[1] Nuffield Department of Orthopaedics, Rheumatology and Musculoskeletal Sciences (NDORMS), University of Oxford, Oxford, UK

Correspondence to: E Morrow
Eileen.Morrow@ndorms.ox.ac.uk

Cite this as: *BMJ* 2025;391:r2128
http://doi.org/10.1136/bmj.r2128

Threat of imposter participants in health research

Inconsistent detection risks undermining research integrity

Eileen Morrow, [1] Sally Hopewell, [1] Esther Williamson, [1] Tim Theologis[1]

Online recruitment has become central to modern health research. The speed and reach of internet based recruitment, particularly since the covid-19 pandemic, has transformed how we collect data.[1-3] However, alongside this digital transformation lies a growing and under-recognised phenomenon: imposter participants.

Imposter participants (sometimes called fraudulent or suspected participants)[4] provide deceptive or inaccurate data in order to take part in health research.[5] They can be divided into two categories: the first is humans who provide deceptive responses, such as lying about having the condition under investigation. The second is increasingly sophisticated automated computer software (bots) which mimic human behaviour and responses.[6] The undetected presence of imposter participants in quantitative datasets threatens the integrity of health research and, by extension, the policies and clinical decisions built on it.

Imposter participants were described as early as 2011.[7] However, articles investigating their prevalence in health research have grown in recent years. A 2025 scoping review found that 96% of identified studies describing methods to detect imposter participants had been published within the past five years.[8]

The motivations of imposter participants remain unknown, although a focus on financial incentives suggests that monetary benefit is a driver. Several authors have reported that suspected imposters often make multiple inquiries about the timing and format of payments.[9-11] However, not all studies that identified imposter participants offered financial incentives,[8] indicating that other motives contribute. Proposed alternatives include boredom, curiosity, or even an ideological intent to disrupt research.[4]

Health research now faces the same risks of fraud that have plagued non-health spaces such as market research.[12] However, the stakes are higher; health research informs clinical decisions, service design, and resource allocation. Results clouded by imposter participants may affect clinical treatment.

Problems for quantitative health research

The 2025 scoping review also reported that 18 of the 23 studies which looked for imposter participants in their datasets, found them.[8] The variance in the detected prevalence of imposter participants was notably wide, from 3%[13] to 94% in an online survey investigating communication during ovarian cancer treatment.[14]

The cancer treatment survey received 576 responses within seven hours, with most submitted between midnight and 4 am. The authors judged 94% of responses to be fraudulent and the remaining 6% suspicious, with no participant deemed unquestionably legitimate. As a result, they closed and relaunched the survey with stricter protocols to prevent imposter participants, yet continued to detect fraudulent responses.[14]

The problem extends beyond survey research. In the iDEAS randomised controlled trial[15] evaluating an alcohol reduction app, 76% of online enrolments were identified as bots at screening.[16] A further 4% of participants were identified as deceptive human respondents.[16] Without measures to detect imposter participants, such as face-to-face eligibility assessments, even intervention triallists may report large sample sizes with spurious results, not realising that much of their dataset is contaminated.

Approaches to tackle imposter participants

It is essential that researchers who recruit online critically evaluate their datasets for imposter participants. Various detection strategies have been proposed, including checking for implausible home addresses (eg, business or charity addresses)[16] or submissions from multiple formulaic email addresses (eg, surname-plus-two-digits@domain.com).[4] Proposed prevention strategies include identity verification procedures[17] or CAPTCHA tests (asking participants to complete a task such as to read and type distorted letters).[8] After the introduction of CAPTCHA tests in the iDEAS trial, no further bots were detected.[16] However, other reports indicate these tests do not prevent all bot submissions.[18] Researchers seeking further strategies should refer to recent reviews summarising published imposter detection and prevention approaches.[8 17]

Although these approaches make intuitive sense, their efficacy in preventing or identifying imposter participants is largely untested.[6 8 17] In addition, their effect on responses from marginalised communities, which online recruitment often targets, is untested.[19] For example, people living with stigmatised health conditions may be reluctant to submit to identity verification, and those with lower literacy skills may struggle with CAPTCHA tests.

Researchers should routinely integrate imposter participant detection and prevention into online research,[5] while considering the potential effect on their study population. At a minimum, studies should transparently report which safeguards were used and acknowledge their limitations, and journals should encourage consistent and transparent reporting of these safeguards. Funders and institutions should invest in infrastructure and training to help researchers keep pace with evolving tactics.[5] Clinicians and policy makers should be cautious

when interpreting studies that use online recruitment if imposter participant prevention is not mentioned.

Imposter participants are more than a nuisance; they are a systemic threat to health research. Their effect is demonstrable and their detection inconsistent. In an age where online recruitment underpins everything from randomised controlled trials to surveys,[2] they risk undermining the integrity of health research and the decisions built on it. The research community must acknowledge the problem and dedicate resources to testing and implementing safeguards. These steps are critical to ensure that the data guiding clinical care reflect the real patient voice.

Competing interests: *The BMJ* has judged that there are no disqualifying financial ties to commercial companies. The authors declare no other interests.

Provenance and peer review: Commissioned; not externally peer reviewed.

1 Dallison S, Munir S, Chubb E, etal. How have contemporary research studies used social media to recruit to digital self-help intervention research for young people's mental health?: a mapping review. *BMC Med Res Methodol* 2025;25:. doi: 10.1186/s12874-025-02636-9 pmid: 40877795

2 Darko EM, Kleib M, Olson J. Social media use for research participant recruitment: integrative literature review. *J Med Internet Res* 2022;24:e38015. doi: 10.2196/38015 pmid: 35925655

3 Kaur MN, Skolasky RL, Powell PA, etal. Transforming challenges into opportunities: conducting health preference research during the covid-19 pandemic and beyond. *Qual Life Res* 2022;31:-8. doi: 10.1007/s11136-021-03012-y pmid: 34661806

4 Garcia-Iglesias J, Heaphy B, Yodovich N, Atherton S, Merchant A. Imposter participants? Towards a reflexive epistemology of 'suspected participants'. *Int J Qual Methods* 2025;24:16094069251335497doi: 10.1177/16094069251335497.

5 Giles FC, McKenzie M, Kyei-Nimakoh M, Satyen L, Tarzia L, Hegarty K. Management of imposter participants when conducting online research with victim-survivors and perpetrators of violence. *Methodol Innov* 2025;18:-88doi: 10.1177/20597991251333345.

6 Pinzón N, Koundinya V, Galt RE, etal. AI-powered fraud and the erosion of online survey integrity: an analysis of 31 fraud detection strategies. *Front Res Metr Anal* 2024;9:1432774. doi: 10.3389/frma.2024.1432774 pmid: 39687573

7 Buchanan E, Aycock J, Dexter S, Dittrich D, Hvizdak E. Computer science security research and human subjects: emerging considerations for research ethics boards. *J Empir Res Hum Res Ethics* 2011;6:-83. doi: 10.1525/jer.2011.6.2.71 pmid: 21680978

8 Comachio J, Poulsen A, Bamgboje-Ayodele A, etal. Identifying and counteracting fraudulent responses in online recruitment for health research: a scoping review. *BMJ Evid Based Med* 2025;30:-82. doi: 10.1136/bmjebm-2024-113170 pmid: 39715631

9 Sharma P, McPhail SM, Kularatna S, Senanayake S, Abell B. Navigating the challenges of imposter participants in online qualitative research: lessons learned from a paediatric health services study. *BMC Health Serv Res* 2024;24:. doi: 10.1186/s12913-024-11166-x pmid: 38867177

10 Pellicano E, Adams D, Crane L, etal. Letter to the Editor: a possible threat to data integrity for online qualitative autism research. *Autism* 2024;28:-92. doi: 10.1177/13623613231174543 pmid: 37212144

11 Ridge D, Bullock L, Causer H, etal. 'Imposter participants' in online qualitative research, a new and increasing threat to data integrity?*Health Expect* 2023;26:-4. doi: 10.1111/hex.13724 pmid: 36797816

12 Murdoch-Gibson S. Here for the incentive: recognizing and rooting out fake respondents. QRCA Views. 2022. https://www.qrcaviews.org/2022/03/02/here-for-the-incentive-recognizing-and-rooting-out-fake-respondents/

13 Guest JL, Adam E, Lucas IL, etal. Methods for authenticating participants in fully web-based mobile app trials from the iReach project: cross-sectional study. *JMIR Mhealth Uhealth* 2021;9:e28232. doi: 10.2196/28232 pmid: 34463631

14 Pozzar R, Hammer MJ, Underhill-Blazey M, etal. Threats of bots and other bad actors to data quality following research participant recruitment through social media: cross-sectional questionnaire. *J Med Internet Res* 2020;22:e23021. doi: 10.2196/23021 pmid: 33026360

15 Oldham M, Beard E, Loebenberg G, etal. Effectiveness of a smartphone app (Drink Less) versus usual digital care for reducing alcohol consumption among increasing-and-higher-risk adult drinkers in the UK: a two-arm, parallel-group, double-blind, randomised controlled trial. *EClinicalMedicine* 2024;70:102534. doi: 10.1016/j.eclinm.2024.102534 pmid: 38685934

16 Loebenberg G, Oldham M, Brown J, etal. Bot or not? Detecting and managing participant deception when conducting digital research remotely: case study of a randomized controlled trial. *J Med Internet Res* 2023;25:e46523. doi: 10.2196/46523 pmid: 37707943

17 Merchant AA, Atherton S, García-Iglesias J. Imposter participants: a call for social science intervention. *Sociol Res Online* 2025;0:13607804251340013.doi: 10.1177/13607804251340013

18 Goodrich B, Fenton M, Penn J, Bovay J, Mountain T. Battling bots: experiences and strategies to mitigate fraudulent responses in online surveys. *Appl Econ Perspect Policy* 2023;45:-84. doi: 10.1002/aepp.13353

19 Drysdale K, Wells N, Smith AKJ, Gunatillaka N, Sturgiss EA, Wark T. Beyond the challenge to research integrity: imposter participation in incentivised qualitative research and its impact on community engagement. *Health Sociol Rev* 2023;32:-80. doi: 10.1080/14461242.2023.2261433 pmid: 37786312