey**

Participant Verification

The following strategies can help to positively identify survey respondents to prevent bots, duplicate submissions, and submission of data by ineligible participants:

- Remove back button to prevent the retaking of a survey.

- Implement CAPTCHA / ReCAPTCHA or other Bot detection technology. If using Qualtrics, this feature is Bot Detection. In REDCap, add CAPTCHA in Survey Settings
- Implement RelevantID in Qualtrics that measures likelihood of duplicates based on metadata in responses
- Request mailing address in the survey to allow for post survey address verification. Note that this control may result in collecting more private information than is necessary and should only be considered for high-risk instances (e.g., posting links to social media, offering high compensation).
- Conduct the survey in person / over the phone or video call / one-on-one.
- Create a unique survey link for each participant. Application of this is determined by the survey instrument being used.
- Perform IP address verification to assess geographic consistency with expected location of respondent, or to identify duplicate submissions. Note that:
 - Duplicate IP addresses may be a result of separate submissions from participants of the same household, institutions, or across shared computers (library, for example).
 - Geolocation based on IP address may not be consistent for respondents who use VPN's.
 - IP address is a PII identifier recognized by DHS and their collection may be prohibited in some instances.
 - In REDCap a module IP-Encrypt allows collection of encrypted IPs, masked to researchers but allowing comparison of IP addresses to detect duplicates.
- Implement pre-distributed passwords for invited respondents to access the survey for high-risk surveys.
- Review database of respondents to identify duplicate identifiers, if collected.
- Create links to survey that are one-time use to prevent sharing and/or reuse of links.
- Avoid posting links to surveys on publicly accessible sources including social media.
- Add a response limit (in REDCap or Qualtrics) for surveys with known participant caps to prevent extra or automated responses, or monitor and increase incrementally an initial cap to halt automated "survey farm" entries.
- Use a screening survey to determine eligibility of participants as a prerequisite to providing a link to the actual survey.
- Include a question that would be difficult for people outside of the target audience to answer, when possible for the population being surveyed, ideally not easily found by a search engine

Input Validation

The following strategies help to prevent the acceptance of survey submissions that are blatantly fraudulent, inaccurate, irrelevant, duplicate, or fabricated:

- Add fields to the survey that are invisible to humans but would be answered by bots "honeypot" questions. Note that these items may show up for participants using assistive technologies for people with vision or hearing impairment.
- Perform statistical analysis of responses to identify outliers
- Add a question at the end of the questionnaire asking respondents if they looked up any answers online or received assistance to complete the survey.
- Measure time taken to complete survey, or individual sections and then assess to identify anomalies that indicate automation.
- Include at least one question that asks for a text-based qualitative response.
- Include a duplicate question with one requiring a text response, the other multiple choice. Then compare differences.
- Include a simple validation question. For example, "To prove that you are not a robot, select response B."
- Review responses for consistency across questions. For example, age misaligned with year of birth.

- Use a URL shortener to obfuscate the link so that bots may not recognize it as a survey. Do not use the word "survey" in the URL.
- Include a duplicate question or similar congruent question and compare responses for inconsistencies, (e.g. DOB and ask later for age in years.)
- Compare all responses to identify duplication across submissions.
- Review responses to identify anomalous time of day submissions that might indicate a submission from an unexpected location based on time zone.
- Review submission times to identify groups of submissions entered within statistically unlikely period or at regular intervals (suggesting automation).
- Include a tiered response question asking for a typed response to a previous multiple-choice question. For example, ask "What was your response to question x (type your response)."

The following prevention strategies

- Do not implement mechanisms that automatically issue compensation based on survey completion unless other controls have been implemented to mitigate the risk of financial loss.
- In Qualtrics, implement Fraudulent Detection Fields that embed fraud detection fields into surveys to facilitate post submission fraud analysis
- Include a statement in the informed consent form or description that participants will not be paid if evidence of fraud is found.
 - Example language: *In order to preserve data integrity, this study may include safeguards against fraudulent responses and the collection of data from automated bots. If you agree to participate in this study, you acknowledge that our team may take steps to verify the authenticity of responses. This verification process may be conducted prior to issuing compensation. If responses cannot be verified, compensation may not be issued.*
 - Note: if there is a planned verification process, consider including the timeline for the verification process to the above (i.e., the verification process will be completed within 7 days of survey response).
- Perform post survey assessment to identify if multiple compensation/incentives are requested for the same destination (mailing/email address).
- Carefully consider the value and type of incentive/compensation offered. Higher values also incentivize fraud.
- Send incentive/compensation/reward through US Mail rather than to email address if the compensation is of a significant value.
- Inform prospective participants in the consent form and in the survey that payments may not be sent immediately to validate submissions and complete fraud detection analysis.

Resources

[Johns Hopkins Bloomberg School of Public Health Guidance on Fraud Prevention Regarding Use of Survey](#)

[UNH Scholars Repository, "A Simple Guide for Researchers and Institutional Review Boards \(IRBs\) to Protect Data Integrity in Online Human Subjects Survey Research.](#)