Striking a Balance: Mitigating Fraud While Ensuring Equity in Online Qualitative Research Recruitment

Eunji Cho, Laura Foran Lewis, Elizabeth Broden

Submitted to: Journal of Medical Internet Research
on: November 04, 2024

Table of Contents

Striking a Balance: Mitigating Fraud While Ensuring Equity in Online Qualitative Research Recruitment

Eunji Cho[1] PhD; Laura Foran Lewis[2] PhD; Elizabeth Broden[3] PhD

[1]Connell School of Nursing Boston College Chestnut Hill US
[2]College of Nursing and Health Sciences University of Vermont Burlington US
[3]School of Medicine and School of Public Health Yale University New Haven US

Corresponding Author:
Eunji Cho PhD
Connell School of Nursing
Boston College
Maloney Hall 378B
140 Commonwealth Avenue
Chestnut Hill
US

Abstract

After the COVID-19 pandemic, online recruitment became a critical component of qualitative research in healthcare fields. However, fraudulent participants targeting research incentives have become more prevalent in health studies, raising significant issues for research ethics, data integrity, and the inclusion of diverse patient voices. While qualitative health research aims to listen to and amplify patients' and communities' voices, such fraud can severely impact research quality and foster mistrust toward participants. This issue is particularly critical in qualitative studies, where careful communication, engagement, and mutual trust between researchers and participants are hallmarks of the research process, especially when working with marginalized populations. Behaviors that researchers may associate with fraudulent participants also appear in the communication patterns of marginalized groups, especially when discussing sensitive topics. This similarity could lead to misplaced suspicion, unintentionally disadvantaging marginalized populations when they attempt to share their experiences. In this paper, three qualitative nursing researchers reflect on their experiences with recruitment and data collection in recent studies, including methods to address challenges with potentially fraudulent participants, existing strategies from prior studies facing similar issues, unaddressed areas requiring future attention, and ways to promote inclusivity for diverse and marginalized populations who may be disproportionately affected by mistrust in participant integrity.

(JMIR Preprints 04/11/2024:68393)
DOI: https://doi.org/10.2196/preprints.68393

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Viewpoint

Striking a Balance: Mitigating Fraud While Ensuring Equity in Online Qualitative Research Recruitment

Eunji Cho, PhD, RN[1]
Laura Foran Lewis, PhD, RN[2]
Elizabeth Broden, PhD, RN[3]
1 Boston College Connell School of Nursing, Chestnut Hill, Massachusetts 02467
2 The University of Vermont College of Nursing and Health Sciences, Burlington, Vermont 05405
3 National Clinician Scholars Program, School of Medicine, Yale University
4 School of Public Health, Yale University

*Corresponding Author:
Eunji Cho, PhD, RN
Assistant Professor
Maloney Hall 378B, Connell School of Nursing
Boston College
Chestnut Hill, Massachusetts 02467

*Declaration of Conflicting Interests: Authors report no conflict of interest.
*Funding: The original studies received funding support from (a) CTSA award No. UL1 TR002243 from the National Center for Advancing Translational Sciences (Eunji Cho) and (b) Health 5T32HS017589, as well as CTSA Grant Number TL1 TR001864 from the National Center for Advancing Translational Sciences (NCATS), a component of the National Institutes of Health (NIH) (Elizabeth Broden).

Abstract

After the COVID-19 pandemic, online recruitment became a critical component of qualitative research in healthcare fields. However, fraudulent participants targeting research incentives have become more prevalent in health studies, raising significant issues for research ethics, data integrity, and the inclusion of diverse patient voices. While qualitative health research aims to listen to and amplify patients' and communities' voices, such fraud can severely impact research quality and foster mistrust toward participants. This issue is particularly critical in qualitative studies, where careful communication, engagement, and mutual trust between researchers and participants are hallmarks of the research process, especially when working with marginalized populations. Behaviors that researchers may associate with fraudulent participants also appear in the communication patterns of marginalized groups, especially when discussing sensitive topics. This similarity could lead to misplaced suspicion, unintentionally disadvantaging marginalized populations when they attempt to share their experiences. In this paper, three qualitative nursing researchers reflect on their experiences with recruitment and data collection in recent studies, including methods to address challenges with potentially fraudulent participants, existing strategies from prior studies facing similar issues, unaddressed areas requiring future attention, and ways to promote inclusivity for diverse and marginalized populations who may be disproportionately affected by mistrust in participant integrity.

Keywords

Online recruitment, social media recruitment, qualitative research, fraudulent participants, data integrity, participant inclusivity

Introduction

Online recruitment has become an essential strategy in health care research involving human participants, especially for engaging diverse populations that are traditionally underrepresented in health research. Researchers frequently identify target populations using social media platforms (e.g., Facebook, Instagram, Reddit, Craigslist) and websites popular among specific groups,[1,2] as well as ResearchMatch, a national registry for clinical research volunteers.[3] These methods help overcome physical barriers like location and time, facilitating access to large pools of potential participants cost-effectively.[2] Online recruitment approaches are especially effective for recruiting hard-to-reach groups such as minoritized and rural populations, which are often underrepresented in health related studies.[4] The importance of these strategies was highlighted during the COVID-19 pandemic when traditional recruitment methods were limited.

Despite its benefits, online and social media recruitment poses significant risks, such as the potential for fraudulent activities that threaten research integrity [5]. For instance, Pozzar, Hammer, Underhill-Blazey, Wright, Tulsky, Hong, Gundersen and Berry [6] found 94.5% of their online survey responses completed within seven hours were fraudulent. Participants may use fake identities, complete surveys multiple times, or employ bots or server farms to maximize financial incentives.[7] To mitigate these risks, researchers suggest incorporating technologies like reCAPTCHA, filtering IP addresses, and adding qualitative components such as free-text responses and interviews.[8,9]

However, common strategies to mitigate fraud are primarily developed for quantitative research and are not entirely applicable to qualitative methods. The researcher's positionality becomes integral to the data collection, analysis, and interpretation in qualitative research, making threats to participant legitimacy particularly critical. For example, Jones, Caes, Rugg, Noel, Bateman and Jordan [10] reported challenges in ensuring data quality and integrity in asynchronous qualitative data collection, which might not be fully preventable despite various mitigation strategies. Similarly, Sefcik, Hathaway and DiMaria-Ghalili [11] encountered potential fraud in their qualitative descriptive study with caregivers, leading to the exclusion of this data from their analysis. These examples highlight the need for qualitative researchers to be vigilant about such issues. Emerging strategies to minimize fraudulent participation during social media recruitment are still limited and largely untested empirically, which restricts establishing efficacy and best practices. Most importantly, techniques to detect and manage fraudulent participants often risk disproportionately excluding already marginalized groups, including neurodivergent, racially/ethnically minoritized, socioeconomically diverse, or individuals with limited written or spoken proficiency with dominant languages.

While online recruitment methods can reach more diverse groups, they also introduce significant risks to research integrity and equity. Based on our experiences during the COVID-19 pandemic and a review of the literature, we propose specific strategies for each phase of the research process. We also identify issues that remain unaddressed and require further efforts from qualitative researchers. Finally, we call for a critical examination of how online recruitment procedures, which aim to promote research integrity, might inadvertently exacerbate inequity and bias.

Methods

We began by sharing and summarizing our three different recruitment experiences (Appendix 1), uncovering that we shared similar experiences. Then we searched the existing literature to identify and summarize similar recruitment challenges and strategies (Appendix 2). While we did not limit the time range of the search, we found that most studies were published during or after the COVID-19 pandemic, from 2021 to 2023. We intentionally excluded studies with a survey-only design, as strategies to mitigate fraudulent participation within this research design aim to prevent bot and hacking attacks, a characteristically different challenge. We summarized six qualitative or intervention trials that used online recruitment methods and described their recruitment challenges due to potentially fraudulent activities in detail.

Recommendations

Based on our experience (Appendix 1) and a literature review (Appendix 2), we suggest potential strategies for each phase of the qualitative research process to mitigate limitations in existing online recruitment and data collection safeguards (Table 1).

Table 1. Detecting and Moderating Fraudulent Responses at Different Phases of Qualitative Research

Detection Strategies	Moderation Strategies	Inclusivity Considerations
A. Designing/Planning		
1. Partnering with IRB and media office	Engage in discussions with the institution's IRB early on for support in preparing for and handling unexpected fraudulent activities. Consider sequencing information (eligibility criteria, incentive).	Include community partners on the research team when possible to ensure design is accessible and respectful. Facilitate open discussion with the team about needs for accessibility and whether/how those may affect data quality.
2. Planning to flag and manage suspicious participants	Predetermine responses and language usage for encounters with fraudulent activities and include predetermined consequences in the consent form (e.g., "You could be excluded from this study if you are identified as not eligible, and no compensation will be provided."). Craft protocols with clear but flexible language. Train research staff accordingly so they can properly respond to unexpected situations in a standardized manner. Compare the collected information of one participant with that of others. Multiple researchers have reported similar patterns among fraudulent participants, such as specific email address patterns, overly general names, similar voices, identical background noises, the same timing in submitting screening forms, or unusually short survey response times. Trust your instincts and discuss your observations with team members.	Plan to review potentially fraudulent findings with community partners when possible to better understand whether responses may represent expected norms within the population of interest (e.g. insider knowledge, language used, manner of speaking). Be mindful not to dismiss negative cases, or those representing different perspectives, solely because they differ from the main body of evidence. Consider responses in light of their holistic context (e.g. suspicious patterns identified in moderation strategies). Use language that maintains the dignity of participants, even if suspected to be fraudulent (e.g. "Thank you for your interest in this study. Based on your responses, unfortunately you are not eligible to continue in this study.").

3. Assigning funding and time for additional verification process	Allocate time and funds to develop and apply tools for verifying respondents, aiming to limit fraudulent participation from the outset. This consideration should occur during the design phase and when securing funding.	Allocate time and funds for community partners to be involved in verification processes when possible.
B. Recruiting/Enrolling Participants		
1. Identifying suspicious patterns	Be vigilant for unusual patterns identified during recruitment. For instance, a sudden spike in interest, as compared to the common trend, could be a potential red flag, necessitating further authentication of individuals.	Consider unusual patterns that may reflect unique characteristics of the population of interest (e.g. sudden spikes in interest may come after a recruitment post is shared by an influential person in the community; overly general names and/or email addresses may reflect a privacy fear and thus a lack of willingness to share one's real information). Familiarity with the population of interest can help differentiate fraudulent versus expected patterns.
2. Enhancing verification for accurate participant information	Utilize a two-step screening process, including in-depth questioning and a manual check over the phone/video. Perform a synchronous review of collected background information to detect inconsistencies early, confirm authenticity, and build rapport with genuine participants. Plan to verify participant information through additional documents, such as driver's licenses. Consider requesting a formal email (e.g., an email address connected to their work profile or email accounts created under a federal organization) or their social media account, if necessary. Collaborate with IT specialists to monitor IP addresses to ensure the geographical locations claimed by participants are accurate. Integrate open-ended and additional objective test questions into the screening survey to detect suspicious patterns and complement self-reported data. For example, researchers can include a question separate from data collection to test whether respondents possess common knowledge expected of the target population.	Recognize that participants may be reticent to participate in data verification processes for reasons unrelated to fraud, particularly those from targeted and/or minority groups. Discuss the rationale with participants, and if they are not willing or able to comply, prepare for this in your protocol (e.g. reasons that are acceptable versus reasons that would be cause for exclusion). Work with community partners to identify questions that would be appropriate for verification of the group. Consider executive functioning, technical savvy, social, and financial implications of requiring additional verification (e.g. access to stable housing, means to acquire driver's license, ease of accessing documents for participant, citizenship status, etc.).
3. Providing detailed written and spoken information during the consenting and	Clearly state in the consent form the criteria that could lead to exclusion from the study and explain the consequences.	Recognize that even legitimate participants may feel concerned about privacy. Offer information

further research process	During the consent process, inform participants about the expectations for participating in the study, including details about compensation (e.g., delivery timing, payment method, and activities required for compensation). Ensure transparent communication with potential participants during the recruitment process about study requirements and privacy protections. This approach aims to prevent genuine participants from altering their information out of fear of personal information exposure, which could potentially lead to unintentional fraud.	about protections of privacy before meeting potential participants when possible. Ensure materials are comprehensive and in accessible language and format (e.g. written and video format). Consider offering an informal meeting with researcher to discuss protections before collecting information.
4. Balancing verification and privacy protection	Balance the need for participant verification with privacy protection, requiring minimal but essential information and potentially conducting final verification calls. Researchers' strategies (e.g., allowing participants to remain off video camera, not requiring the provision of personal information) to protect participant privacy often led to drawbacks and become targets of fraud, but protecting their privacy remains important.	Consider alternative ways to support participant comfort that do not jeopardize participant verification. Examples may include: turning camera on for initial verification and then allowing camera off for the remainder of the interview may decrease social anxiety during interview; creating a pre-recorded video introduction of the researcher prior to interview; offering a diverse group of interviewers and inviting participants to select their preferred interviewer; etc.
5. Strategically reaching the intended audience	Consider recruiting participants from online or offline locations specifically tailored to reach the target population, using appropriate methods (e.g., snowballing by reliable personnel, online platforms accessible only to qualified individuals). If using social media for recruitment, consider employing targeted social media hashtags or advertisements designed to be primarily exposed to specific groups of people. Inform participants not to share any study information disclosed to them unless requested by the research team. If they wish to share the study information with potentially interested parties, they should first discuss it with the research team. Should the study information become public, there would be minimal ways for the researchers to control its exposure to unintended audiences.	Identify trusted community members who can support gaining entrée into the community, e.g. social media influencers, group moderators and admin. Consider ways to use the recruitment budget that can both target and potentially support the population of interest (e.g. collaborating with non-profit organizations for networking support in exchange for fees rather than spending funds on social media ads).
6. Ensuring security with up-to-date measures for digital platforms	Implement proper and up-to-date security measures on study websites or electronic survey system, if applicable.	Seek feedback from community members before deploying study websites or surveys to address any

		accessibility issues that may arise from security measures.
7. Developing secure incentive delivery procedures	Carefully consider the method of incentive delivery, opting for physical gift cards sent to verified addresses and excluding financial compensation details from advertisements to deter fraud. Indicate this information in the consent form and inform participants during the consenting process.	Consider populations that may be affected by the requirement of a physical address (e.g. those who are unhoused, those for whom "home" is not a safe location to disclose information about the study). Include flexibility in the compensation plan in case these situations arise.
8. Tracking recruitment process	As part of background information collection, ask where participants heard about the study. This tracking can help identify potentially suspicious applicants and understand what is happening. It could be helpful to know when and where the recruitment process has been contaminated and to determine further procedures for their data, if already collected, and plan to complete the study by creating additional screening procedures or changing the recruitment strategy.	Assess the costs and benefits of recruitment strategies when they yield both fraudulent and legitimate data. For example, a website that attracts diverse legitimate participants may still hold value even if it attracts some fraudulent participants. This must be individualized to the needs of the study.
9. Enhancing team communication	Use a proper communication platform or strategy among all team members. Follow the standardized protocol and share potential fraudulent scenarios so that all members can detect potentially suspicious activities.	Include team members in decision-making about exclusion, particularly community partners who may have particular insights about the authenticity of participant responses.
C. Collecting Data		
1. Monitoring through technical tools	If the design includes any electronic surveys (e.g., demographic and background information questionnaires), use technical tools, including IP address tracking, to safeguard data integrity.	Recognize that some participants may opt to use a virtual private network (VPN) for their own privacy protections, which may obscure their IP address and/or geo-location. Request that users turn these off during the participant verification process.
2. Employing experienced interviewers	Employ experienced interviewers with expertise and specialized knowledge (e.g., in nursing and research) to detect suspicious patterns, crucial for early fraud detection. If possible, let one experienced interviewer primarily lead the interviews so that they can identify any suspicious patterns as early as possible. If not possible, prepare a clear team communication strategy.	When possible, include content experts and/or individuals with lived experience when making decisions about exclusion, as these individuals may be able to identify subtle and nuanced cues about authenticity (e.g. specific words or phrases used, insider knowledge).
3. Asking camera activation for identity verification	Mandate video enabling during virtual interviews. If participants are unable to use their camera, consider other methods to verify their identity.	Recognize that not all participants will be comfortable with camera activation. Offer ways for participants to familiarize with the interviewer prior to the interview, such as a pre-recorded video introduction or "About Me" page

		prior to the start of the interview. Consider requiring camera only for initial verification and then allowing participants to turn camera off as desired.
4. Protecting privacy with anonymized data linkage	If decided to separate personal information from research data to protect privacy, consider linking it to pseudo-identifiable data (e.g., code name) for verification purposes without compromising privacy.	If using pseudonyms, ensure that code names are culturally appropriate and/or ambiguous (e.g. consider gender, race, etc.) so that you do not compromise privacy but also respect the identity of the participant.
5. Enhancing team communication	Utilize an appropriate communication platform or strategy among all team members. For instance, a live dashboard can be useful for tracking progress in real-time and identifying any issues as early as possible.	Ensure any team communication platform is accessible within and outside the institution if working with community partners who need to access.
D. Managing/Analyzing Data		
1. Checking data quality through manual and/or automatic system	Utilize both manual reviews and automated systems effectively to detect unusual patterns or inconsistencies in the data (e.g., matching information reported in screening survey, demographic questionnaire, and interview narratives), thereby confirming its authenticity. Determine which check methods would be most beneficial in their specific context and situation, based on discussions with the team, collaborators, committees, other experts, and the institution's IRB. Consider involving all team members in manual data quality checks to some extent to identify suspicious patterns and ensure data quality.	Include community partners in manual checking for authenticity when possible, ideally including those with shared aspects of identity with participants who may have insight into the experiences being shared and thus the legitimacy of the account.
2. Enhancing team communication	Communication among all members is critical at this phase, using all information tracked throughout the process.	Consider optimal strategies for accessibility for team members, particularly when working with community partners. Plan for support and training if using an analytic tool that is unfamiliar to these team members.
3. Modifying analysis strategies	Develop an analysis procedure for any suspicious data identified. If it is difficult to determine whether the data is clearly fraudulent, consider conducting multiple data analyses with multiple datasets (e.g., dataset with all data and cleaned data after excluding suspicious data) and report all findings with clear descriptions.	When considering data that is suspicious but not clearly fraudulent, be careful not to discount negative cases simply because they reflect an experience that differs from other accounts. This is particularly important when suspicious data comes from participants who report an aspect of identity that represents a minority perspective within the sample. Be mindful of aspects of identity that may affect an experience.

E. Reporting Findings		
1. Reporting details	Share a clear and detailed summary of incidents, strategies, and outcomes related to potential fraud with the research community to aid future efforts.	Include input from those with lived experience if possible when developing this summary to capture strategies that are important to the population of interest even if they increase the likelihood of data compromise.
2. Enhancing academic awareness	Inform academic communities and researchers about challenges encountered and solutions implemented to promote integrity in research.	Partner with organizations and/or individuals who share aspects of identity with the intended sample to better inform academic approaches for the future.

In this table, we highlight that early preparation for research procedures, in collaboration with the institution's ethical review board, funding agency, and community partners is critical (Table 1-A). Researchers should allocate sufficient time, staff, and funding to address any potential issues during the recruitment process, enabling them to manage any unexpected events effectively.[5] Screening procedures should be carefully designed and prepared with clear protocols to identify and address any suspicious patterns (Table 1-B). Written documents that inform participants about their eligibility and responsibilities for receiving participation incentives should be delivered during the consenting process.

Researchers should fully understand their chosen recruitment methods and platforms that they decided to use including up-to-date online security measures to prevent any bot or cyberattack that can contaminate their participant pool. For example, one study reported how snowballing recruitment from one volunteer referral led to multiple fraudulent activities because the person who initiated the referral was also a fake participant.[11] Glazer, MacDonnell, Frederick, Ingersoll and Ritterband [5] conducted a post-hoc analysis of recruitment methods that led to a higher incidence of fraudulent cases, which were identified as social media platforms like Craigslist. These findings are noteworthy for future researchers. Researchers might consider using technical tools, software, or computer cameras to further screen participants' authenticity and eligibility, [1,5,11] while also preparing strategies to protect participants' privacy and respect their dignity, even if they are suspected of fraud (Table 1-B-4). For example, when considering the collection of IP addresses from participants, it may be necessary to notify potential participants that their approximate geographical locations will be collected through their IP addresses. As financial incentives make research a target of research scam, researchers may need to prepare clear statement on the eligibility to receive financial incentives, rigorous incentive delivery methods, and clear protocols [5] as summarized in the Table 1-B-7.

Throughout all research processes, clear and coordinated team communication is essential.[7] Research teams should constantly monitor all research activities and investigate when any suspicious patterns arise and discuss such questions with team members and community partners. If any damage is identified, researchers can employ strategies to address the damage and consider many creative ways to report their findings. For example, Willis, Wright-Hughes, Skinner, Farrin, Hartley, Walwyn, Weller, Althaf, Wilson, Gale and Foy [7] identified the potential contamination point, created multiple datasets (with and without potentially fraudulent data), and reported all results, including comparisons between datasets. Most importantly, all procedures, events, and strategies should be thoroughly tracked and transparently reported to inform other researchers and prevent future fraud.[12] Finally, procedures should be conducted, discussed, and

collaborated on with the institutions' research support teams, funding agencies, and other community partners to protect and inform research teams, enhancing organizational plans and protocols to prevent damages to other researchers in the future. Table 1 summarizes more details and strategies to deal with potential challenges in each step.

Unaddressed Issues

While we offer potential strategies to prevent and address fraudulent research participation, several issues remain unaddressed that future studies should consider, particularly to protect scientific integrity and ensure the dignity, privacy, and inclusivity of participants.

Issue 1. How do we preserve the critical role of trust in the qualitative research process amidst concerns about participant integrity, without biasing our results? A recurring issue we have encountered is the challenge of fully trusting the authenticity of participants. This skepticism is based on experiences and a review of similar studies, which reveal a pattern of potentially fraudulent behavior. Participants involved in such behavior often display certain characteristics: specific racial or ethnic backgrounds, poor English grammar proficiency, substandard video quality due to inadequate camera or internet connections, unclear audio, and peculiar email formats.[1,12] Additionally, in some cases, the demographics of fraudulent participants significantly differ from those typically recruited for similar studies, or they show a lack of knowledge in expected topics.[1] This observation raises concerns about unintentional biases that could affect how researchers recruit and interact with participants, undermining the mutual trust, curiosity, and respect essential to qualitative research. Some researchers have suggested restricting incentives to residents of the study's host country to mitigate such biases and ensure a diverse participant pool. However, this approach could unintentionally exclude legitimate participants from diverse backgrounds, potentially introducing a different kind of bias.

This argument leads to a critical question: how to distinguish between genuine patterns of fraud and unintentional bias towards certain groups. This challenge is compounded by the concern that our suspicions might be tainted by subjective biases, rather than being purely objective. Such skepticism, while possibly justified, can cause discomfort and raise ethical concerns, especially for researchers committed to conducting their work ethically and respectfully, upholding human dignity. In light of the characteristics shared by research scam groups, as noted in the literature and our experiences,[1,12] we must be cautious. The realization of potential unintentional biases necessitates in-depth self-reflection and a reevaluation of recruitment practices. How do we determine if a pattern is suspicious, or if it reflects our own biases? The refusal of some participants to turn on their cameras or disclose certain information may be an attempt to conceal a fake identity, but it could also be a legitimate privacy concern from genuine participants discussing sensitive topics. This issue highlights the importance of developing ethical online recruitment practices that promote inclusivity and diversity, without compromising the quality and trustworthiness of research. Future studies should continue to navigate the delicate balance between preserving research integrity and respecting the dignity of all participants, including those whose authenticity may be in question.

Issue 2. How can we boost recruitment rates while ensuring research integrity, enhancing screening processes, and safeguarding participant privacy? As experienced by all authors in our review and documented by Roehl and Harland [12] and Davies, Monssen, Sharpe, Allen, Simms, Goldsmith, Byford, Lawrence and Schmidt [13], researchers often face a dilemma: efforts to protect participants' privacy and reduce their burden

— such as permitting disabling video cameras during interviews—can unfortunately expose the study to fake participants. Implementing additional verification methods, as described in Table 1 and Appendix 2, such as checking participants' identification documents (e.g., driver's licenses) or verifying information through official channels (e.g., email addresses, professional social media accounts), and requiring them to disclose more personal information (e.g., turning on the camera during interviews), might deter potential participants, thereby reducing recruitment and retention rates. If the project is managed by a small team, these additional tasks could also hinder research progress and place greater demands on the team. Faced with this situation, qualitative researchers may need to decide whether to prioritize enhancing participant recruitment or to adopt more stringent screening measures to safeguard data integrity. Depending on their choice, the benefits of online recruitment, which include better accessibility for marginalized and hard-to-reach populations, might be compromised. Although some literature highlights the importance of clear communication, standardized protocols, staff training, and careful selection of personal information to be collected to manage this issue, more concrete guidelines are needed to help researchers navigate the persistent challenges of recruiting appropriately diverse participants in human subject research.

Issue 3. What specific and individualized prevention strategies are appropriate for different types of studies and teams? One of the authors, EC, notes that her dual role as the principal investigator and main interviewer enabled her to detect suspicious activities by comparing cases based on her experience, expertise in the target population, and instincts. Sefcik, Hathaway and DiMaria-Ghalili [11] support this observation, suggesting that having one experienced interviewer can be effective in identifying potentially fraudulent behavior. However, this approach may not be suitable for all teams, depending on the scope of the research or team size. While some studies advocate for a structured team communication protocol to keep all members informed of every research activity, more comprehensive guidelines for conducting and reporting studies that utilize online recruitment would help improve rigor. This is particularly vital for early career investigators who are developing skills to build and manage research teams, helping them to safeguard their studies.

Issue 4. How do we deal with advancing technology and evolving attempts to misuse benefits from human subject studies? Despite ongoing efforts, new technologies and sophisticated strategies to exploit human subject research will likely continue. Numerous incidents have demonstrated that identifying and addressing such issues may demand prolonged and collective efforts. Researchers must remain vigilant to maintain the integrity of their research. It is essential to establish a group of well-prepared experts, implement thoughtful guidelines and policies, and ensure that community and academic institutions are aware and can actively participate in the prevention and recovery from fraudulent activities. Continuous efforts are necessary to inform qualitative researchers about potential technical tools they can implement in their projects, but such strategies should be standardized, verified, and broadly disseminated.

Issue 5. How should researchers identify and report suspicious participants before, during, and after a qualitative data collection episode? While there is no universal guideline for addressing fraudulent participation in research, some studies explicate potential strategies. These include relying on intuition based on experience, ending interviews when suspicion arises, implementing additional screening methods to verify participant reliability, and, in some cases, excluding or adapting data analysis to maintain integrity.[1,5,7,11,13] All studies we reviewed transparently reported their approaches for the benefit of future researchers. However, no standard protocol or reporting structure exists, especially for ambiguous situations during sensitive, in-depth interviews. Qualitative interviewers may hesitate to express doubts when engaging closely with participants, particularly on sensitive topics or with marginalized populations. Clearer guidelines are needed, including professional and IRB-approved language, protocols for addressing suspicious participants in the midst of data collection, data management strategies, and reporting metrics. Future research should focus on developing such protocols to enhance data integrity and protect the participation of legitimate respondents.

Moreover, it is important to acknowledge that no single strategy can completely prevent threats. Each strategy, even those detailed in Table 1, can still be susceptible to fraudulent activities. Despite applying precautionary strategies after the initial incident, Willis, Wright-Hughes, Skinner, Farrin, Hartley, Walwyn, Weller, Althaf, Wilson, Gale and Foy [7] still encountered fraudulent participants in subsequent recruitment rounds. While snowballing recruitment from reliable personnel has been recommended, Sefcik, Hathaway and DiMaria-Ghalili [11] reported issues originating from such sampling methods. Although many researchers endorse a two-step screening process to verify participants' authenticity,[5,9] we found it cannot completely prevent fraudulent activities. Individuals can still manipulate this process by tailoring their responses to meet eligibility criteria, exploiting the detailed information provided in screening questionnaires. Moreover, research scam groups can discover and employ new methods that we might not yet recognize to create multiple online identities. Consequently, all suggested strategies should be collectively considered for implementation in research projects, and researchers must be prepared to handle unforeseen threats effectively.

Future Implications

As there are numerous unanswered questions essential for future qualitative studies that consider online recruitment, we recommend specific actions and urge researchers to collectively address these issues. Firstly, informing research support groups such as institutional IRBs, academic institutions, administrators, professional organizations, and funding agencies can enhance community awareness and foster a collective effort to mitigate future damage. Secondly, there should be a concerted effort in partnership with communities to develop standardized protocols, guidelines, and tools to address this issue, with regular updates to keep pace with rapid technological developments and evolving schemes that exploit research intended to benefit

human health and well-being. Furthermore, other institutions involved in research, such as academic journals and publication authorities, should recognize this issue and prepare tools like standardized checklists, which can serve as research guidelines and promote transparent reporting by researchers as they disseminate their findings. We strongly advocate for a culture that accepts mistakes, failures, and unexpected outcomes related to these issues, as this could encourage researchers to comfortably report unsuccessful aspects of their work and provide guidance to others. Educators who teach research should also include information on rigorous research conduct and discuss strategies with their students to prevent such problems. Finally, there is an urgent need to build a community for collective action to tackle current problems and establish a sustainable task force that can continuously address evolving research scams targeting researchers.

Conclusion

Online recruitment has proven to be an effective tool for engaging diverse population groups that are traditionally difficult to access through conventional, in-person strategies. This method allows participants to share their stories from the safety and convenience of their own environments, facilitating the inclusion of hard-to-reach and vulnerable populations in research. Despite these advantages, our exploration of the potential risks associated with online recruitment for qualitative studies—drawn from our experiences and those of other researchers—highlights significant challenges.

Throughout the research and preparation informing this paper, we recognized recurring patterns of fraudulent activity in our and others' studies, particularly during or after the COVID-19 pandemic. This realization prompted a deeper examination of the literature, and a reevaluation of past strategies aimed at preventing such issues. While techniques like enhancing the clarity of research advertisements and informed consent forms and applying technical strategies to vet participants have been implemented, they have often been reactive rather than proactive, leading to varied levels of damage to our studies.

As qualitative researchers, our experiences underscore the need for ongoing vigilance and innovative approaches to safeguard research integrity. Encountering fraudulent participants in qualitative research can be distressing for researchers, undermining trust and posing risks to data integrity. Such incidents prompt feelings of betrayal and self-doubt, particularly in research environments where a deep human connection is essential. The persistent and evolving nature of these challenges calls for collective efforts within the research community to develop more effective strategies to manage and mitigate risks in online recruitment while maintaining and promoting equitable and inclusive practices.

References

1. Mizerek E, Wolf L, Moon MD. Identifying and mitigating fraud when using social media for research recruitment. *J Emerg Nurs*. 2023;49(4):530-533. doi:10.1016/j.jen.2023.04.002
2. Arigo D, Pagoto S, Carter-Harris L, Lillie SE, Nebeker C. Using social media for health research: Methodological and ethical considerations for recruitment and intervention delivery. *Digit Health*. 2018;4:2055207618771757. doi:10.1177/2055207618771757
3. Harris PA, Scott KW, Lebo L, Hassan N, Lightner C, Pulley J. ResearchMatch: A national registry to recruit volunteers for clinical research. *Acad Med*. 2012;87(1):66-73. doi:10.1097/ACM.0b013e31823ab7d2
4. Benedict C, Hahn AL, Diefenbach MA, Ford JS. Recruitment via social media: advantages and potential biases. *Digit Health*. 2019;5:2055207619867223. doi:10.1177/2055207619867223
5. Glazer JV, MacDonnell K, Frederick C, Ingersoll K, Ritterband LM. Liar! Liar! Identifying eligibility fraud by applicants in digital health research. *Internet Interv*. 2021;25:100401. doi:10.1016/j.invent.2021.100401
6. Pozzar R, Hammer MJ, Underhill-Blazey M, et al. 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(10):e23021. doi:10.2196/23021
7. Willis TA, Wright-Hughes A, Skinner C, et al. The detection and management of attempted fraud during an online randomised trial. *Trials*. 2023;24(1):494. doi:10.1186/s13063-023-07517-4
8. Teitcher JE, Bockting WO, Bauermeister JA, Hoefer CJ, Miner MH, Klitzman RL. Detecting, preventing, and responding to "fraudsters" in internet research: Ethics and tradeoffs. *J Law Med Ethics*. 2015;43(1):116-33. doi:10.1111/jlme.12200
9. Wang J, Calderon G, Hager ER, et al. Identifying and preventing fraudulent responses in online public health surveys: Lessons learned during the COVID-19 pandemic. *PLOS Glob Public Health*. 2023;3(8):e0001452. doi:10.1371/journal.pgph.0001452
10. Jones A, Caes L, Rugg T, Noel M, Bateman S, Jordan A. Challenging issues of integrity and identity of participants in non-synchronous online qualitative methods. *Methods in Psychology*. 2021;5:100072. doi:10.1016/j.metip.2021.100072
11. Sefcik JS, Hathaway Z, DiMaria-Ghalili RA. When snowball sampling leads to an avalanche of fraudulent participants in qualitative research. *Int J Older People Nurs*. 2023;18(6):e12572. doi:10.1111/opn.12572
12. Roehl J, Harland D. Imposter participants: Overcoming methodological challenges related to balancing participant privacy with data quality when using online recruitment and data collection. *The Qualitative Report*. 2022;27(11):2446-2459. doi:10.46743/2160-3715/2022.5475
13. Davies MR, Monssen D, Sharpe H, et al. Management of fraudulent participants in online research: Practical recommendations from a randomized controlled feasibility trial. *Int J Eat Disord*. 2024;57(6):1311-1321. doi:10.1002/eat.24085

Supplementary Files

Multimedia Appendixes

Reflections on Experiences.
URL: http://asset.jmir.pub/assets/e1fdd2f885f47560a33bf2b53a70500d.docx

Literature Review.
URL: http://asset.jmir.pub/assets/c30674bb373455fec17e35273981f95c.docx