 doi:10.20944/preprints202203.0243.v1

Communication

The Wasps are Clever: Keeping Out and Finding Bot Answers in Internet Surveys Used for Health Research

Julii Brainard [1,*], Kathleen Lane [2], Laura Watts [2] and Diane Bunn [2]

[1] Norwich Medical School, University of East Anglia Norwich NR4 7TJ, United Kingdom
[2] School of Health Sciences, University of East Anglia Norwich NR4 7TJ, United Kingdom; kathleen.lane@uea.ac.uk; l.watts1@uea.ac.uk; d.bunn@uea.ac.uk
* Correspondence: j.brainard@uea.ac.uk

Abstract: Automated software bots infiltrate online surveys and corrupt data integrity, not to mention waste researcher time and budgets. Although resources exist to help keep bots out and identify bots when they do evade survey barriers, bot attacks may be a persistent problem for online surveys for a long time to come. Bots are evolving -- even as survey designers try ever more sophisticated methods to fend them off and weed their answers out. Vigilance needs to be high and the bot generators should not be under-estimated. We recount here some bot features we encountered after our own survey was attacked that helped to identify them, and that have not been detailed elsewhere. We also discuss reasons why commonly recommended strategies for how to keep bots out may not be feasible for many scientific researchers.

Keywords: data analysis; surveys and questionnaires; internet; social class

The Internet has brought many wonderful things but also its own special headaches. Health researchers can quickly and easily invite large numbers of potential human research subjects to give us some of their data via online surveys, but the same technology makes it relatively easy for survey respondent data to be simulated by anyone with dishonest motives.

Here we describe our experiences dealing with bot (automated software 'robot') answers when trying to undertake an online survey of residential care home staff during the covid pandemic. As recently as 2015 [1], bot answers were a minor theme in discussion of online survey data quality, but now deliberately fake rather than merely 'insincere' respondents are a central problem topic.

Our experience of bots infiltrating an online survey is therefore not novel, but it is evident that that refreshed observations are useful to share, just as bot technology and methods themselves are also evolving. We considered ourselves experienced researchers who had run online surveys previously without bot problems, but we were still caught out. We hope that recounting our experience may help others to be more aware and prepared – at least in the near future.

Context: Research study for which the online survey collected data

Our health and social care research project focused on residential care homes (CHs) for older adults during the COVID-19 epidemic in the United Kingdom. We wanted to ask staff, resident and family member about their experiences in a mixed methods study design: large online survey of staff and detailed interviews. The online survey was intended to be a key recruitment vehicle for potential interviewees.

In the UK, CH staff typically come from socio-demographic groups that tend to be under-represented in health research [2]. Their occupation is considered low skill and historically has been relatively poorly paid [3]; carers are often employed on insecure ("zero hours") contracts and given few training or career progression opportunities [4].

 doi:10.20944/preprints202203.0243.v1

In designing our recruitment strategy, we were concerned that many of our target participants would be *unable* to answer: either due to lack a suitable internet-enabled device (phone or tablet, etc), or lack of a cheap data package / access to wifi to enable them to answer at no cost. Moreover, this workforce seemed likely to have less rather than more leisure time compared to many socio-demographic groups. Therefore, the survey was designed to be concise, in plain English and, given these participants might be hard-to-reach, we added an incentive in the form of a shopping voucher (value GBP 10) to be allocated at random to ten respondents after survey closed. Our survey ran for 4 months, Aug – Nov 2021. We were required by our institution to use a survey platform that conformed with General Data Protection Regulation (GDPR 2018) legislation. The GDPR-compliant and free (to our project) survey platform supported by our Institution was Microsoft Forms.

Recruitment for the survey was done through advertisements on social-media channels (Twitter and Facebook), email distribution lists, bulletins and newsletters which reach care-home workers (which include Care Workforce; CHAIN eNewsletter; care-home eNewsletters; Adult Social Services eNewsletters for their workforce).

Bot Detection

At survey close, we had 1147 survey responses, 47% of which were submitted in the preceding 4 weeks. Unfortunately, we soon realised that many survey responses were fake, coming from bots rather than human beings. After identifying both hard red flags (eg., impossible phone numbers) and soft flags (eg., duplicated formatting of contact detail) we were left with 115 valid responses –10% of the raw set of original total received.

To reward or not?

It is widely believed that offering a reward for filling in surveys will attract bots, "like wasps to a jam jar," as summarised by one colleague. However, *not* offering a reward is no guarantee of no bot answers. There are at least three reasons that no-reward surveys may still attract bots:

- Bots are cheap to run. It's low effort to deploy them at even seemingly no-reward surveys
- No reward stated in advertising material doesn't mean there isn't a reward after all. From the perspective of a bot profiteer, it's worthwhile to send the bot through the questionnaire just in case
- Bots often deploy artificial intelligence algorithms (AI) to answer open-ended questions and even to help choose multiple choice answers: no-reward surveys are still training opportunities for AI engines

It is up to individual research teams to decide if offering a completion reward would help achieve their target recruitment. There is a debate about whether some surveys actually attract higher response rates than when no reward is offered. We can report that our genuine respondents were much less likely (than bots) to leave any contact details for the reward voucher. We have described why we felt that our targets could be hard to reach and the reward was offered to incentivise participation. We also note that many commercial survey organisations such as IpsosMori or Yougov routinely pay respondents to take surveys. We have spoken to colleagues who use these platforms to collect survey data and stated that their respondents were therefore 'unpaid' and thus the respondent pool is bot resistant. However, these colleagues were unaware that these platforms do in fact promise an (admittedly) small reward for each survey completion.

Lessons Learned

Similar to anti-bot strategies adopted by other researchers [5, 6], ultimately our team applied customised decision rules to identify and eliminate bot answers. We don't share our rules very specifically, lest they become known and useful to bot writers trying to

 doi:10.20944/preprints202203.0243.v1

evade detection. Nevertheless, we believe it may be useful to share some observations about what we learned, that they may help other online surveyors and that we have not seen described elsewhere, or at least not as fully:

- Our bots deployed a diversity of strategies with some stochastic ways of answering the questions, so were not easy to spot in successive runs, or from answer patterns alone. An attention-check question caught 200 fake entries, but missed over 700. This is probably because bots can be trained with human input; there is easily accessible bot-training advice online. There are mathematical algorithms for finding bot answers in surveys [7], but these rely on technical skills that won't be present in many researcher teams; and bots may be evolving to evade these pattern checking tests, anyway. It was evident that our survey had at least 4 bot waves and probably different bot projects that attacked it (so different algorithms in how they answered). One of the email addresses supplied was traced back to a project management website (for big software projects). We believe that at least some of the bot attacks were linked to someone using this website to manage their bot software.
- We found clustering such as very similar completion/ start times clustered with other attributes. Bots often got fired at our survey in near identical start-time batches, and are observed elsewhere to often be fired out from server "farms" [8].
- Bot greed can be its own undoing; it's much easier to find bot answers when you have lots of them, to reveal their answer patterns, than if you only have a few bot answers.
- Revealing were strange comments entered in the open text part of the survey (where respondents were invited to add address infection control in care homes). Bot comments tended to be written like slogans and they used (luckily for us) irrelevant phrases such sanatoriums, convalescents, pets and repeat phrases (i.e., identical phrases were repeated by ostensibly different respondents).
- Some of the repeat phrases in response to open text questions were strange but seemingly innocuous, like "temporarily no". This was not obviously from a fake human; we believe these were test phrases to see what the field might accept without terminating out of the survey completely.
- Not all bot answers try to get a reward. Many of our bot respondents were seemingly test runs where the bot learned how to answer the survey in a sufficiently varied and possibly credible way, and to navigate the full range of questions in the survey. These learning bots most often did not leave contact details for the reward offer, although in general, bots did leave contact details more often than real respondents did.
- Some survey platforms keep out bots better than others. The platform we used did not capture IP addresses; IP addresses can be used to identify high numbers of surveys submitted from the same domain or a group of related domains. Similarly, only some survey platforms (not ours) deploy a 'Captcha' feature. The general wisdom at this time of writing is that 'Captcha' features are hard for Bots to fill in correctly, although it seems likely this hurdle will be surmounted soon enough.
- AI is still an emerging technology; AI-trained survey bots lack the diversity of human experiences and can't *yet* easily answer questions that can be described as requiring "executive function", such as "Choose the word which is a black bird from: horse, cat, goose, crow, parakeet, dog". Moreover, cultural references may completely defeat them for many years. As future Bot filter, we considered a question like "When was Adele prime minister? Answer choices: 1984-1987; 1991-1996; 1897-1903; 2013-2015; never."
- We noted a tendency for bots to give answers nearer the start than end of a list. We deduce that bot programmers have learned that survey designers tend to put their most common answers near the start of a list. Putting an impossible answer at the start of a list may catch some bots out.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 17 March 2022 doi:10.20944/preprints202203.0243.v1

- Misspelling in open-text answers. Real people often mistype and misspell, certainly more often than bots misspell . This seems mildly ironic given we had hints that at least some of our bot waves were managed by non-English speakers, such as complete Open Text answers in not Latin alphabet.

From a selection of available publications and online advice web pages, Table 1 list actions recommended to prevent or identify bot answers. However, we note that such a list cannot be complete or finalised. Some of the suggestions are also problematic to implement in scientific research. The available survey platforms may not offer a desirable bot prevention feature (such as captcha [9], respondents' IP addresses, click times, or completion times). Health scientists are subject to scrutiny by strict Institutional (Ethics) Review Boards (IRB). An IRB may take a dim view of all respondents being asked to give home address [10] as unnecessarily personal data collection. With regard to scientific merit and research targeting marginalised social groups, hard-to-reach research subjects may simply not be interested enough to continue with duplicate questions or multiple survey participation hurdles. The hard-to-reach may also be under-represented in existing panels of vetted prospective respondents. Individuals who fall under the 'hard to reach' descriptor may by their very nature, be more likely to use unusual wordings or phrases such that they could supply what seem like 'odd' answers to open text questions -- or at least 'odd' sounding to conventionally educated academics. Technical skills may not be present within a research team to undertake robust statistical analysis of survey answers, and the methods may anyway not be able to distinguish unusual genuine from false answers [7]. However, most problematically, if we can find information in the public domain about how to prevent and detect bot answers - then bot creators can find the same information and plan how to better hide themselves. Therefore, our key advice is fundamentally to maintain vigilance: assume that bots will try to infiltrate any online survey, reward-offering or not. Multiple strategies should be deployed both to try to keep them out and to look for them among the survey responses received.

Addendum: Our survey of nominal care-home staff asked if respondents would be available for interview. Bots often left their details here, too. We received some odd and terse replies to the interview invitation from email addresses subsequently identified as bots, such as "Where's my voucher?" (complete reply). Not only are the bots rife, they lack social graces, rather like certain jam-loving stinging insects.

Table 1. Examples of Bot Fighting advice.

Bot-fighting Advice	Source
To keep bots out completely	
Add extra validation checks (such as home addresses or email registration) before survey can commence	Pozzar et al. (2020) [8] Storozuk et al. (2020) [10]
Work with panel organisations that have pre-vetted that all invited respondents are real people	https://www.infosurv.com/some-bot-or-somebody-whos-taking-your-online-survey
Captcha features, including advanced versions	https://www.iths.org/news/how-to-protect-your-surveys-from-spam Kennedy et al. (2021) [9]
Do not offer a reward upon completion	https://www.surveymonkey.co.uk/mp/survey-prizes-pros-and-cons Storozuk et al. (2020) [10]
Look for excessive submissions from same or very similar IP addresses; Blacklist repeat offender ISPs	Storozuk et al. (2020) [10] Kennedy et al. (2021) [9] https://verstaresearch.com/blog/how-many-bots-took-your-survey/
Simple (low implementation skill, simple flag) detection methods	
Attention check and cognitive skill questions	Griffin et al. (2021) [5]
Hidden questions – some platforms allow questions to be written that only bots but real humans can't see	https://www.psychstudio.com/articles/bots-randoms-satisficing/#honeypot-method Pozzar et al. (2020) [8]
Less simple detection strategies	
Validate contact details, or at least, that they are a valid format	https://www.ipqualityscore.com/articles/view/67/8-methods-to-prevent-market-research-fraud

 doi:10.20944/preprints202203.0243.v1

Add repeat questions for consistency, especially if phrased slightly differently such as "How old are you" and "in which decade were you born"	Kennedy et al. (2021) [9] https://www.ipqualityscore.com/articles/view/67/8-methods-to-prevent-market-research-fraud
Look for illogical linked answers, such as a 20 year old person saying they had 15 years of driving experience	Teitcher et al. (2015) [1]
Require open text answers; Look for Identical or odd answers to open text questions	https://verstaresearch.com/blog/how-many-bots-took-your-survey/ https://www.ipqualityscore.com/articles/view/67/8-methods-to-prevent-market-research-fraud Storozuk et al. (2020) [10] Kennedy et al. (2021) [9]
Note the completion time (too long? Too short? Middle of the night?)	https://www.psychstudio.com/articles/bots-randoms-satisficing Storozuk et al. (2020) [10]
Sophisticated detection methods (high technical skills may be required)	
Statistical analysis of answer patterns, especially useful for very large survey datasets	https://www.psychstudio.com/articles/bots-randoms-satisficing Dupuis et al. (2019) [7]
Monitor click or page response times	Buchanan and Scofield. "Methods to detect low quality data and its implicataion for psychological research." *Behavior Research Methods* 50.6 (2018): 2586-2596.

Declarations

We declare that we have no competing interests.

Ethics: The research study for which the survey was run, Exploring and Understanding the lived experience in CAre homes for older people of Infection risk and transmission during the COVID-19 pandemic: a mixed-methods study to inform what we can learn for future infectious disease outbREaks (UCAIRE), was approved by the Faculty of Medicine and Health Sciences Research Ethics Committee at the University of East Anglia, reference 2020/21-148

Funding: All authors were funded by the UK National Institute for Health Research (NIHR) School for Social Care Research (SSCR), reference 102645/ER/UEAKL-P178. The views expressed are those of the authors and not necessarily those of the NHS, NIHR SSCR, UEA or the UK Department of Health and Social Care.

Acknowledgements: We are grateful to our UCAIRE scientific advisors and all of our genuine survey respondents, whose responses helped to distinguish the bot replies.

References:

1. Teitcher JE, Bockting WO, Bauermeister JA, Hoefer CJ, Miner MH, Klitzman RL. Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs. Journal of Law, Medicine & Ethics. 2015;43(1):116-133.
2. Bonevski B, Randell M, Paul C, Chapman K, Twyman L, Bryant J, Brozek I, Hughes C. Reaching the hard-to-reach: a systematic review of strategies for improving health and medical research with socially disadvantaged groups. BMC Medical Research Methodology. 2014;14(1):1-29.
3. Hussein S. "We don't do it for the money"… The scale and reasons of poverty-pay among frontline long-term care workers in England. Health & Social Care in the Community. 2017;25(6):1817-1826.
4. Allan S, Vadean F. The association between staff retention and English care home quality. Journal of Aging & Social Policy. 2021;33(6):708-724.
5. Griffin M, Martino RJ, LoSchiavo C, Comer-Carruthers C, Krause KD, Stults CB, Halkitis PN. Ensuring survey research data integrity in the era of internet bots. Quality & Quantity. 2021:1-12.
6. How to Battle the Bots Wrecking Your Online Study. 2019. Accessed Nov 25 2019.
7. Dupuis M, Meier E, Cuneo F. Detecting computer-generated random responding in questionnaire-based data: A comparison of seven indices. Behavior Research Methods. 2019;51(5):2228-2237.

 doi:10.20944/preprints202203.0243.v1

8. Pozzar R, Hammer MJ, Underhill-Blazey M, Wright AA, Tulsky JA, Hong F, Gundersen DA, Berry DL. Threats of bots and other bad actors to data quality following research participant recruitment through social media: cross-sectional questionnaire. Journal of Medical Internet Research. 2020;22(10):e23021.
9. Kennedy C, Hatley N, Lau A, Mercer A, Keeter S, Ferno J, Asare-Marfo D. Strategies for Detecting Insincere Respondents in Online Polling. Public Opinion Quarterly. 2021;85(4):1050-1075.
10. Storozuk A, Ashley M, Delage V, Maloney EA. Got bots? Practical recommendations to protect online survey data from bot attacks. The Quantitative Methods for Psychology. 2020;16(5):472-481.