A black and red logo

Description automatically generated

**Safeguarding REDCap Public Surveys: Tips to Prevent Fraud**

Web-based survey data collection has become increasingly popular, and REDCap is  a valuable tool that can be used to collect survey data. However, as with any data collection undertaking, you need to take measures to ensure the integrity of the data and its source.  This is especially important when that data is collected through a public-facing survey link. You may find your survey being targeted by malicious actors or, at minimum, disingenuous respondents. You may also find your survey infiltrated by bots, automated software programs that enter fraudulent responses. This is especially common if you are offering participation incentives; however, it can happen in all surveys and for a variety of reasons. Therefore, preventing fraudulent survey responses is critical to maintaining the credibility of your data.

Here are 10 strategies to enhance the security and authenticity of survey responses in REDCap:

**1. CAPTCHA:**

REDCap offers a Google reCAPTCHA feature that can help protect from bots. You can enable this feature on REDCap projects with public-facing surveys. A survey participant will never have to pass the reCAPTCHA test more than once per day on a given device/computer.

To turn on CAPTCHA:

* In your survey, navigate to the left navigation menu under **Data Collection**.  Select ‘**Survey Distribution Tools**’
* Once you have created and saved your public survey, click the checkbox below the public survey URL to enable the feature.



**2. Time Limits:**

Time limits can deter individuals from spending an excessive amount of time crafting fake responses.  In REDCap, survey time limits can be defined in days, hours, minutes, or a combination of all three units. To set up this option for a survey, go to the Online Designer, under the **Survey Settings** menu and modify your survey settings to your desired time limit.

A screenshot of a computer

Description automatically generated

**3. Cross Question Validation:**

When possible, build survey questions that allow you to check for internal consistency between responses.  For example, if you are conducting a survey restricted to a geographical area, such as may be used for screening or recruitment, you can create questions to ask respondents to report their area of residence (e.g. county) and zip code. Internal validation can be used to ensure that respondents live in an eligible geographical area AND their zip code is associated with that area.

**4. Timestamps:**

Bots frequently respond in clusters, so an influx of surveys with the same or similar timestamps could indicate fraud. In REDCap, you can include an automatic time stamp as part of your dataset by using @NOW action tags. When @NOW is applied to a text field, REDCap will automatically track the date and time in which the survey was opened and record the data to that field.  Timestamp data can be used to look for clustering of responses that appear suspect.

**5. Payment:**

The most efficient way to prevent fraudulent responses in your surveys is to remove the temptation to script a bot. Instead of providing compensation immediately through the public survey link, offer compensation once you have verified the identity and contact information of your study participant and provided a unique survey link.

**6. Honeypot Questions**

Add some text fields that are completely hidden (HIDDEN-SURVEY) and this way the bots will see them / fill them in but actual participants won't / can't.

* This will only address bots, as they are accessing the survey via the application code, not the survey link (even though it may appear they are “survey respondents”)
* This will NOT address actual malicious survey respondents (from an actual person)

**7. Randomization of Question Order and Response Options:**

Fraudulent respondents may try to manipulate surveys by quickly selecting predefined answers without thoroughly reading the questions. Randomizing the order of both questions and response options can disrupt this pattern, making it more challenging for individuals to submit fake responses systematically.

The action tag **@RANDOMORDER** randomizes the order of multiple-choice field options. When applied to a field, it will automatically randomize the response options. Just remember that this action tag will not work for a matrix of fields.

**8. Attention-Check Questions:**

You can also include attention-check questions within your survey to help identify respondents who are not paying proper attention to the content. These questions typically require participants to select a specific response, and failure to do so accurately may suggest a lack of genuine engagement.

Example: The following question is to verify you are a real person.*Which of the following is a vegetable?*  (*fish, pizza, broccoli, milk*)

**9. Data Audits:**

Periodically auditing data for anomalies, patterns, or irregularities can help detect and address any fraudulent responses. As an example, check open-ended text field to look for identical, incoherent, or nonsensical responses. If you have a grid response format, you may want to look for straight-lining response items (e.g. choosing ‘strongly agree’ for all statements).

**10. Email Verification:**

To enhance the authenticity of respondents, consider implementing email verification. Participants would need to confirm their identity through a verification link sent to their provided email address before accessing the survey.

If you discover that your survey/project has been targeted by malicious actors, then you should regenerate a new survey link. To do this:

* Create a new instrument or move an existing one into the first position. This action generates a new public survey URL, rendering the old URL inactive.
* Use this new first instrument as a welcome or introductory page. This can help guide legitimate survey participants smoothly into the survey process.
* Implement an auto-continue in the survey settings of the new first instrument. This setting will redirect respondents to the next instrument in the project after they complete the first.

**PROTECT YOUR SURVEYS, PROTECT YOUR DATA**

For more information: [**Detecting and Preventing BOT and Fraudulent Survey Responses**](https://health.uconn.edu/clinical-research-center/wp-content/uploads/sites/50/2024/05/Avoiding-and-Detecting-Bots-and-Fraud_REDCapSurveys_.pdf)and[**CAPTCHA**](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fhealth.uconn.edu%2Fclinical-research-center%2Fwp-content%2Fuploads%2Fsites%2F50%2F2024%2F05%2FnedCAPTCHA.docx&wdOrigin=BROWSELINK)**.**