# Guidance on Online Survey Research to Protect Against Bots

Preventing computer and internet-based research from being compromised is becoming more challenging as technology develops. Therefore, certain precautions should be taken when constructing surveys for online recruitment and data collection. The purpose of this guidance is to help researchers plan, develop, and implement internet-based research protocols to protect against bots and scams. The IRB recommends that you contact [OIT HelpDesk](https://oit.utk.edu/) by phone at 865.974.9900 or [chat](https://liveutk-my.sharepoint.com/personal/utkirb_utk_edu/Documents/HRPP/Admin%20Procedures/oit.utk.edu/chat) to schedule a consult before you design or launch your survey, to prevent these issues from arising.

1. **Recruiting on Social Media for an Online Survey**
	* When posting a recruitment message on social media, upload the message as JPEG rather than text. This prevents bots from scrapping the post for data and auto filling surveys. The IRB requests that recruitment messages be submitted to iMedRIS as Word documents because they are easier for us to review in that format. However, after the IRB has approved the recruitment messaging, it can be uploaded online as a JPEG file.
2. **Options available in Qualtrics to Reduce Bots and Scams in Online Surveys**

*Open “Survey Options” in Qualtrics:*

* + Select “Bot Detection” to flag suspicious responses
	+ Select “Prevent Ballot Box Stuffing” to prevent participants from taking the survey more than once
	+ Add Captchas requesting participants to select the certain items in an image as additional protection (i.e. cars in a picture of a street)
	+ If you are recruiting multiple groups to participate in your survey, add a unique identifier to the end of the URL to create unique links for each group. For example, if you post on Facebook, twitter, and Instagram, set up each post to have a unique end identifier. Then, if one gets hacked you only have to shut down one link, leaving the others to collect data.
	+ If you have a follow-up survey collecting information for compensation, turn on http referrer option in compensation survey to block access unless the respondent is coming from the main survey.

**TIP:** For further questions on Qualtrics options for fraud protection click the following [link](https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/) or contact OIT HelpDesk.

1. **Designing the Survey to Identify Bots by Responses**
	* Add attention checks throughout the survey (i.e. same question twice or worded differently)
	* Repeat qualifying questions at the beginning and end to screen against bots (i.e. are you a student? Are you 18 years or older?)
	* Add a select all that apply question asking participants how they heard about the study and provide options where you did not post a recruitment script/flyer (i.e. craigslist or reddit)

If you have further questions about setting up a survey in Qualtrics to protect against bots please contact [OIT HelpDesk](https://oit.utk.edu/) by phone at 865.974.9900 or [chat](https://liveutk-my.sharepoint.com/personal/utkirb_utk_edu/Documents/HRPP/Admin%20Procedures/oit.utk.edu/chat).