

International Journal of Social Research Methodology

ISSN: 1364-5579 (Print) 1464-5300 (Online) Journal homepage: www.tandfonline.com/journals/tsrm20

The FIT framework for mitigating participant fraud in online surveys: a synthesis of two international LGBTQ+ social research case studies

Ashley S. Brooks , Tin D. Vo & Shelley L. Craig

To cite this article: Ashley S. Brooks , Tin D. Vo & Shelley L. Craig (29 Oct 2026): The FIT framework for mitigating participant fraud in online surveys: a synthesis of two international LGBTQ+ social research case studies, International Journal of Social Research Methodology, DOI: 10.1080/13645579.2026.2751627

To link to this article: https://doi.org/10.1080/13645579.2026.2751627

Published online: 29 Oct 2026.

Submit your article to this journal

Article views: 30

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=tsrm20

INTERNATIONAL JOURNAL OF SOCIAL RESEARCH METHODOLOGY
https://doi.org/10.1080/13645579.2026.2751627

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

Check for updates

The FIT framework for mitigating participant fraud in online surveys: a synthesis of two international LGBTQ+ social research case studies

Ashley S. Brooks, Tin D. Vo and Shelley L. Craig

Factor-Inwentash Faculty of Social Work, University of Toronto, Toronto, Ontario, Canada

ABSTRACT

Participant fraud poses a growing threat to international LGBTQ+ social research, yet existing mitigation recommendations are fragmented and inconsistent across the literature. This paper addresses this gap by synthesizing insights across two case studies of international surveys on LGBTQ+ populations compromised by fraud. Case study 1 ($N = 1,707$) details a preventative screening process in a survey about LGBTQ+ leisure spaces, combining Qualtrics security tools with geolocation and email checks. Case study 2 ($N = 3,681$) outlines an eliminative strategy in an LGBTQ+ video gaming survey using 10 fraud indicators analyzed using unsupervised machine learning. Each study found fraud rates of 43–45% ($n = 2,540$) and fraud check utility varied across studies. Practical context-dependent recommendations and future research directions are synthesized into the feasibility, inclusion, trustworthiness (FIT) framework, emphasizing methodological and ethical trade-offs between competing research demands and the need for dynamic and tailored mitigation strategies.

ARTICLE HISTORY
Received 14 July 2025
Accepted 14 October 2026

KEYWORDS
Participant fraud; survey bots; data integrity; machine learning; LGBTQ+

Introduction

Online surveys have become a cornerstone of social science research because they are cost-effective, fast, and convenient (Evans & Mathur, 2005). Despite these advantages, data quality can be inconsistent due to satisficing (i.e. choosing superficially adequate rather than carefully considered responses), careless responding (e.g. not reading instructions properly), malicious responses (e.g. targeted hate speech), and other undesirable respondent behaviors that generate measurement error, threaten validity, and delay knowledge production (Krosnick, 1991; Meade & Craig, 2012; Smith et al., 2025).

Of growing methodological concern in online survey research are fraudulent research participants – bad actors who take dishonest actions to participate in research studies with the purpose of extracting incentives (e.g. gift cards). Unlike other forms of careless and malicious response, fraudulent respondents use deliberate misrepresentation and are primarily financially motivated – for example, falsely claiming to be eligible for a study or programming bots – short for 'robots' – to autonomously search for and complete online

CONTACT Ashley S. Brooks ashley.brooks@utoronto.ca Factor-Inwentash Faculty of Social Work, University of Toronto, 246 Bloor Street West, Toronto, ON, M5S 1V4 Canada

© 2026 Informa UK Limited, trading as Taylor & Francis Group

surveys, with the intent to redeem participant incentives (C. Kennedy et al., 2021; Prince et al., 2012; Storozuk et al., 2020). Because fraudulent participants often do not meet eligibility criteria and may not even be human, their data are invalid. If undetected, fraudulent participants can misappropriate thousands of dollars in participant incentives (Nur et al., 2024; Sterzing et al., 2018) and contribute to paper retraction (Farquhar-Leicester et al., 2022).

While there are important practical and ethical imperatives to prevent fraudulent participants from receiving incentives intended for genuine participants (Griffin et al., 2022; Pullen Sansfaçon et al., 2024; Teitcher et al., 2015), excessive measures to curtail fraud can create unacceptable barriers to participation (Ménard et al., 2025) and result in genuine participants being incorrectly excluded (Garcia-Iglesias et al., 2025). Tensions between feasibility, inclusion, and data trustworthiness – collectively referred to here as FIT – are especially pronounced in online surveys recruiting hard-to-reach lesbian, gay, bisexual, trans, queer, and other sexual and gender diverse (LGBTQ+) people (Craig et al., 2017). Financial incentives and social media-based recruitment are often essential for recruiting LGBTQ+ participants (McInroy, 2016) but make such studies targets of fraud. Some preventative fraud mitigation approaches, such as identity verification checks (C. K. Campbell et al., 2022), may deter prospective LGBTQ+ participants due to privacy concerns. Conversely, some eliminative approaches, such as cross-referencing demographic details, risk incorrectly excluding genuine participants who authentically report different identity labels at different timepoints (A. Campbell et al., 2021). Given these challenges, there is need for participant fraud mitigation guidance; however, recommendations are fragmented across case studies (Bybee et al., 2022; Griffin et al., 2022; McKinnon et al., 2025; Ménard et al., 2025; Shaw et al., 2025; Sterzing et al., 2018), with limited methodological synthesis.

Addressing this gap through comparison and synthesis of case studies would improve the FIT of data integrity strategies in online survey research with LGBTQ+ populations. As such, this paper synthesizes developments in online survey fraud detection and mitigation over time and presents two case studies of online surveys of LGBTQ+ populations compromised by fraudulent participants. Each case study outlines the unique research context and initial fraud breach, details the bespoke multipronged fraud mitigation strategies employed, and recommends different fraud mitigation strategies. Finally, these recommendations are synthesized into a high-level FIT framework to aid researchers in balancing ethical and methodological demands with regard to participant fraud mitigation. Together, these case studies address the research question: How can researchers mitigate participant fraud in LGBTQ+ online surveys, and what are the ethical and methodological implications of their approaches?

The changing landscape of participant fraud mitigation

Online survey research has always been vulnerable to participant fraud, but it became increasingly common in the late 2010s with the growing popularity of social media (Green et al., 2021) and platforms such as Amazon Mechanical Turk (R. Kennedy et al., 2020). This emergent problem prompted a wave of scholarship advancing easily implemented 'gold-standard' survey features and data checks that could mostly prevent or eliminate fraudulent participation altogether (Gadiraju et al., 2015, p. 1631).

Accordingly, participant fraud at this time was considered a minor risk (Hitches et al., 2024).

Today, many of these strategies are less effective due to rapid technological advancements. One common practice of checking internet protocol (IP) addresses to detect participants completing a survey multiple times or from ineligible geolocations (R. Kennedy et al., 2020) has been undermined by widespread adoption of virtual private networks (VPNs), a technology that hides a user's internet activity and location. Another gold-standard involved inserting a browser cookie into the survey session, which 'remembers' the participant and prevents repeat responses (e.g. Qualtrics' 'ballot box stuffing' feature) (Hardesty et al., 2024) – but this can be circumvented by clearing a browser's cache or using a private or incognito window. Recent quasi-experimental findings also point to the declining effectiveness of Turing tests known as CAPTCHAs (Simone et al., 2023), once described as being, 'at the forefront of preventing bots from accessing surveys' (Yarrish et al., 2019, p. 242). CAPTCHAs present problem-solving tasks designed to be easily solvable by humans but difficult for bots. However, technological improvements have enabled bots to circumvent CAPTCHAs (Egel et al., 2010); correctly respond to attention checks (e.g. 'select the third response option'); ignore honeypot questions, which are hidden from human eyes using code but remain 'visible' as a trap for bots that read the underlying code (C. Kennedy et al., 2021); and generate human-like Likert scale responses (Irish & Saba, 2023).

The increasing sophistication of participant fraud – coinciding with the shift to online research in 2020 during the global coronavirus pandemic (Griffin et al., 2022) – precipitated another decline in online survey data quality, with one review of 36 studies between 2013 and 2023 suggesting that the percentage of usable responses dropped from 76% in 2019 to just 6% in 2020 (Pinzón et al., 2024). Accordingly, this has driven another recent wave of participant fraud research proposing a wide array of indicators for identifying potential participant fraud in online survey data (e.g. Bybee et al., 2022; Goodrich et al., 2023; Griffin et al., 2022; King-Nyberg et al., 2023; Storozuk, 2020), including: (1) responses initiated across consecutive minutes, (2) incoherent or nonsensical qualitative answers, (3) survey speeding, (4) suspiciously structured email addresses (e.g. firstname.lastname@domain.com), (5) inconsistent or implausible answers, and (6) failing proprietary fraud scores such as Qualtrics' RelevantID. Furthermore, a comparison of 31 fraud indicators showed that they vary in their effectiveness (Pinzón et al., 2024).

Consequently, this rapid proliferation of potential fraud indicators has generated confusion and overwhelm among researchers making decisions about which participants to exclude, how, and why. Rules of thumb have been proposed to reduce this complexity (e.g. excluding responses that fail 2 or more fraud checks (Buchanan & Scofield, 2018)), but Nur et al. (2024) note that 'no standard exists for adjudicating among different fraud checks to identify invalid responses' (p. 2), indicating a need for clarity. To address this, we describe two case studies that mitigated participant fraud in different ways and close with a synthesis of findings and recommendations across both case studies, organized within an overarching FIT framework.

Case study 1: the wellbeing and inclusion in recreation and leisure (WIRL) study

Background

The WIRL Study was a binational mixed methods survey exploring the relationship between intersectional discrimination in leisure spaces, resilience factors, and the social and mental wellbeing of LGBTQ+ communities (Vo, 2022). Between January and May 2021, the second author recruited LGBTQ+ individuals residing in Canada and the U.S.A. who were at least 16 years old, had participated in an LGBTQ+ leisure setting within the past two years, and could participate in English. The WIRL Study was approved by Wilfrid Laurier University's Research Ethics Board (REB#6710). Participants were recruited using emails to LGBTQ+ organizations and leisure groups across Canada and the U.S.A.; paid targeted ads on Facebook, Instagram, Her, and Grindr; and posts in Facebook groups, Twitter/X, and LinkedIn. Participants received $10 as compensation (noted on the recruitment poster) or had the option to donate the money to one of 10 LGBTQ+ organizations in Canada or the U.S.A.

Within 24 hours of recruitment beginning – despite implementing CAPTCHA – the survey unexpectedly received 167 responses with data features indicative of fraud, including response initiation across consecutive minutes, inconsistencies between the reported country of residence and IP address geolocations, irrelevant responses to open-text questions (e.g. giving the name of a lawn care company when asked about a leisure space), completion under 5 minutes, a single response option selected for most Likert scale questions, incorrect responses to attention checks, and mismatched birth year and age. To address this, data collection was suspended for one month before relaunching with a four-step fraud mitigation process aligned with recommendations from Nur et al. (2024): (1) participants completed a screener survey, a short preliminary questionnaire to confirm respondents met study inclusion criteria before accessing the full survey; (2) screener survey responses were inspected using a fraud indicator checklist; (3) acceptable respondents were assigned a unique identifier linked to their screener survey and emailed a single-use invitation to complete the full survey; and (4) the final data were reviewed using the fraud indicator checklist.

Fraud indicator checklist

Qualtrics security features

A license for Qualtrics' integrated security features was procured. All respondents completed a reCAPTCHA, which generates a score between 0 and 1, with scores less than 0.5 potentially indicative of a bot. Secondly, RelevantID generates a fraud score ranging from 0 to 130 for each respondent using machine learning of their behavioral data, browser history, and metadata (Bonett et al., 2024). Scores equal to or greater than 30 suggest that the response is fraudulent.

Logic and attention checks

Respondents reported their age and year of birth in separate sections of the screener survey and the full study survey and answers were compared for consistency. Demographic information was also checked for potential inconsistencies (i.e. self-

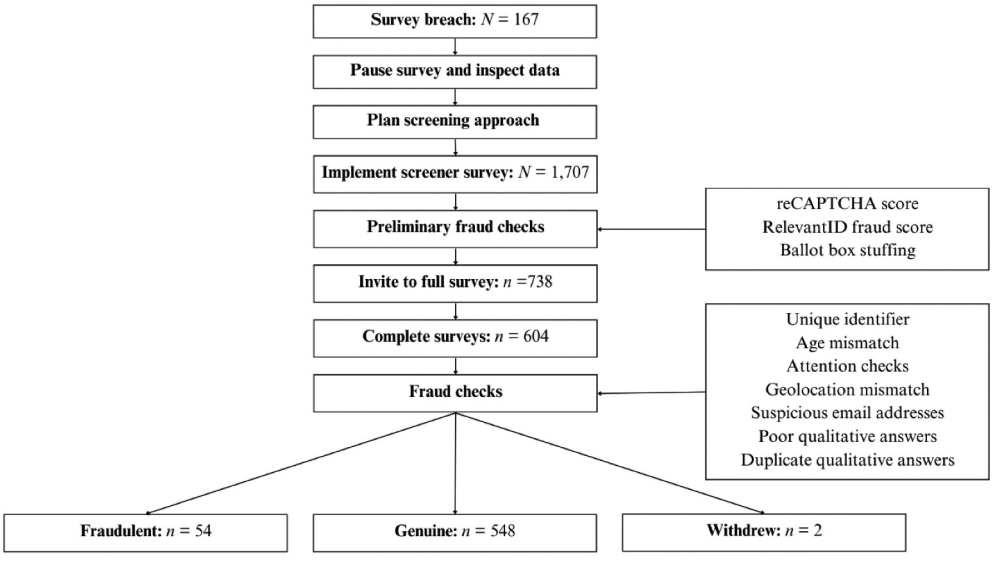


Figure 1. The WIRL study's preventative screening process.

identifying as a racialized person but selecting only 'White' as their racial identity). Participants also completed four attention check questions. Participants were asked, 'What does the fifth letter in LGBTQ2S+ stand for?', with the answer of 'queer' or 'questioning' being accepted. A comprehension question was implemented in the full survey, 'Miley Cyrus came in like a wrecking ball. Who came in like a wrecking ball?', with the correct answer being 'Miley Cyrus'. The third attention check in the full survey instructed participants to move a slider to the one-third position (i.e. 33%), with responses within 5% passing the check. The final attention check asked participants to select 'the word that represents many colors' (i.e. rainbow) out of four possible answers.

Geolocation checks

IP addresses were reviewed for geolocation to determine whether responses originated from Canada or the United States. IP addresses were also matched between the screener survey and the full study survey using the unique identifier.

Open-text answer checks

Answers to two qualitative questions, 'describe an experience of discrimination and the impact it had on you', and 'how did the COVID-19 pandemic affect your leisure experiences over the past year?' were inspected for relevance and coherence. Email addresses were reviewed to identify potentially suspiciously concatenated or random strings of characters and duplicate email addresses. The full screening process is shown in Figure 1.

Results

Of the 1,707 screener surveys, 90 (5.57%) were incomplete submissions and 879 (54.46%) were deemed fraudulent based on failing one of the Qualtrics fraud checks or a combination of the other checks (Table 1). Most of the screener survey responses

Table 1. Number of responses in the WIRL study failing each fraud check.

Fraud check	Screener survey excluded responses (%) *	Full survey excluded responses (%)
reCAPTCHA score < 0.5	64 (3.96%)	4 (0.54%)
RelevantID score ≥ 30	171 (10.58%)	4 (0.54%)
Logic and attention checks	146 (9.03%)	0 (0%)
Geolocation mismatch	122 (7.54%)	46 (6.23%)
Suspicious or incomplete email address	583 (36.05%)	0 (0%)
Poor qualitative answers	n/a	0 (0%)

*column total is more than the total number of excluded responses due to responses failing multiple fraud checks.

($n = 583$, 36.05%) that were considered fraudulent were due to suspicious/incomplete email addresses. Inspection of the Qualtrics fraud metrics and IP addresses resulted in the exclusion of 64 responses (3.96%) from reCAPTCHA, 171 responses (10.58%) from Relevant ID, and 122 responses (7.54%) from geolocation. Responses were also excluded if they failed one of the attention checks in addition to one other fraud check, resulting in 146 (9.03%) exclusions. In many instances, responses failed multiple fraud checks.

The remaining 738 (42.30%) respondents were emailed to complete the full survey with a unique single-use participant identifier. Of these, 662 respondents (89.70% response rate) initiated the survey, and 604 responses were fully completed, verified with their unique identifier, and subjected to further quality checks. Of the 604 responses reviewed from the full survey, 54 (8.94%) were determined to be fraudulent based on the predetermined criteria and 2 participants withdrew (Table 1). The fraudulent responses were primarily due to suspicious or missing geolocation ($n = 46$, 6.23%). Although several participants failed at least 1 logic and attention check in the full survey, these did not appear to co-occur with other fraud indicators and were not factored into data exclusions in the final survey.

Case study 1 discussion

Implementing a screener survey substantially improved the data quality of the WIRL study, with the incidence of suspected participant fraud decreasing from 54.26% at prescreening to 9.27% in the full survey, with a total fraud rate of 45.24%. Most fraudulent participants were flagged based on suspicious or incomplete email addresses at screening, corroborating findings that features of email addresses such as character length and structure can be used as potential indicators of participant fraud (Griffin et al., 2022; Pinzón et al., 2024). Though it is not possible to determine the extent to which issuing participant identifiers by email reduced participant fraud, 76 participants who were invited to participate were lost to attrition. It is plausible that the participant code mechanism added friction that bots could not easily bypass; however, this increased friction may also increase the dropout rate among genuine participants, potentially producing sampling biases. Similarly, while inconsistent geolocation between surveys accounted for most data exclusions after completing the full survey, there could be legitimate reasons for this discrepancy. Researchers should therefore consider exceptions to rules-based exclusion criteria.

While platform-level security features such as reCAPTCHA and Qualtrics' RelevantID provided some utility, they accounted for few exclusions and were not

sufficient in guiding exclusion decisions solely, reinforcing previous findings (Sophus & Mitchell, 2025). Logic and attention checks performed inconsistently depending on their task difficulty. While several participants failed attention checks, this did not coincide with other failed fraud checks, and open-ended responses indicated that many failures reflected confusion or high task difficulty. For example, one participant answered, 'not sure what is being asked' to the comprehension question. Several participants also struggled with the question requiring them to parse the LGBTQ+ character string, often answering with a correct word beginning with the adjacent incorrect letter. Such difficulty and confusion may lead to dropout, and we therefore recommend using attention checks strategically and not relying solely on them for LGBTQ+ study populations, among whom neurodivergence or literacy variation may be more common (Goetz & Adams, 2024). Altogether, this case study demonstrates the importance of flexibility in fraud detection protocols to balance fraud prevention with participant inclusion.

Case study 2: LEVEL UP! LGBTQ+ video gaming

Background

LEVEL UP! was a mixed methods international survey conducted by the International Partnership for Queer Youth Resilience (INQYR) (Craig et al., 2022) between April 2022 and January 2024. The survey was hosted on Qualtrics and explored: (a) motivations, preferences, behaviors, and experiences of LGBTQ+ youth who play video games; (b) how LGBTQ+ identities and experiences are represented in video games; and (c) how video games may contribute to LGBTQ+ youth wellbeing. Eligible participants were LGBTQ+ youth aged 14–29 who play video games regularly; live in Canada, the United States, the United Kingdom, Australia, or Mexico; and were able to participate in English or Spanish. The study received research ethics board approval from the University of Toronto Health Sciences Research Ethics Board (#41573). Several recruitment methods were used, including blanket emails to lists of LGBTQ+ organizations, promotional posts in private Facebook groups and Subreddits, and paid targeted ads on Facebook, Instagram, Twitter, and TikTok, which included the survey link, study inclusion criteria, and information about a prize draw for respondents to win one of 13 Amazon gift cards ranging from CAD 50 to 250 in value. The survey comprised six sections collecting: (a) demographics and a screenshot from a video game; (b) video gaming preferences and behaviors; (c) single-player gaming experiences; (d) negative and (e) positive experiences while playing multiplayer video games; and (f) email addresses to opt into the prize draw. Full study design and recruitment information is available elsewhere (DiCesare et al., under review).

Despite implementing reCAPTCHA and preventing ballot box stuffing, four months into data collection it became apparent that bots had infiltrated the survey when large numbers of responses were submitted in short periods of time and could not be accounted for by our recruitment efforts. Over 4,000 responses had already been collected by this time. Our Qualtrics license did not include the fraud detection metrics used in Case Study 1 and it is impossible to generate them retroactively. Given our need for data cleaning and the informative value of the fraudulent data in achieving this, we

continued with recruitment and developed a systematic multidimensional data cleaning protocol.

Data cleaning procedure

The survey collected 7,825 responses and, following exclusion of ineligible or incomplete responses, 3,681 responses were subjected to a battery of 10 quality checks by a team of three coders. During pilot testing, 1,400 responses were coded by counterbalanced coder pairs to reduce individual coder fatigue and ensure consistency between coders. The procedure yielded high inter-rater reliability (92.12–100%) across all coding categories, except for one fraud indicator – suspicious email address – which was dropped because coders could not establish consistent criteria for it in such a large sample. The remaining responses were single coded in Microsoft Excel as either 1 (fail) or 0 (pass).

Qualitative answer checks

Qualitative answers that did not match the question or were gibberish (i.e. random character strings) failed the qualitative answer quality check (C. Kennedy et al., 2021). Responses with no qualitative answers or duplicate qualitative answers failed respective checks. One example of an inspected qualitative question was, 'Name a video game character that you have identified with or related to and briefly describe how you identified with or related to them'.

Logic checks

Age was compared with year of birth, and responses with impossible values failed the age mismatch check. Secondly, answers to two questions about actual and ideal time spent video gaming per week were inspected to check for extreme or ineligible responses. Responses failed this check if they reported video gaming per week for 0 hours (i.e. ineligible), 70 or more hours (i.e. 90th percentile), or ideally playing for 168 or more hours a week (i.e. more than the number of hours in a week).

IP address checks

IP address geolocations were derived from an IP lookup service (https://www.showmyip.com/bulk-ip-lookup/), which was cross-referenced with the reported country of residence. Responses with incongruous information failed this check. IP addresses were also screened using a domain name system blacklist, CleanTalk (https://cleantalk.org/), a database of IP addresses with histories of sending email spam, botting, abuse reports, and unusual traffic (e.g. VPNs). Responses from an IP address on the blacklist failed this check. Finally, responses were inspected for duplicate IP addresses, with all duplicates failing this check.

Spamming checks

During survey testing, testers took approximately 30 minutes to fully complete the survey. Given that survey logic would skip sections of the survey in certain instances (e.g. sections (d) and (e) would be skipped if the respondent did not play multiplayer games), shorter response times were expected. Based on our testing of different response time thresholds (i.e. <5, <10, and <15 minutes) during data analysis, response times of

<10 minutes failed the speeding check. Finally, responses initiated in consecutive minutes failed the spamming check.

Analysis plan

A macro-micro analytic approach was taken to explore the macro-level patterns of fraud characteristic across the entire dataset and apply these findings at the micro-level to make data exclusions (Hitches et al., 2024). Fraud checks were analyzed in SPSS 29 using cluster analysis, an unsupervised machine learning approach to grouping objects with similar characteristics to each other into distinct clusters (Yim & Ramdeen, 2015). The 10 fraud check scores were analyzed using hierarchical agglomerative cluster analysis with the Ward method and squared Euclidean distances. These parameters minimize the amount of variance within clusters, so similar responses are clustered together, and maximize the amount of variance between clusters so clusters are distinct. This produces a tree-like dendrogram that illustrates how the algorithm clustered responses and a perpendicular cut point is made by visually inspecting the dendrogram for an interpretable and parsimonious clustering. Subsequent K-means cluster analysis was conducted to refine each cluster, describe their fraud characteristics, and determine the most effective fraud indicators to guide micro-level data exclusions. To assess confidence in the procedure, sensitivity analyses were conducted to compare the results of the macro-micro approach to rule-of-thumb-based exclusions, and the sample demographics were compared to assess face validity.

Results

Cluster analyses

The cut-off point was chosen at the 3,678th stage of the agglomeration schedule, with a linkage distance of 8 (Figure 1). Visual inspection of the dendrogram indicates that three distinct clusters formed, with the following number of observations in each cluster: Cluster 1: 1,116 responses (30.32%); Cluster 2: 1,652 responses (44.88%); and Cluster 3: 913 responses (24.80%).

The cluster centers (i.e. the mean score of each fraud check in each cluster) were used to initialize the K-means algorithm, which was set to form three clusters. The clustering converged after four iterations, resulting in the following final cluster assignments: Cluster 1: 695 responses (18.88%); Cluster 2: 1818 responses (49.39%); and Cluster 3: 1168 responses (31.73%). Cluster characteristics are shown in Table 2. Cluster 1 was characterized by the highest rates of non-response to qualitative answers, low response time, and spamming, suggestive of fraud. Cluster 2 showed low scores across all data checks, with some nominal duplication in answers to more closed qualitative questions (e.g. 'What types of features are you satisfied with in the characters that you've been able to create or select? (e.g. gender, skin tone, hair, voice)'), indicating genuine data. Cluster 3 demonstrated the highest rates of poor qualitative answers, duplicate qualitative answers, failure of logic checks, and spamming, suggestive of fraud. Clusters 1 and 3 also had the highest rates of mismatch between IP geolocation and reported country of residence. IP blacklisting and duplicate IP addresses were similarly common across all clusters.

Table 2. Change in cluster size between hierarchical and K-means cluster analyses, average number of failed fraud checks, and final cluster centers. The number of responses that failed each check are shown in brackets.

Cluster characteristics	Cluster 1 (n = 695)	Cluster 2 (n = 1,818)	Cluster 3 (n = 1,168)
% change	−24%	+12.71%	+4.66%
Average number of failed checks	2.47	0.66	3.78
Fraud check			
No qualitative answers	0.79 (546)	0.00 (0)	0.01 (7)
Poor qualitative answers	0.00 (2)	0.04 (73)	0.95 (1,112)
Duplicate qualitative answers	0.01 (7)	0.24 (437)	0.93 (1,088)
Age mismatch	0.19 (129)	0.01 (20)	0.30 (346)
Extreme playtime	0.12 (83)	0.07 (124)	0.14 (165)
Geolocation mismatch	0.22 (155)	0.05 (82)	0.29 (342)
IP blacklist	0.22 (154)	0.18 (319)	0.21 (251)
Duplicate IP addresses	0.06 (40)	0.03 (55)	0.07 (85)
Speeding	0.29 (205)	0.05 (86)	0.15 (178)
Spamming	0.57 (296)	0.00 (0)	0.72 (839)

Finally, fringe cases in each cluster failing between 1–3 of the checks were inspected with micro-level attention paid to the checks that were most discerning of Cluster 1 and Cluster 3 membership (i.e. no qualitative answers, poor qualitative answers, duplicate qualitative answers, and spamming). Responses in Clusters 1 or 3 that failed the poor qualitative answer check or any two of these other checks were deemed fraudulent. This resulted in a final distribution of 1,607 (43.66%) fraudulent responses and 2,074 (56.34%) genuine responses. As a sensitivity analysis, the clustering-based fraud classifications were compared with two rule-of-thumb exclusion thresholds (i.e. failing ≥ 2 or ≥ 3 fraud checks). Agreement with the rules of thumb was high ($\kappa = .81$ and .80, respectively) but each method produced different sample sizes: adopting the ≥2-fail threshold would have resulted in 356 additional, potentially false positive exclusions, whereas the ≥3-fail threshold would have retained 225 participants that we identified as likely fraudulent. Fraudulent responses were disproportionately from US-based, cisgender, heterosexual participants without reported disabilities or neurodivergence, whereas genuine responses reflected greater international, gender diverse, and neurodiverse representation. Sample demographics are shown in Table 3, and the cleaning process is shown in Figure 2.

Case study 2 discussion

Upon initial detection of fraud, we took a machine learning approach integrating several survey fraud indicators to study the macro- and micro-level fraud characteristics of the dataset. This novel use of cluster analysis contributes a flexible, scalable, and data-driven procedure for detecting participant fraud that may offer more precision than common rules-of-thumb. The process delineated two sub-samples that markedly differed: (a) a fraudulent sample characterized by high rates of spamming and deficient, duplicate, or absent qualitative answers emulating cisheteronormative, neurotypical, US participant characteristics; and (b) a genuine sample characterized by low-to-null scores on all fraud measures from participants disclosing a diverse array of sexual and gender diversity who were more equally distributed across countries.

Table 3. Participant demographics for the fraudulent and genuine LEVEL UP! data.

Variable	Fraudulent Data (n = 1,607)	Genuine Data (n = 2,074)
Country of residence		
Australia	146 (9.09%)	267 (12.87%)
Canada	286 (17.80%)	521 (25.12%)
Mexico	54 (3.36%)	305 (14.71%)
United Kingdom	145 (9.02%)	240 (11.57%)
United States	976 (60.73%)	741 (35.73%)
Gender Identity*		
Agender	275 (17.11%)	151 (7.28%)
Cis man/male	438 (27.26%)	337 (16.25%)
Cis woman/female	368 (22.90%)	399 (19.24%)
Man/male of trans experience	206 (12.82%)	137 (6.61%)
Woman/female of trans experience	116 (7.22%)	98 (4.73%)
Nonbinary	101 (6.29%)	693 (33.41%)
Gender fluid	60 (3.73%)	275 (13.26%)
Gender queer	236 (14.69%)	266 (12.83%)
Trans man/masculine	111 (6.91%)	405 (19.53%)
Trans woman/feminine	36 (2.24%)	156 (7.52%)
Two-Spirit	13 (0.81%)	21 (1.01%)
Muxe	0 (0%)	1 (0.05%)
Brotherboy	7 (.44%)	1 (0.05%)
Sistergirl	6 (0.37%)	0 (0%)
Other	6 (0.37%)	158 (7.62%)
Sexual/Romantic Orientation*		
Asexual	107 (6.66%)	372 (17.94%)
Aromantic	204 (12.69%)	143 (6.89%)
Bisexual	420 (26.14%)	680 (32.79%)
Demisexual	102 (6.35%)	270 (13.02%)
Gay	366 (22.78%)	407 (19.62%)
Lesbian	136 (8.46%)	318 (15.33%)
Not sure or questioning	56 (3.48%)	151 (7.28%)
Pansexual	98 (6.10%)	441 (21.26%)
Queer	171 (10.64%)	555 (26.76%)
Straight/heterosexual	294 (18.29%)	36 (1.74%)
Other	6 (0.37%)	116 (5.59%)
Disability or neurodivergence*		
None	1,058 (65.84%)	891 (42.96%)
Prefer not to answer	79 (2.18%)	181 (5.00%)
Vision (e.g. blindness)	91 (5.66%)	97 (4.68%)
Hearing (e.g. deafness)	97 (6.04%)	50 (2.41%)
Mobility	141 (8.77%)	184 (8.87%)
Head injury	108 (6.72%)	28 (1.35%)
Mental health condition	167 (10.39%)	757 (36.50%)
Stamina or breathing difficulty	57 (3.55%)	116 (5.59%)
Social, attention, or behavioral issues (e.g. ADHD)	147 (9.15%)	532 (25.65%)
Autism spectrum	88 (5.48%)	515 (24.83%)
Learning (e.g. dyslexia)	69 (4.29%)	191 (9.21%)
Communication or language disorders	45 (2.80%)	67 (3.23%)
Other	3 (0.19%)	125 (6.03%)

*Participants could select more than one option and percentages do not add up to 100%.

The demographics of the genuine data demonstrate better face validity than those of the fraudulent data. The data better reflects the expansiveness of LGBTQ+ individuals who use self-descriptors captured under the '+' suffix (e.g. non-binary, pansexual, asexual) or select 'other' and write-in options to describe their sexual orientation and gender identity (Garrett-Walker & Montagno, 2023; Pao et al., 2025). It also corresponds more closely with estimates that a third of LGBTQ+ youth meet the criteria for any mental disorder (Mustanski et al., 2010). Further, 40% of autistic adults report having a sexual orientation other than heterosexual and 10% report being a gender minority

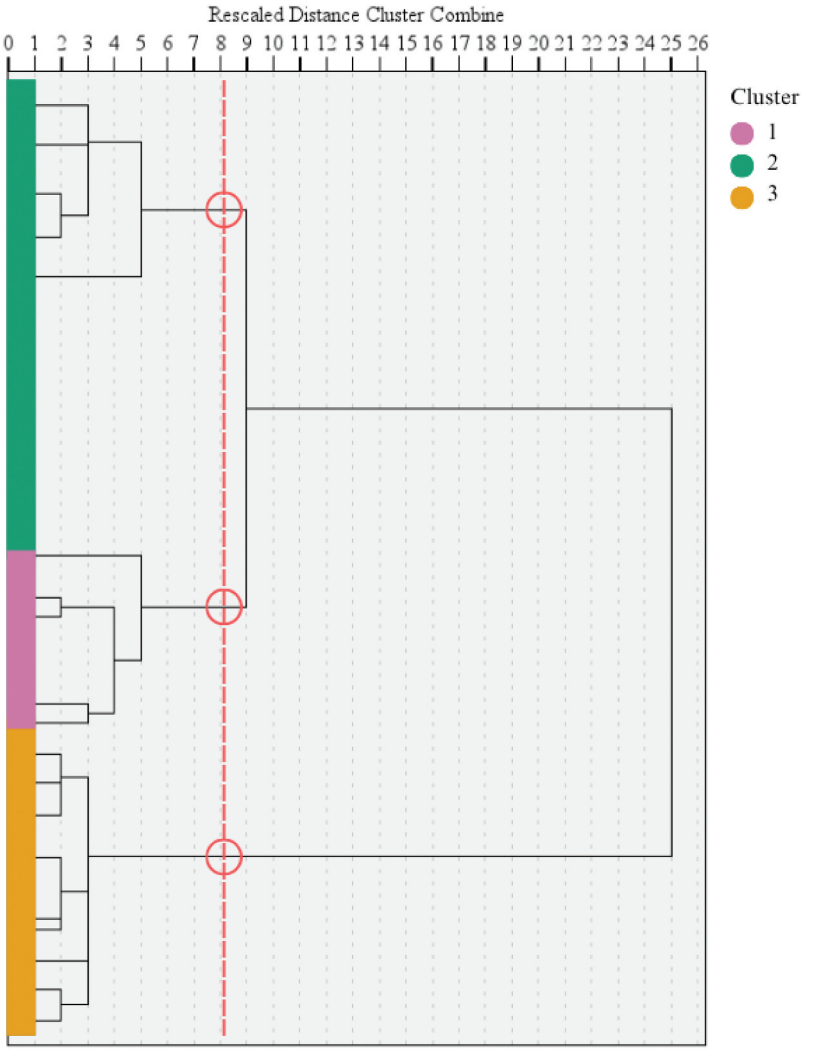


Figure 2. Dendrogram using Ward's distance, dashed line indicating cut-off point (linkage distance = 8).

(McQuaid et al., 2023) – proportions that align more closely with the genuine sample demographics. Similarly, approximately 14.5% of sexual minority and 23.9% of gender minority college students self-report an ADHD diagnosis compared to their heterosexual (7.5%) and cisgender (8.6%) counterparts (Orantes et al., 2025). Inversely, the demographics of the fraudulent sample contrast with previous research suggesting that fraudulent samples overestimate 'rare' LGBTQ+ demographic characteristics (Chandler & Paolacci, 2017), possibly suggesting changing fraud tactics over time. Indeed, findings from a more recent study of Latin American sexual minority men showed minimal demographic differences between fraudulent and genuine samples (Matos et al., 2025).

Confirming previous findings, we found that responses submitted over consecutive minutes and poor, duplicate, and absent qualitative answers were useful in identifying

fraudulent respondents (Bybee et al., 2022; C. Kennedy et al., 2021; Nur et al., 2024). Given individual differences in written language proficiency, qualitative answers should be appraised in concert with other fraud indicators to avoid sampling biases. More recent research has pointed to qualitative answers suspected of being generated by artificial intelligence (AI) and the pseudo-demand characteristics such answers exhibit, such as being overly verbose (Jean Louis & Thompson, 2025). While this issue was not observed in the LEVEL UP! study because most of the screened responses were collected before human-like AI chatbots became widely available, it is now likely essential to check for this also. Also consistent with recent research, we found that formerly effective logic, speeding, and geolocation checks were less useful for detecting fraudulent responses (Pinzón et al., 2024).

To our knowledge, this study is among the first to measure IP address blacklisting as part of a participant fraud detection protocol. IP address blacklisting was observed equally among genuine and fraudulent participants and was not an effective fraud indicator, which may be due to the unique ways in which LGBTQ+ respondents participate in online surveys. Due to their stigmatized identities, LGBTQ+ participants have enhanced needs for digital security and privacy and may be more likely to use VPNs (Geeng et al., 2022). Similarly, due to potential surveillance at home, LGBTQ+ youth could be more likely to participate using shared public networks (Macapagal et al., 2017). Because these behaviors may be flagged as suspicious traffic, IP blacklisting should not be used as a fraud indicator among LGBTQ+ survey samples. In summary, the findings emphasize the need to make data exclusions based on multiple concordant fraud indicators Figure 3.

General discussion

Across two case studies, we found participant fraud rates of 43–45% and demonstrated that researchers must devise multilayered and responsive participant fraud prevention strategies tailored to their unique research circumstances. This is most apparent in the case studies' diverging strategies, which were respectively implemented in a preventative (WIRL study) or eliminative fashion (LEVEL UP!) to respond to different circumstances (King-Nyberg et al., 2023). The use and effectiveness of different fraud checks also varied across the case studies (e.g. inspecting email addresses). As such, rather than making recommendations that may apply only to specific study contexts or someday become obsolete, we synthesize lessons learned from these case studies and propose a more generalizable framework for participant fraud mitigation.

Central to both case studies were methodological and ethical tensions between demands for feasibility (i.e. practical and resource constraints shaping what researchers can realistically implement), inclusion (i.e. preserving sample size and enabling genuine eligible participants to participate), and trustworthiness (i.e. validity, transparency, and integrity of the mitigation procedures and resulting dataset). Therefore, drawing on the project management triple constraints of cost, time, and quality (Atkinson, 1999), and complementing previous research advancing frameworks for conceptualizing participant fraud mitigation (Jean Louis & Thompson, 2025; Lawlor et al., 2021), we propose the Feasibility, Inclusion, Trustworthiness (FIT) framework, a dynamic mental model to help researchers understand how participant fraud mitigation involves inherent trade-offs

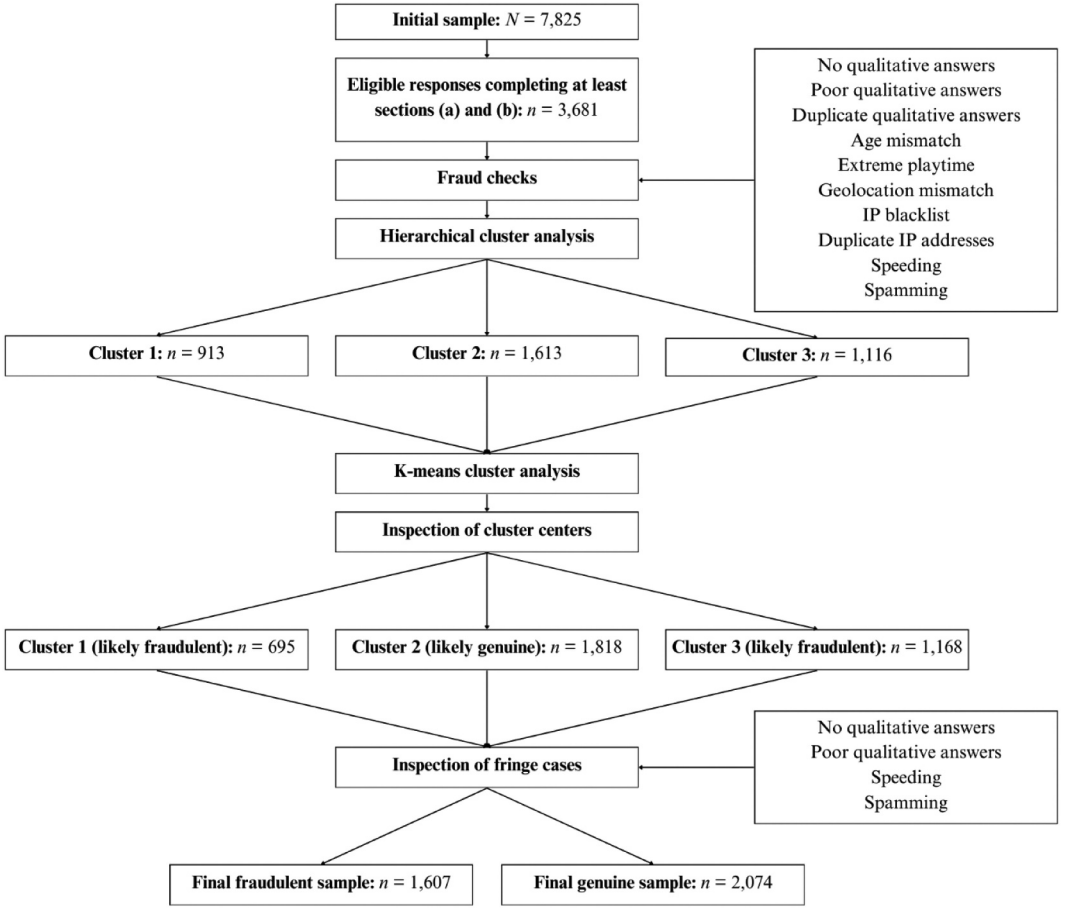


Figure 3. The LEVEL UP! study's eliminative screening process.

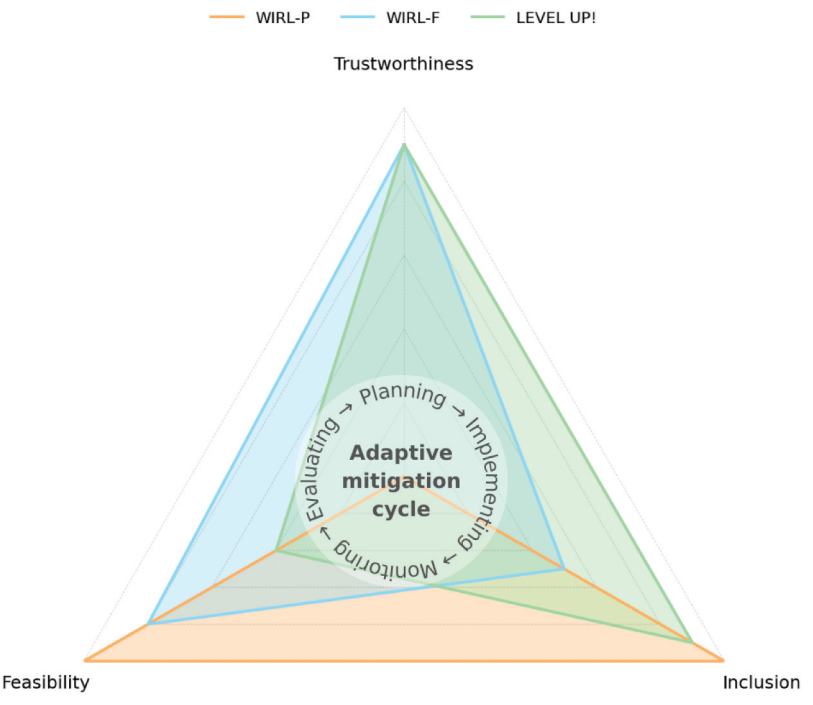


Figure 4. The feasibility, inclusion, and trustworthiness (FIT) framework approximating the FIT of the WIRL-P (pilot), WIRL-F (final), and level UP! studies.

between feasibility, inclusion, and trustworthiness (Figure 4). For example, it would be feasible and inclusive to publish an online survey with no pre-screening, but the collected data would not be trustworthy. Poor trustworthiness could be remedied using feasible pre-screening procedures, but pre-screening could reduce inclusion by introducing participation barriers. In turn, inclusion could be preserved through careful post hoc data cleaning, but this may not be feasible due to the significant resources this requires.

Further, the FIT framework emphasizes that the salience of these competing demands is dynamic, requiring iterative and adaptive decision-making throughout study planning, implementation, monitoring, and evaluation processes. To illustrate further, data trustworthiness became salient at different points in the WIRL (i.e. 24 hours) and LEVEL UP! (i.e. 4 months) studies. Consequently, this precipitated different responsive fraud mitigation strategies. Because the initial launch of the WIRL study collected no usable data, it was treated as a pilot study, and lessons learned were applied to collect more trustworthy data using preventative screening. This approach was feasible, but it diminished inclusion by introducing friction into recruitment procedures (e.g. multiple surveys, difficult attention checks). By comparison, the LEVEL UP! study had been successfully recruiting for several months and pausing the study would have impacted this. Fortunately, the research team had enough resources (i.e. several research assistants, statistical expertise) to painstakingly analyze the entire dataset for fraud. While this would be unfeasible for some, inclusion was preserved by not introducing barriers to participation. In summary, both case studies described adaptive and rigorous procedures to ensure the data were trustworthy, but the salience and fulfilment of demands for feasibility and inclusion

differed. Put simply: fraud mitigation strategies should FIT their unique and dynamic study contexts.

Future directions

The FIT framework also points towards a need for future participant fraud mitigation research to address feasibility, inclusion, and trustworthiness. Much of this research presently studies the trustworthiness of different fraud mitigation methods, but gaps remain. For example, future research is needed to evaluate proprietary automated fraud metrics such as Qualtrics RelevantID, of which little public knowledge exists. Such features cost thousands of dollars in license fees, yet their trustworthiness is not well-established in the literature (Bonett et al., 2024). Future research into automated fraud mitigation procedures is also necessary to address the demand for feasibility, given the significant manual efforts employed in both case studies to mitigate participant fraud. The unsupervised machine learning approach utilized in the LEVEL UP! study may provide a foundation for future supervised machine learning approaches utilizing labeled datasets of fraudulent and genuine participants – an approach widely used to detect social media bots (Aljabri et al., 2023). However, automated algorithmic decision-making also raises ethical concerns around inclusion, particularly for LGBTQ+ populations (McAra-Hunter, 2024), necessitating future research addressing tensions between feasibility and inclusivity in research involving marginalized participants. Finally, cutting across all three of these competing demands, research is urgently needed to address the emerging methodological frontier of so-called 'silicon' samples, AI-generated datasets created to emulate human participants (Sarstedt et al., 2024). While silicon samples are beyond the scope of this paper, we suggest that feasibility, inclusion, and trustworthiness tensions highlighted in the FIT framework will be implicated in their adoption and anticipate that future research will position silicon samples both as a potential tool for participant fraud mitigation *and* as a new form of participant fraud.

Limitations

There are some important limitations to highlight. First, the methods and FIT framework described here are intended to mitigate fraudulent participants such as survey speeders and bots and may not apply to other undesirable forms of participation, such as satisficing respondents. Although the FIT framework emphasizes data trustworthiness, it is impossible to say with certainty that the methods used here were successful in mitigating all participant fraud given the lack of a known correct answer to compare the findings against. Finally, fraudulent participation will likely change over time, and so the specific methods described in these case studies may be ineffective in the future, reaffirming the need for vigilance, adaptive decision-making, and ongoing information sharing in the research community.

Conclusion

Fraudulent research participation will continue to be a risk to online surveys that researchers must be prepared to mitigate. While multiple strategies and resources

must be employed to mitigate it with due diligence, researchers can exercise discretion in the strategies they use. Preventative screening can mitigate fraud risk as early as possible, but it can introduce barriers to participation. Yet, while eliminative screening can reduce these barriers, it can require significant resources. Researchers thus need to balance these demands for inclusion and feasibility with those of trustworthiness. The FIT framework may be a useful tool for orienting researchers towards participant fraud mitigation strategies suited for a given study context and informing future research directions.

Acknowledgments

Thank you to Zoe Ablett, Chase Staras, Emily Harle, Sheona Goodyear, and Renan Santiago for their research assistance.

Author contributions

CRediT: **Ashley S. Brooks:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Supervision, Visualization, Writing – original draft, Writing – review & editing; **Tin D. Vo:** Data curation, Investigation, Methodology, Writing – review & editing; **Shelley L. Craig:** Funding acquisition, Resources, Writing – review & editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The LEVEL UP! study was supported by a Partnership Grant from the Social Sciences and Humanities Research Council (SSHRC) under grant number #[895-2018-1000]. Shelley L. Craig is the Canada Research Chair in Sexual and Gender Minority Youth. The Wellbeing and Inclusion in Recreation and Leisure Study was supported by the SSHRC Joseph-Armand Bombardier Canada Graduate Scholarship Doctoral Award, Government of Ontario's Hilary M. Weston Scholarship, and Wilfrid Laurier University's Lyle S. Hallman Faculty of Social Work Dissertation Fund.

Notes on contributors

Ashley S. Brooks, PhD. is a social psychologist and the Research Associate for the International Partnership for Queer Youth Resilience (INQYR) at the Factor-Inwentash Faculty of Social Work, University of Toronto, Canada. He received his PhD. in 2017 from Anglia Ruskin University, UK, and adopts interdisciplinary perspectives to research prejudice towards LGBTQ+ communities, LGBTQ+ mental health and technology use, and LGBTQ+ research methods. Dr. Brooks is currently on the editorial board of the Journal of Sexual and Gender Diversity in Social Services and previously served on the editorial board for Psychology & Sexuality.

Tin D. Vo, PhD. is an assistant professor (CLTA) in community-based social work practice at the Factor-Inwentash Faculty of Social Work, University of Toronto. Dr. Vo completed Postdoctoral Fellowships at the Dalla Lana School of Public Health, University of Toronto and at Unity Health

Toronto. Dr. Vo's interdisciplinary, community-engaged research centres on social climate and exclusion as determinants of health with an emphasis on belonging, resilience/resistance, and overall wellbeing.

Shelley L. Craig, PhD. is the Canada Research Chair for Sexual and Gender Minority Youth, a Full Professor at the Factor-Inwentash Faculty of Social Work at the University of Toronto, and Project Director of the International Partnership for Queer Youth Resilience (INQYR). She has over twenty years of community-based leadership, practice and research with sexual and gender minority and marginalized populations. As a registered and licensed clinical social worker, Dr. Craig creates, delivers, and evaluates affirmative practice and effective services to individuals, groups and communities.

ORCID

Ashley S. Brooks http://orcid.org/0000-0003-4664-3784
Tin D. Vo http://orcid.org/0000-0002-5909-7789
Shelley L. Craig http://orcid.org/0000-0002-7991-7764

References

Aljabri, M., Zagrouba, R., Shaahid, A., Alnasser, F., Saleh, A., & Alomari, D. M. (2023). Machine learning-based social media bot detection: A comprehensive literature review. *Social Network Analysis and Mining*, *13*(1), 20. https://doi.org/10.1007/s13278-022-01020-5

Atkinson, R. (1999). Project management: Cost, time and quality, two best guesses and a phenomenon, it's time to accept other success criteria. *International Journal of Project Management*, *17*(6), 337–342. https://doi.org/10.1016/S0263-7863(98)00069-6

Bonett, S., Lin, W., Topper, P. S., Wolfe, J., Golinkoff, J., Deshpande, A., Villarruel, A., & Bauermeister, J. (2024). Assessing and improving data integrity in web-based surveys: Comparison of fraud detection systems in a COVID-19 study. *JMIR Formative Research*, *8*, e47091. https://doi.org/10.2196/47091

Buchanan, E. M., & Scofield, J. E. (2018). Methods to detect low quality data and its implication for psychological research. *Behavior Research Methods*, *50*(6), 2586–2596. https://doi.org/10.3758/s13428-018-1035-6

Bybee, S., Cloyes, K., Baucom, B., Supiano, K., Mooney, K., & Ellington, L. (2022). Bots and nots: Safeguarding online survey research with underrepresented and diverse populations. *Psychology and Sexuality*, *13*(4), 901–911. https://doi.org/10.1080/19419899.2021.1936617

Campbell, A., Perales, F., & Baxter, J. (2021). Changes in sexual identity labels in a contemporary cohort of emerging adult women: Patterns, prevalence and a typology. *The Journal of Sex Research*, *58*(5), 612–624. https://doi.org/10.1080/00224499.2020.1814092

Campbell, C. K., Ndukwe, S., Dubé, K., Sauceda, J. A., & Saberi, P. (2022). Overcoming challenges of online research: Measures to ensure enrollment of eligible participants. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, *91*(2), 232–236. https://doi.org/10.1097/QAI.0000000000003035

Chandler, J. J., & Paolacci, G. (2017). Lie for a dime: When most prescreening responses are honest but most study participants are imposters. *Social Psychological and Personality Science*, *8*(5), 500–508. https://doi.org/10.1177/1948550617698203

Craig, S. L., Eaton, A. D., Brooks, A. S., McInroy, L. B., Lozano-Verduzco, I., Austin, A., Dentato, M. P., Mendoza Pérez, J. C., & McDermott, D. T. (2022). Building bridges and breaking down silos: A framework for developing interdisciplinary, international academic-community research collaborations for the benefit of sexual and gender minority youth. *Psychology & Sexuality*. https://doi.org/10.1080/19419899.2022.2043421

Craig, S. L., McInroy, L., D'souza, S., Austin, A., Eaton, A., McCready, L., & Shade, L. (2017). Influence of information and communication technologies on the resilience and coping of

sexual and gender minority youth in the United States and Canada (project #Queery): Mixed method. *JMIR Research Protocols*, *6*(9), 1–11. https://doi.org/10.2196/resprot.8397

DiCesare, D. M., Brooks, A. S., Doll, K., McInroy, L. B., Lozano-Verduzco, I., Mendoza-Pérez, J. C., McDermott, D. T., Perry, Y., Schaub, J., Byron, P., Alessi, E., & Craig, S. L. (2026). Video gaming and psychological well-being among sexual and gender diverse youth in Canada, the United States, Mexico, the United Kingdom, and Australia: Protocol for a LEVEL UP! cross-sectional survey and screenshot elicitation interview study. *JMIR Research Protocols 15*, e95804. https://doi.org/10.2196/95804

Egel, M., Bilge, L., Kirda, E., & Kruegel, C. (2010). CAPTCHA smuggling: Hijacking web browsing sessions to create CAPTCHA farms. In *SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing* (pp. 1865–1870). https://doi.org/10.1145/1774088.1774483

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research*, *15*(2), 195–219. https://doi.org/10.1108/10662240510590360

Farquhar-Leicester, A. L., Tebbe, E., & Scheel, M. (2022). The intersection of transgender and gender-diverse identity and neurodiversity among college students: An exploration of minority stress. *Psychology of Sexual Orientation and Gender Diversity*. https://doi.org/10.1037/sgd0000603

Gadiraju, U., Kawase, R., & Dietze, S. (2015). Understanding malicious behavior in crowdsourcing platforms: The case of online surveys. In *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 1631–1640). https://doi.org/10.1145/2702123.2702443

Garcia-Iglesias, J., Heaphy, B., Yodovich, N., Atherton, S., & Merchant, A. (2025). Imposter participants? Towards a reflective epistemology of 'suspected participants'. *International Journal of Qualitative Methods*, 1–9. https://doi.org/10.1177/16094069251335497

Garrett-Walker, J. J., & Montagno, M. J. (2023). Queering labels: Expanding identity categories in LGBTQ+ research and clinical practice. *Journal of LGBT Youth*, *20*(4), 865–881. https://doi.org/10.1080/19361653.2021.1896411

Geeng, C., Harris, M., Remiles, E., & Roesner, F. (2022). "Like lesbians walking the permieter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice. *Proceedings of the 31st USENIX Security Symposium*. https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

Goetz, T. G., & Adams, N. (2024). The transgender and gender diverse and attention deficit hyperactivity disorder nexus: A systematic review. *Journal of Gay and Lesbian Mental Health*, *28*(1), 2–19. https://doi.org/10.1080/19359705.2022.2109119

Goodrich, B., Fenton, M., Penn, J., Bovay, J., & Mountain, T. (2023). Battling bots: Experiences and strategies to mitigate fraudulent responses in online surveys. *Applied Economic Perspectives and Policy*, *45*(2), 762–784. https://doi.org/10.1002/aepp.13353

Green, H., Fernandez, R., & MacPhail, C. (2021). Social media as a platform for recruitment to a national survey during the COVID-19 pandemic: Feasibility and cost analysis. *JMIR Formative Research*, *5*(7), e28656. https://doi.org/10.2196/28656

Griffin, M., Martino, R. J., LoSchiavo, C., Comer-Carruthers, C., Krause, K. D., Stults, C. B., & Halkitis, P. N. (2022). Ensuring survey research data integrity in the era of internet bots. *Quality and Quantity*, *56*(4), 2841–2852. https://doi.org/10.1007/s11135-021-01252-1

Hardesty, J. J., Crespi, E., Sinamo, J. K., Nian, Q., Breland, A., Eissenberg, T., Kennedy, R. D., & Cohen, J. E. (2024). From doubt to confidence-overcoming fraudulent submissions by bots and other takes of a web-based survey. *Journal of Medical Internet Research*, *26*, e60184. https://doi.org/10.2196/60184

Hitches, E., Dudley, D., Johnstone, M., & Woodcock, S. (2024). Bots and baddies: Supporting the integrity of online survey research in the face of a growing challenge. *Quality and Quantity*. https://doi.org/10.1007/s11135-024-02001-w

Irish, K., & Saba, J. (2023). Bots are the new fraud: A post-hoc exploration of statistical methods to identify bot-generated responses in a corrupt data set. *Personality & Individual Differences*, *213*, 112289. https://doi.org/10.1016/j.paid.2023.112289

Jean Louis, R., & Thompson, L. M. (2025). Bots and fake participants: Ensuring valid and reliable data collection using online participant recruitment methods. *International Journal of Social Research Methodology*, *28*(4), 463–473. https://doi.org/10.1080/13645579.2024.2410176

Kennedy, C., Hatley, N., Lau, A., Mercer, A., Keeter, S., Ferno, J., & Asare-Marfo, D. (2021). Strategies for detecting insincere respondents in online polling. *Public Opinion Quarterly*, *85*(4), 1050–1075. https://doi.org/10.1093/poq/nfab057

Kennedy, R., Clifford, S., Burleigh, T., Waggoner, P. D., Jewell, R., & Winter, N. J. G. (2020). The shape of and solutions to the MTurk quality crisis. *Political Science Research and Methods*, *8*(4), 614–629. https://doi.org/10.1017/psrm.2020.6

King-Nyberg, B., Thomson, E. F., & Morris-Reade, J. (2023). The bot toolbox: An accidental case study on how to eliminate bots from your online survey. *Journal for Social Thought*, *7*(1). http://ir.lib.uwo.ca/jst/

Krosnick, J. A. (1991). Response strategies for coping with the cognitive demands of attitude measures in surveys. *Applied Cognitive Psychology*, *5*(3), 213–236. https://doi.org/10.1002/acp.2350050305

Lawlor, J., Thomas, C., Guhin, A. T., Kenyon, K., Lerner, M. D., Consortium, U. C. A. S., & Drahota, A. (2021). Suspicious and fraudulent online survey participation: Introducing the real framework. *Methodological Innovations*, *14*(3). https://doi.org/10.1177/20597991211050467

Macapagal, K., Coventry, R., Arbeit, M. R., Fisher, C. B., & Mustanski, B. (2017). "I won't out myself just to do a survey": Sexual and gender minority adolescents' perspectives on the risks and benefits of sex research. *Archives of Sexual Behavior*, *46*(5), 1393–1409. https://doi.org/10.1007/s10508-016-0784-5

Matos, L. A., Silva, S., Relf, M. V., & Gonzalez-Guarda, R. (2025). Addressing survey fraud in online health research: A case study of latine sexual minority men. *Research in Nursing and Health*, *48*(6), 750–762. https://doi.org/10.1002/nur.70021

McAra-Hunter, D. (2024). How AI hype impacts the LGBTQ+ community. *AI and Ethics*, *4*(3), 771–790. https://doi.org/10.1007/s43681-024-00423-8

McInroy, L. B. (2016). Pitfalls, potentials, and ethics of online survey research: LGBTQ and other marginalized and hard-to-access youths. *Social Work Research*, *40*(2), 83–94. https://doi.org/10.1093/swr/svw005

McKinnon, K. R., Khan, N., Newman, K. M., Gould, W. A., Marshall, G., Salway, T., Pullen Sansfaçon, A., Kia, H., & Lam, J. S. H. (2025). Introducing novel methods to identify fraudulent responses (sampling with Sisyphus): Web-based LGBTQ2S+ mixed-methods study. *Journal of Medical Internet Research*, *27*, e63252. https://doi.org/10.2196/63252

McQuaid, G. A., Gendy, J., Lee, N. R., & Wallace, G. L. (2023). Sexual minority identities in autistic adults: Diversity and associations with mental health symptoms and subjective quality of life. *Autism in Adulthood*, *5*(2), 139–153. https://doi.org/10.1089/aut.2021.0088

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological Methods*, *17*(3), 437–455. https://doi.org/10.1037/a0028085

Ménard, A. D., McMurphy, S., Sterling, M., Armstrong, N., Cheek, O., & Balint, S. (2025). Bots, scammer, and fraudulent responders: A year of disrupted data collection. *Ethics & Behavior*. https://doi.org/10.1080/10508422.2025.2518270

Mustanski, B. S., Garofalo, R., & Emerson, E. M. (2010). Mental health disorders, psychological distress, and suicidality in a diverse sample of lesbian, gay, bisexual, and transgender youths. *American Journal of Public Health*, *100*(12), 2426–2432. https://doi.org/10.2105/AJPH.2009.178319

Nur, A. A., Leibbrand, C., Curran, S. R., Votruba-Drzal, E., & Gibson-Davis, C. (2024). Managing and minimizing online survey questionnaire fraud: Lessons from the triple C project. *International Journal of Social Research Methodology*, *27*(5), 613–619. https://doi.org/10.1080/13645579.2023.2229651

Orantes, D., Hartung, C. M., Lefler, E. K., Abu-Ramadan, T. M., Stevens, A. E., Serrano, J. W., Banerjee, M., & Antshel, K. M. (2025). Self-reported lifetime ADHD diagnosis and sexual and gender minority identities in college students. *Journal of Gay and Lesbian Mental Health*. https://doi.org/10.1080/19359705.2024.2446183

Pao, C., Moran, K. D., Compton, D., Kaufman, G., & Dowling, J. A. (2025). The case for "other": Measuring gender and sexual identity in survey research. *Sociology Compass*, *19*(1), e70031. https://doi.org/10.1111/soc4.70031

Pinzón, N., Koundinya, V., Galt, R. E., Dowling, W. O., Baukloh, M., Taku-Forchu, N. C., Schohr, T., Roche, L. M., Ikendi, S., Cooper, M., Parker, L. E., & Pathak, T. B. (2024). AI-powered fraud and the erosion of online survey integrity: An analysis of 31 fraud detection strategies. *Frontiers in Research Metrics and Analytics*, *9*. https://doi.org/10.3389/frma.2024.1432774

Prince, K. R., Litovsky, A. R., & Friedman-Wheeler, D. G. (2012). Internet-mediated research: Beware of bots. *The Behavior Therapist*, *35*(5), 85–88. https://doi.org/10.1037/e643332012-001

Pullen Sansfaçon, A., Gravel, E., & Gelly, M. A. (2024). Dealing with scam in online qualitative research: Strategies and ethical considerations. *International Journal of Qualitative Methods*, *23*, 1–11. https://doi.org/10.1177/16094069231224610

Sarstedt, M., Adler, S. J., Rau, L., & Schmitt, B. (2024). Using large language models to generate silicon samples in consumer and marketing research: Challenges, opportunities, and guidelines. *Psychology and Marketing*, *41*(6), 1254–1270. https://doi.org/10.1002/mar.21982

Shaw, T. J., Cascalheira, C. J., Helminen, E. C., Brisbin, C. D., Jackson, S. D., Simone, M., Sullivan, T. P., Batchelder, A. W., & Scheer, J. R. (2025). Yes stormtrooper, these are the droids you are looking for: Identifying and preliminarily evaluating bot and fraud detection strategies in online psychological research. *Psychological Methods*. Advance online publication. *30*(6), 1294–1310. https://doi.org/10.1037/met0000724

Simone, M., Cascalheira, C. J., & Pierce, B. G. (2023). A quasi-experimental study examining the efficacy of multimodal bot screening tools and recommendations to preserve data integrity in online psychological research. *The American Psychologist*, *79*(7), 956–969. https://doi.org/10.1037/amp0001183

Smith, L., Burke, R. S., Kelsey, F., & Addington, L. (2025). Coopting the rainbow: Analyzing malicious survey responses. *Journal of Homosexuality*. Advance Online Article. https://doi.org/10.1080/00918369.2025.2540369

Sophus, A. I., & Mitchell, J. W. (2025). Assessment of fraud deterrence and detection procedures used in a web-based survey study with adult black cisgender women: Description of lessons learned and recommendations. *JMIR Formative Research*, *9*, e59955. https://doi.org/10.2196/59955

Sterzing, P. R., Gartner, R. E., & McGeough, B. L. (2018). Conducting anonymous, incentivized, online surveys with sexual and gender minority adolescents: Lessons learned from a national polyvictimization study. *Journal of Interpersonal Violence*, *33*(5), 740–761. https://doi.org/10.1177/0886260517744845

Storozuk, A., Ashley, M., Delage, V., & Maloney, E. A. (2020). Got bots? Practical recommendations to protect online survey data from bot attacks. *The Quantitative Methods for Psychology*, *16*(5), 472–481. https://doi.org/10.20982/tqmp.16.5.p472

Teitcher, J. E. F., Bockting, W. O., Bauermeister, J. A., Hoefer, C. J., Miner, M. H., & Klitzman, R. L. (2015). Detecting, preventing, and responding to "fraudsters" in internet research: Ethics and tradeoffs. *Journal of Law Medicine & Ethics*, *43*(1), 116–133. https://doi.org/10.1111/jlme.12200

Vo, T. D. (2022). A quantitative examination of intersectional discrimination, wellbeing, and resilience among diverse 2SLGBTQ+ people within 2SLGBTQ+ leisure spaces. *Journal of Policy Research in Tourism, Leisure and Events*. https://doi.org/10.1080/19407963.2022.2042817

Yarrish, C., Groshon, L., Mitchell, J. D., Appelbaum, A., Klock, S., Winternitz, T., & Friedman-Wheeler, D. G. (2019). Finding the signal in the noise: Minimizing responses from bots and inattentive humans in online research. *The Behavior Therapist*, *42*(7), 235–242.

Yim, O., & Ramdeen, K. T. (2015). Hierarchical cluster analysis: Comparison of three linkage measures and application to psychological data. *The Quantitative Methods for Psychology*, *11*(1), 8–21. https://doi.org/10.20982/tqmp.11.1.p008