

The Right to Be Skeptical: Insights from Recruiting At-Risk Users on Nextdoor

Sam Addison Ankenbauer
School of Information
University of Michigan
Ann Arbor, Michigan, USA
samank@umich.edu

Robin N. Brewer
School of Information
University of Michigan
Ann Arbor, Michigan, USA
rnbrew@umich.edu

Abstract

This case study explores the challenges of recruiting a particular at-risk population, older adults affected by scams, focusing on the complexities of recruitment and trust in online environments. Specifically, we analyze a contentious recruitment attempt on Nextdoor, a hyper-local social platform aimed at fostering community engagement within neighborhoods. While responses varied, a vocal subset of users raised concerns about the legitimacy of the study, the researcher's identity, and the recruitment methods employed. Through an analysis of user responses, this case study examines the individual, community, and researcher-led negotiations of trust and distrust in this recruitment process. We emphasize the validity of doubt, the importance of user engagement, the features of recruitment that were found (un)trustworthy, and the role of context in recruitment. These findings provide insights into the under-researched area of recruitment, specifically concerning effective strategies for engaging at-risk users in online research while navigating distrust.

CCS Concepts

• **Social and professional topics** → *Seniors*; Computer crime; • **Human-centered computing** → **User studies**.

Keywords

case study, online recruitment, older adults, scams, doubt, distrust, trust

ACM Reference Format:

Sam Addison Ankenbauer and Robin N. Brewer. 2025. The Right to Be Skeptical: Insights from Recruiting At-Risk Users on Nextdoor. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25)*, April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 11 pages. <https://doi.org/10.1145/3706599.3706694>

1 INTRODUCTION

Recruitment for research presents unique challenges, particularly when working with at-risk populations¹ [6, 27]. This case study investigates the complexities of recruiting older adults who have

¹By "at-risk," we are informed by Bellini et al. who define individuals "at-risk" if they "face an elevated likelihood of an attack to their digital safety, have factors that

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

CHI EA '25, Yokohama, Japan

© 2025 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-1395-8/25/04

<https://doi.org/10.1145/3706599.3706694>

recently endured a scam—an increasingly relevant topic in today's online landscape. Given the sensitive nature of this topic, our recruitment process needed to navigate a number of social and technological barriers to build trust. Nextdoor, selected as a key platform for recruitment, presents a complex environment for engaging potential participants. The platform is designed to strengthen hyper-local community engagement online. However, the platform also mirrors some of the vigilance of offline local community engagement [9], which, when combined with the sensitive subject matter of our study, complicated recruitment efforts. We unpack the responses to our recruitment posts, ranging from curious to doubtful and distrusting.

As we navigated these various responses, we recognized that distrust itself is both reasonable and informative as it reflects concerns not only about the research and researcher but also broader concerns felt on and about the given platform and the wider context of online (dis)trust². This case study, then, presents an analysis of how distrust shaped recruitment on Nextdoor and how (dis)trust was negotiated throughout the recruitment process both individually and collectively, offering insights for future research involving at-risk or otherwise skeptical populations. In particular, we consider four factors that informed the processes of navigating trust and distrust: the greater platform context, institutional legitimacy, collective interrogation, and the moderation of commentary.

2 RECRUITING OLDER ADULTS AFFECTED BY SCAMS

In this study, we sought to recruit: older adults aged 65 and over, residing in Michigan, who experienced a scam within the previous month. Our recruitment strategy was multi-faceted, incorporating both in-person and online approaches in five neighboring communities to reach a more demographically diverse population of participants. For in-person recruitment, we distributed physical flyers at highly visible community locations such as public libraries, local restaurants, and senior centers across five neighboring communities, ensuring we engaged with spaces frequented by older adults. This approach was designed to foster trust and facilitate engagement by leveraging locations familiar to our target population.

influence or exacerbate their chances of being targeted, and/or experience heightened harm as a result of a digitally-mediated attack" [6, p.2]

²Throughout this work, we use "distrust" rather than "mistrust." While the two are similar, "mistrust" typically suggests a general sense of uncertainty, whereas "distrust" conveys a reasoned doubt rooted in observation or personal experience. This distinction parallels the difference between misinformation and disinformation whereby the prefix "mis-" implies without intention and "dis-" implies with intention [25]. In the context of at-risk users, we use "distrust" to indicate that individuals within our intended recruiting population are intentionally responding with a lack of trust due to personal observations and experiences

Our online recruitment strategy leveraged a range of digital platforms and community networks. We collaborated with community organizations to disseminate the study through online newsletters and senior center websites. Additionally, we partnered with the participant resource pools at the Healthier Black Elders Center and Michigan Medicine. Finally, we utilized Nextdoor, a neighborhood-based social networking platform, to connect with potential participants on a hyper-local level, tapping into community-based digital interactions.

Platform. Nextdoor is a U.S.-based social networking platform that connects users who are spatially situated within local neighborhoods and is therefore designed to strengthen both digital and physical communities, keep users informed about local events and activities, and encourage real-world connections within one's given neighborhood [21]. When a user signs up for Nextdoor, they are required to verify their address to join a specific neighborhood in an attempt to ensure that only people living in an area can interact and guide local discussions. Within Nextdoor, users can engage with neighbors through a variety of features, including posting on a public neighborhood news feed, exchanging private messages via a chat function, inviting others to join the platform through an invitation tool, and buying or selling personal items through a dedicated marketplace³. Nextdoor also integrates with public agencies, enabling local government and law enforcement to share updates directly with local residents. The goal of Nextdoor is to, as per Nextdoor Holdings CEO Sarah Frier, "cultivate a kinder world where everyone has a neighborhood to rely on" [13].

Beyond this, Nextdoor has a strong older adult user base. Out of the applications YouTube, Facebook, Instagram, Pinterest, LinkedIn, Snapchat, Twitter, WhatsApp, TikTok, Reddit, and Nextdoor, Nextdoor is the only application to have a higher percentage of 65+ users to 18-29 users [4]. As early as 2012, four years after its creation, Nextdoor was highlighting its value to older users: "At Nextdoor, seniors happen to be some of our most active members. We often get feedback from the senior community that they love our website for its real-world, practical value" [20]. Because of this older adult presence, Nextdoor played a role in community engagement and recruiting in our previous study [2]. Initially, we selected Nextdoor because its focus on digital interactions with hyper-local community presence makes it a natural ally for local research recruitment.

Recruiting Materials. The first author's initial post on the NextDoor platform was a 166-word, three-paragraph introduction to the study, alongside a flyer. The three paragraphs were as follows,

Hello! My name is Sam, I'm a Ph.D. candidate at the University of Michigan. I am currently beginning work on a project regarding older adults' experiences with fraud and scams.

Experiences with potential scams seem to be increasing, and while older adults do not fall for scams more than any other demographic group, scams themselves can specifically target older adults. My research wishes to uncover what older adults do after falling victim to such frauds or scams and what resources older adults utilize in response. This research will help inform

how we collectively understand the personal and social impacts of scams, as well as how systems may be designed to better remedy situations after one has occurred.

I am looking for older adults (65+) who have recently experienced fraud or scams (online, over the phone, or in person)—if you or anyone you know is 65+ and has recently fallen victim to a scam, please take my survey! I would really appreciate your time and effort.

In the first paragraph, the first author introduces himself by sharing his first name and profession, situating his identity within a recognizable academic institution. While the first author only discloses his first name in the text, it is important to note that, in accordance with the conventions of the NextDoor platform, his full name—both first and last—is visible through his username. The first author unpacks the thrust of the research, making sure to highlight that his research was designed to support older adults—although, in the second paragraph, the first author uses accusatory language, linguistically placing responsibility and, thereby, blame and potential guilt on individuals ("fall for" and "falling victim"). In subsequent outreach, he modified this (using the terms "experienced" and "endured" instead).

Additionally, the first author does not mention monetary compensation. In not mentioning monetary compensation, the first author attempts to weed out potential scammers who might pose as older adults specifically for compensation [22]. However, this approach contrasts with, for instance, Dillman's total design method, which emphasizes enhancing the perceived benefits of participation while minimizing its costs, advocating for the upfront acknowledgment of tangible rewards [17]. The implications of excluding such information, therefore, remain open to interpretation.

The above message was accompanied by a flyer that had been designed for physical distribution. As a platform, NextDoor frequently pairs text with images, such as when a neighbor posts a photo of their yard sale to visually reinforce the abundance of items for sale. In line with the platform's norms, the first author anticipated that a brightly colored flyer with bold fonts would catch attention and be more engaging than his staid text alone. This flyer mirrors all the essential information presented in the first author's Nextdoor post, including the study's objectives and participant recruitment criteria⁴. This ensures that a Nextdoor user can fully understand the purpose of the study simply by reading the flyer. However, the flyer offers additional engagement opportunities that go beyond the Nextdoor post by providing direct access to the survey through three methods: a QR code, a URL link, and a phone number.

Each engagement method was chosen to accommodate different preferences and levels of technological comfort. The QR code and URL both direct participants to a survey hosted on Qualtrics, an experience management platform commonly used for research purposes [23]. The QR code, in particular, is an effective option for the flyer's intended use as a physical artifact, allowing participants to quickly scan and access the survey with a mobile device, enhancing convenience in physical settings like community centers and libraries. The URL, which was shortened using TinyURL, offers a

³Please see Appendix for a screenshot of the user interface

⁴See the flyer in Appendix

more manageable alternative to the often lengthy web links associated with surveys, making it easier to share or manually enter into a browser. Upon engaging with either the QR code or URL, participants are directed to the Qualtrics landing page, which doubles as the study's consent form. This page explains the nature of the study, including eligibility criteria and the compensation offered, ensuring transparency, informed consent, and eventual compensation before the participant proceeds with the survey. For those who prefer or require more traditional communication methods, the flyer also lists a phone number generated through Google Voice. This Voice over Internet Protocol (VoIP) service creates a local area code, ensuring that potential participants feel they are contacting a familiar, nearby number. The first author used a Google Voice number to maintain privacy, separating personal from research-related calls and voicemails, and as a safeguard against potential scammers.

Finally, the flyer provides his academic email address and a logo for his department. According to previous research, a researcher should highlight one's institution to promote feelings of recognition and trust [17]. This has been expanded on by researchers discussing recruitment on sensitive topics (i.e. [6]). Guillemín et al. interrogate the significance of the institution in research/participant trust-building: while researchers tend to think of trust as interpersonal between researcher and participant, participants tend to think of trust as informed by the institution: "The relationship that participants had with researchers was based on researcher's associations with the university" [15, p.290]. As such, the first author wanted to highlight the University of Michigan's maze-colored block M and his institutional email address as markers of trust.

3 RESPONSES TO RECRUITMENT

In late March 2024, the flyer and accompanying text were posted on Nextdoor across two distinct neighborhoods, where they garnered significant attention with 13,700 views, 28 reactions, and 83 comments. The responses from users were mixed, reflecting both a recognition of the study's relevance and concerns about the legitimacy of the post. Some users expressed enthusiasm and support for the study, acknowledging the widespread nature of scams and the importance of collective efforts to address this issue. As one user remarked, "We are surrounded by a sea of scams. From all directions and from all levels. Bring on the survey." Several others echoed these sentiments, noting that the Nextdoor platform itself had increasingly become a space of scam activity: one user commented, "You've come to the right place," while another added, "Definitely the right place." One user elaborated, "What a great idea using this platform with all the posts I see related to fraud and scams. It seems to be more prevalent these days."

However, a significant portion of the comments revealed degrees of doubt. Many users voiced concerns about the authenticity of the post, as per one user: "I am interested but need a way to verify what you say." Other users went further, with multiple users echoing the concern, "This sounds like a scam to me!" One user responded to the initial post with a one-word response—"SCAM!" and took it upon themselves to create a separate Nextdoor post warning the community about the original research post:

SCAM Alert! A person is trying to lure elderly people into taking a survey regarding identity theft. He

claims it's for his PhD. It's a scam. Report it and block him. That survey will ask you for your birthday to prove your age is 65+, which is a consistent security question for banks, healthcare, etc... Don't fall for it!

This new post attracted 76 reactions and 40 comments, with many users thanking the poster for their vigilance and decrying the prevalence of online scams: "Thank you for alerting us. There are so many scams out there." Some users sent the first author direct messages to voice their complaints: "Sick! You are a scammer and I have reported you." These often affective reactions underscore broader anxieties about online security and the challenges of building trust on digital platforms. In particular, the sensitive nature of the study's focus—scams targeting older adults—amplified the community's caution, resulting in an atmosphere where recruitment efforts were perceived as potentially fraudulent.

To better understand what elements of the initial post were perceived as trustworthy or untrustworthy, and how these perceptions were collectively navigated both by users and with help from the first author, we analyze the comments in more detail below. This analysis is undertaken with three examples, focusing on distrust surrounding the mention of older adults, the QR code as a recruitment modality, and the validity of the institution and researcher. These three examples illustrate a progression of user engagement, reflecting increasing levels of effort and trust—from the outright dismissal of recruitment materials to expressing doubt about specific aspects of those materials and, ultimately, to conducting independent research and seeking collective validation to confirm the posts' legitimacy.

3.1 Distrust pertaining to overall study aims

With heightened sensitivity around scams and older adults, users expressed concerns about older adults as a targeted population for recruitment. As noted above, the user post mentioned that the "survey will ask you for your birthday to prove your age is 65+, which is a consistent security question for banks, healthcare, etc." While the survey did *not* request the exact birth date of potential participants, it did ask if respondents were 65 years old or older. For many Nextdoor users, even this general targeting of older adults seemed suspicious. Per one user, "How do we know this isn't just gathering information to better scam seniors?"

These reactions reflect a broader anxiety about protecting older adults, a group often perceived as more vulnerable to scams. The request for age-related data, even in a benign context, seemed suspicious to users already attuned to the ways scammers specifically target older adults [5]. This sensitivity was heightened by Nextdoor's existing reputation as a space where scams circulate and are discussed. In this context, any call for personal information—particularly age-related data—triggered suspicion. Users who were not older adults expressed a collective concern for the well-being of older adults on the platform, illustrating a heightened vigilance. That being said, other users contested the claims of the original poster. Per one user, who directly responded to the original poster's concerns:

Everyone's date of birth is easily accessible all day, every day, so your assertion is absolutely moot. (...) Please do the right thing and remove your post before

someone posts your address, birth date, etc. to prove you wrong. I wouldn't do it but it doesn't mean someone else wouldn't as many people are fed up with this type of aggression. We are old enough to know better.

This user's comment reflects a layered response to the issue of trustworthiness, privacy, and the perceived threat of public personal information. The user both dismisses concerns about the personal information they consider already accessible *while also* suggesting it can be misused and exploited by bad-faith actors—an acknowledgment and, in some ways, a reinforcement of the volatile nature of community interactions.

3.2 Distrust of QR codes

An aspect of the flyer that was considered untrustworthy was the QR code. Per one Nextdoor user, "DO NOT SCAN THAT QR CODE. QR codes can let scammers right into your phone. My son is a Cybersecurity grad and advises to avoid QR codes from restaurants and or unknown sources." Other users expressed suspicion about QR codes: "Why should anyone believe that you are a phd student and that QR code doesn't put a worm or virus that compromises the old persons phone? Be careful people." These reactions suggest that QR codes, while commonly used, remain a point of contention for many users and the inclusion of a QR code may have complicated efforts to establish trust.

In response, the first author engaged with both posts, guided by prior research emphasizing the critical role of researcher involvement in moderating discussions around online recruitment efforts [14, 26, 28]. For instance, in response to the first post, the first author said,

I appreciate your son's expertise! QR codes are just a modality that some people prefer (my flyer is also going to various libraries in the area, I think [QR codes are] better for physical locations). A tip for QR codes: they don't automatically open when you scan them. You can hover over them and your phone will show you where the link would take you. So, if you hover over mine, a yellow box will pop up that says "qualtrics.com" and if you look up "qualtrics," you'll find that it's a survey-building and experience management site—so it's just taking you to a survey! If you hover over a QR code for, say, Turbo Tax but the link says something other than "turbotax.intuit.com," it might be a scam.

Alongside the comment, the first author included a screenshot demonstrating that hovering over a QR code does not directly lead to the page but instead displays the URL, allowing users to see the destination before clicking. Despite this effort, the initial poster remained wary, responding with, "I'm not hovering over any stranger's QR code, and older folks should be warned as well." The poster's remark reflects a protective stance, not just for themselves but for their peers, underscoring the broader community's concerns about ensuring that older adults avoid potential online risks. It also reveals the limitations of technical explanations when trust has already been undermined—while the first author attempted to provide a clear demonstration of QR code safety, the social dynamics of distrust reasonably persisted.

3.3 Distrust of identity of researcher and institution

Finally, Nextdoor users began to investigate the first author's identity and institutional affiliation, reflecting varying levels of trust in both the researcher and the institution. Some users conveyed a sense of trust, likely influenced by the institution's proximity or their personal connections to it. For instance, one user expressed interest, stating, "I'd love to get in touch. I'm a UofM grad." On the other hand, several users voiced doubt, questioning the first author's identity and his proximity to the institution. One user articulated this critical stance:

I'm curious to learn what evidence [users] had to identify this as a scam, or [the first author] has to prove it isn't. Posting lots of words doesn't help, just like "not me" never worked for us when we were kids. Links claiming it is legit doesn't prove anything either. Edu accounts are especially suspicious as they are often stolen and used for scams. So, wise people, what do we do when there is no hard evidence it isn't as scam? Assume it is and don't respond/reply.

This comment underscores a distrust of ".edu" email accounts, which the user claims are susceptible to being appropriated by scammers—a claim echoed by other users: "[scammers] spoof and fake links to national banking institutes, I'm pretty sure it wouldn't be hard to trick someone to believe a school website, email." The rhetorical question ("What do we do when there is no hard evidence it isn't a scam?") and its answer ("Assume it is [a scam] and don't respond/reply") captures the defensive posture many users adopted in this online environment, where caution can supersede engagement.

Perhaps due to an abundance of caution, Nextdoor users did due diligence work, investigating the identity of the first author in an attempt to authenticate the legitimacy of the recruitment post and dispel growing doubts about its authenticity. Users commented with links to the first author's previous research, photos of him, and his personal page on his institution's website. As per one user,

This doesn't look to be a scam. Sam's UofM profile can be found in multiple areas and shows that their areas of interest are directly related to this survey. I am 100% behind being cautious of scams, and would be one of the first to tell you to verify and rarely if ever give out your personal information. But I am definitely against posting that someone or something is a scam without any supporting information. Do your own research and don't proceed unless you are comfortable. But unless you can provide information that can verify that this survey is a scam, you may want to stick with just reminding people to be wary and careful of scams and not state that you know and are certain this a scam and for people to block and report without any supporting information.

This post was accompanied by a picture of the first author and his university-listed research interests. This user's comment not only highlights the depth of their investigation but also attempts to

set a standard for responsible digital behavior. By encouraging others to conduct their own research and make informed decisions, the user shifts the conversation toward a more nuanced understanding of online trust. Rather than outright dismissal, they advocate for an evidence-based approach and community self-moderation, with members stepping in to clarify facts and encourage others. As time went on and some Nextdoor users transitioned from distrustful observers to study participants, a few returned to the thread to share their experiences. One participant reassured the community, posting, “I was interviewed. This IS NOT A SCAM. He is a legitimate PhD candidate at UM.” While this garnered mostly positive responses, others remained wary. One responded:

How do you know? Did you meet him in person? Did you get outside confirmation? I am inclined to believe you, but a good scammer can easily convince people that they are legitimate. I want to trust Sam, because what he is trying to do could be quite helpful, but he’s going to have to prove himself before we can all just ‘trust’ him.

This reply illustrates that even stated involvement with the research did not fully resolve doubt for each user. The user expressed a desire to trust but underscored the expectation for more concrete evidence, reinforcing the idea that online trust demands continued and required dynamic validation. In response, the participant elaborated on his experience, “We had multiple texts followed by emails followed by a one-hour interview. (...) All are so correct, scamming is pervasive both on the internet & mail. Better to be suspicious, vigilant & cautious. Best of luck to all.” Here, the participant acknowledged the importance of caution, echoing the broader sentiment within the community. By affirming the need for vigilance, even in the face of personal assurances, the participant demonstrated a balanced understanding—offering his endorsement of the study while respecting the community’s collective doubt. The challenge for researchers lies in navigating this complex landscape, where affiliation and testimonial alone may not be enough to inspire trust from already wary at-risk communities.

Some Nextdoor users, exercising individual caution, chose to request additional information before participating in the study. Post-recruitment discussions further revealed that these participants initially felt distrust, particularly during their early interactions with the first author. In one instance, a participant who had recently been scammed expressed distrust after the first author sent them a PDF file containing state-based scam resources intended to help them recover lost funds. In their email, the participant wrote:

I am definitely not going to open your attachment, I’m sure you understand. (...) I understand that this email is coming from a .edu address but since I don’t know you, I’m hesitant to trust you and will be very careful with any details I give you. If you need more details, we’ll have to find a way for you to earn my trust. I’m sure you also understand that.

This participant later elaborated on their reluctance during a phone conversation, recounting their initial response: “I felt so raw that I was like, Listen buddy, what are you sending me a PDF for?” This reflection illustrates the affective resonance of a scam and heightened sensitivity to seemingly benign communication. Other

participants echoed similar sentiments, reflecting on their initial distrust: “No offense to you. But I thought, ‘Is this a scam too?’ You know? ‘He hasn’t asked me for any personal information, so maybe I can relax.’” Another participant detailed their careful process of verifying the first author’s identity before feeling comfortable moving forward. They explained,

You had sent me a letter on letterhead. And I thought, well, but anybody can do that. I mean, you could make up your letterhead. (...) You had posted on that neighborhood website. And someone went in there and wrote, “This is a scam, don’t do this.” I’m lucky that I have my son and my husband, they are kind of computer people. (...) Before I answer[ed you], I Googled you. My son always says he’s Googling. And it did show that you are a PhD student at U of M. And then I recognized your email, that “umich” email from the school...

Even after receiving formal communication, participants cross-referenced information with family members and online resources to verify the legitimacy of the researcher and study. This was not the only participant to reference family members. In one phone interview, after a long conversation with the first author, a participant revealed that their husband had been quietly listening in to ensure that the interaction was genuine and not part of a scam.

4 THE ROLE OF TRUST IN RECRUITMENT

As detailed above, recruitment efforts were complicated by evolving challenges, largely driven by distrust. Previous research in human-computer interaction has examined the growing issue of “bad actors posing as legitimate research participants,” highlighting how this can, among other issues, distort the representation of the lived experiences of the actual population being studied [22]. These “imposter participants” are significant because they increase the labor required for recruitment: “The incidence of fraudulence in qualitative research brings up several challenges and questions for the qualitative researcher—how to confirm fraud when relying on one’s subjective expertise, how to cope with the stress and decision-making caused by fraudulent behavior, and how to respond when integrity is questioned” [22, p.2]. This case study takes an alternative position on the same central issue of (dis)trust in the often-momentary connection between participant and researcher: instead of bad actors posing as legitimate participants, we interrogate a situation in which legitimate research participants question whether or not the researcher is a bad actor posing as a legitimate researcher. In such a case, the challenges and questions above are flipped: how can potential participants confirm legitimacy when relying on one’s subjective expertise, cope with the ever-widening landscape of online distrust, and respond to additional context, both individually and collectively?

This case study, then, preliminary interrogates these questions and emphasizes the reciprocal nature of trust and distrust in the context of research recruitment. It recognizes that distrust is not only a valid response to recruitment efforts but is also a critical lens through which to understand the complexities of engagement with potential participants and at-risk users. In research surrounding technology use, non-use is as analytically interesting as use as it

provides valuable insights into the social, cultural, and individual factors that shape how and why people choose to engage with technology [8, 24]. Similarly, distrust offers crucial insights into the dynamics and complexities of relationships, behaviors, and systems, as well as into our roles as researchers, our research aims and objectives, the spaces where distrust arises, and the perspectives of potential participants and collaborators.

Historically, recruitment has always faced challenges related to non-response, a phenomenon well-documented in survey methodology that highlights how factors such as survey design, the medium of delivery, and perceived legitimacy influence participant engagement [17]. Elsewhere, in considering online recruitment for qualitative research, Allison et al. noted potential participant suspicion around social media advertisements for research recruitment, reflecting broader concerns about privacy and trust in online recruitment [1]. In the twelve years since Allison et al., the prevalence of fraudulent activity online, and scams more specifically, has only increased. As such, it is an unsurprising reality that potential participants exhibit increased distrust towards recruitment, especially concerning sensitive topics and at-risk populations. This heightened distrust signifies a proactive and protective response from individuals, shaped by their past experiences and the broader socio-technological context. In recognizing these dynamics, this paper seeks to contribute to a deeper understanding of how trust and distrust inform the recruitment process, ultimately aiming to foster more effective and ethically sound engagement with participants.

4.1 Negotiating trust and distrust during recruitment

Trust in the recruitment process, like online research ethics more generally, should be thought of as constantly negotiated [19]. Researchers navigate the shifting boundaries of trust and distrust, adapting to the specific contexts and concerns of their participants (and vice versa). Below, we present a non-exhaustive list of key factors that informed the process of navigating trust and distrust during recruitment, from the researcher's perspective. We compile these insights alongside those from Section 3 into Table 1 to provide succinct takeaways and actionable steps for researchers. While these considerations are not meant to fully assuage distrust, they can inform approaches to recruitment.

Context. Markham and Buchanan encourage us to critically consider the context in which the participant and researcher are situated [19]. In this consideration, trust is not merely a matter of interpersonal trust between researcher and participant but is also shaped by the broader environment, including the platform used for recruitment. Understanding the platform's role in mediating trust then becomes essential in fostering recruitment [27]. As Henderson et al. point out, platforms have “particular affordances, and concomitant consequences, that make [them] unlike other research contexts” [16, p.546]. These affordances and consequences influence the ways users interact with content on the platform. For example, Nextdoor's structure, designed for hyper-local neighborhood-based interaction, shapes participant responses by fostering a close-knit but wary community dynamic. This can be seen in other research on Nextdoor in which Nextdoor is described as a “surveillance-heavy state” that, in some ways, mirrors the cultures of vigilance

that inform physical neighborhood watches [9, 10, 18]. This feeling of vigilance was noted by research participants, including one participant who described his experience navigating Nextdoor as one marked by pervasive distrust: “People are like ‘what’s going on here, this guy knocked on my door, my car got broken into,’ you know, all this stuff going on... it creates an atmosphere of menace that I actually don’t feel [in the community] myself.” In such an environment, recruitment is likely to be perceived through community vigilance and heightened scrutiny, especially on a sensitive subject like scams. As such, this case study suggests understanding the recruitment context is essential.

Institution. While interpersonal rapport between researcher and participant builds trust, research has shown that institutional trust plays a critical role in shaping participants' willingness to engage in research [15]. In this way, potential participants may feel more trusting toward research that is affiliated with a reputable or well-known institution and view this affiliation as a marker of legitimacy. Potential participants may also have personal ties with or feelings towards the institution—recall the user who wanted to get in touch because they were a graduate of the institution. However, this previous research was complicated in our case by potential participant reactions to institutional logos, URLs, email addresses, and the like. Recall users who suggested letterheads and other affiliations could be faked or appropriated by scammers as signifiers of trust. Nextdoor user views on this potential appropriation are backed up by research in social engineering research that suggests scammers use trust signifiers as legitimizing agents: “Social engineers pretend to be executives of corporations, attorneys, retired FBI officials, and doctors in order to further their credibility” [3, p.29]. This case study suggests institutional legitimacy is still valued, but distrust can also be expected, depending on the recruitment materials, proposed research, and context of recruitment. In some cases, professional partnerships with multiple or local institutions could further bolster user confidence. As Freed et al. suggest, research collaborations with well-respected and local organizations or advocacy groups can lend credibility to the research and make potential participants more likely to engage [12].

Collective interrogation. This case study argues for the value of collective interrogation of recruitment materials. To be sure, potential participants have always scrutinized recruitment materials—consider a potential participant reading a recruitment flyer in a library and deciding not to respond. However, this process is altered when undertaken collectively. Despite (or perhaps owing to) the prevalence of distrust on Nextdoor, users worked together to interrogate the legitimacy of the first author's posts. In this way, recruitment can be significantly influenced by the collective interrogation and validation of the researcher and their project by the user community. Recruitment in a public forum, such as an online platform, enables open dialogue about the legitimacy of the research and provides opportunities for multiple voices to contribute. This communal discussion and confirmation can be more powerful than an individual researcher's claims of credibility, such as stating an affiliation with a prestigious institution. Recall, for instance, the user who said links from the first author that claimed legitimacy did not prove anything. However, when users themselves independently verify the researcher's credentials—by finding their personal

or institutional website, for example—the community has effectively done its own legwork, building a collective sense of trust. This collective interrogation shifts some of the power dynamics in recruitment, allowing users to take an active role in verifying the legitimacy of the study, ensuring that trust is not passively given or invisibly denied but collaboratively and publicly constructed.

Moderation of commentary. Following this, researchers can moderate commentary on their online recruitment materials. On a practical level, moderation allows researchers to address direct questions about the study, such as eligibility criteria like age or location. This kind of engagement helps clarify the purpose of the study and resolves immediate concerns, creating a smoother recruitment process. Additionally, being available as an active voice can foster trust and make potential participants feel more comfortable engaging with the study. However, as noted by Waling et al., the moderation of commentary goes beyond practicality and serves an ethical function [27]. By engaging in discussions and addressing concerns, researchers provide critical information that extends beyond recruitment, offering valuable insights into broader issues affecting the targeted population. For instance, in our study, we shared perspectives on digital literacy, platform navigation, and security concerns raised by potential participants. When the first author explained how QR codes work and demonstrated ways to verify the safety of QR codes—such as hovering over them to preview their landing page—this guidance not only supported recruitment efforts but also empowered users to navigate digital platforms more securely in their daily lives.

It should be noted that the value of this moderation extends beyond actively engaged users. Even if individuals do not leave comments, they can still benefit from reading the moderated discussion. As noted, the first author's Nextdoor posts were viewed 13,700 times and garnered 83 comments—a ratio of 165:1. Previous research has highlighted the significance of “lurkers,” those individuals who utilize digital environments without evidently participating [7, 11]. Such research has noted how these users are “active, reading, listening, being receptive, connecting, forwarding” despite few footprints of their activity [11, p.647]. These users, though silent, may connect with and act upon the information provided in moderated discussions, amplifying the impact of moderation efforts. Thus, the moderation of commentary should not be seen as a tool to *control* the narrative of recruitment but as a means to inform and engage a broader audience beyond recruitment itself. By moderating the collective interrogation of recruitment materials, researchers can contribute to their immediate goals of recruitment while also addressing critical issues and offering value that transcends the study's immediate aims.

5 CONCLUSION

This case study has highlighted the complexities of recruiting a particular at-risk population, older adults affected by scams, specifically in the online context of Nextdoor. We began by outlining the challenges of recruitment, emphasizing how platform-specific dynamics and heightened distrust shaped potential participant responses. Through an analysis of user interactions, we traced three common examples of distrust and further examined how recruitment materials and researcher actions could foster trust or amplify

doubt. Ultimately, we demonstrate that trust in recruiting is not static but is dynamically negotiated on online platforms, requiring researchers to consider platform context while actively acknowledging and addressing potential participant concerns.

Stage	Insight	Description	Actionable Steps
Before Recruitment	Address Preliminary Reactions to Materials	Consider in advance how targeted populations might react to recruitment, data collection, use of language.	Pilot recruitment materials ahead of their release. Stagger recruitment to modify materials according to reactions.
	Provide Multiple Layers of Legitimacy	Materials should reference one’s legitimacy, both visually and textually, to support engagement and trust.	Add institutional markers. Partner with community organizations and make note of their involvement in materials.
	Adapt Recruitment Based on Context	Tailor recruitment approaches to the platform(s) being used, as platform dynamics significantly influence responses.	Consider the platforms and use them ahead of recruitment. Read about platform dynamics and their culture ahead of time to tailor materials.
	Be Prepared for Engagement	Researchers should anticipate potential participant engagement that requires attention.	Consider the time frame for recruitment and schedule time in anticipation of moderating recruitment commentary.
During Recruitment	Shift Power Dynamics to Empower Users	Foster a collaborative atmosphere where potential participants can verify researcher identity and the study themselves.	Encourage participants to validate the researcher’s identity and study details through independent means. Allow the community to assess researcher and research credibility collectively.
	Acknowledge and Address Distrust	Recognize that distrust is a reasonable response, particularly with at-risk populations and sensitive topics.	Build trust by reaffirming and addressing concerns transparently, demonstrating patience, and allowing the community to remain distrustful.
	Moderate Commentary Thoughtfully	Use moderation of commentary to build trust and provide valuable information beyond a single study’s recruitment.	Actively respond to questions, respectfully clarify misunderstandings, and offer tips that go beyond recruitment. Ensure moderated discussions are clear and informative, benefiting users who observe but do not directly engage.
	Leverage Institutional Trust with Care	Signal credibility through institutional affiliations but recognize their limitations.	Combine institutional signals from recruitment materials with transparent communication to build trust. See if valued institutions will support platform engagement. Recognize that institutional trust is also dynamic.

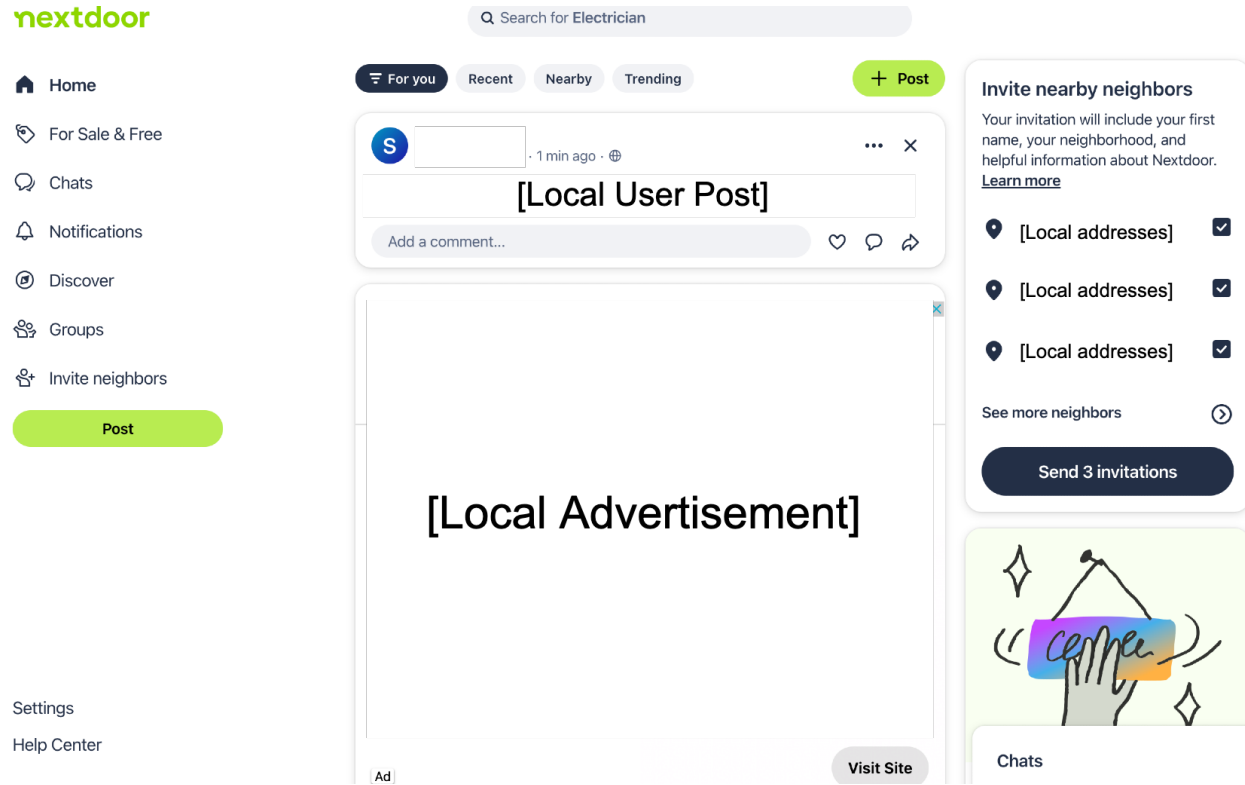
Table 1: Practical insights for researchers recruiting at-risk populations in online contexts.

References

- [1] Susannah Allison, Jose A Bauermeister, Sheana Bull, Marguerita Lightfoot, Brian Mustanski, Ross Shegog, and Deb Levine. 2012. The intersection of youth, technology, and new media with sexual health: moving the research agenda forward. *Journal of Adolescent Health* 51, 3 (2012), 207–212.
- [2] Sam Ankenbauer and Robin N. Brewer. 2024. Spirits in the Material World: Older Adults' Personal Curation of Memory Artifacts. *Companion Publication of the 2024 Conference on Computer Supported Cooperative Work and Social Computing* (2024).
- [3] Brandon Atkins, Wilson Huang, et al. 2013. A study of social engineering in online frauds. *Open Journal of Social Sciences* 1, 03 (2013), 23.
- [4] Brooke Auxier and Monica Anderson. 2021. Social media use in 2021. *Pew Research Center* 1 (2021), 1–4.
- [5] Jan Bailey, Louise Taylor, Paul Kingston, and Geoffrey Watts. 2021. Older adults and “scams”: Evidence from the mass observation archive. *The Journal of Adult Protection* 23, 1 (2021), 57–69.
- [6] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. 2024. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 635–654.
- [7] Robin Brewer, Sam Ankenbauer, Manahil Hashmi, and Pooja Upadhyay. 2024. Examining voice community use. *ACM Transactions on Computer-Human Interaction* 31, 2 (2024), 1–29.
- [8] Anders Bruun, Rikke Hagensby Jensen, Jesper Kjeldskov, Jeni Paay, Camilla Mejlbj Hansen, Katarína Leci Sakáčová, and Mette Hyllested Larsen. 2020. Exploring the non-use of mobile devices in families through provocative design. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 813–826.
- [9] Madiha Zahrah Choksi, Marianne Aubin Le Quééré, Travis Lloyd, Ruojia Tao, James Grimmelman, and Mor Naaman. 2024. Under the (neighbor) hood: Hyperlocal Surveillance on Nextdoor. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–22.
- [10] Amanda Druck. 2021. As a hyperlocal form of social media, Nextdoor helps neighbours connect—but not always for the better. In *Debating Communities & Networks XII Conference*. 1–9.
- [11] Noella Edelmann. 2013. Reviewing the definitions of “lurkers” and some implications for online research. *Cyberpsychology, Behavior, and Social Networking* 16, 9 (2013), 645–649.
- [12] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. “A Stalker’s Paradise” How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–13.
- [13] Sarah Friar. 2022. Nextdoor’s CEO Sarah Friar is Opening Doors for Smaller Businesses. *TIME* (September 15 2022). <https://time.com/6210774/nextdoor-ceo-sarah-friar-interview/>
- [14] Luke Gelinias, Robin Pierce, Sabune Winkler, I Glenn Cohen, Holly Fernandez Lynch, and Barbara E Bierer. 2017. Using social media as a research recruitment tool: ethical issues and recommendations. *The American journal of bioethics* 17, 3 (2017), 3–14.
- [15] Marilys Guillemin, Emma Barnard, Anton Allen, Paul Stewart, Hannah Walker, Doreen Rosenthal, and Lynn Gillam. 2018. Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics* 13, 3 (2018), 285–294.
- [16] Michael Henderson, Nicola F Johnson, and Glenn Auld. 2013. Silences of ethical practice: Dilemmas for researchers using social media. *Educational research and evaluation* 19, 6 (2013), 546–560.
- [17] Susan N Hoddinott and Martin J Bass. 1986. The dillman total design survey method. *Canadian family physician* 32 (1986), 2366.
- [18] Katie Lambright. 2019. Digital redlining: The Nextdoor app and the neighborhood of make-believe. *Cultural Critique* 103 (2019), 84–90.
- [19] Annette Markham, Elizabeth Buchanan, with feedback from the AOIR Ethics Working Committee, et al. 2012. Ethical decision-making and internet research: Recommendations from the AoIR Ethics Working Committee (Version 2.0). *AoIR Ethics Working Committee* (2012).
- [20] Nextdoor Blog. 2012. Seniors Connecting Online with Nextdoor. <https://blog.nextdoor.com/2012/06/26/seniors-connecting-online-with-nextdoor/>
- [21] Nextdoor, Inc. 2024. Nextdoor: The Neighborhood Hub. <https://www.nextdoor.com>.
- [22] Aswati Panicker, Novia Nurain, Zaidat Ibrahim, Chun-Han Wang, Seung Wan Ha, Elizabeth Kaziumas, Maria K Wolters, and Chia-Fang Chung. 2024. Forms of Fraudulence in Human-Centered Design: Collective Strategies and Future Agenda for Qualitative HCI Research. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. 1–5.
- [23] Qualtrics, Inc. 2024. Qualtrics: Experience Management Platform. <https://www.qualtrics.com>.
- [24] Devansh Saxena, Patrick Skeba, Shion Guha, and Eric PS Baumer. 2020. Methods for generating typologies of non/use. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW1 (2020), 1–26.
- [25] Bernd Carsten Stahl. 2006. On the difference or equality of information, misinformation, and disinformation: A critical research perspective. *Informing Science* 9 (2006), 83.
- [26] Fiona Vera-Gray. 2017. “Talk about a cunt with too much idle time”: Trolling feminist research. *Feminist Review* 115, 1 (2017), 61–78.
- [27] Andrea Waling, Anthony Lyons, Beatrice Alba, Victor Minichiello, Catherine Barrett, Mark Hughes, and Karen Fredriksen-Goldsen. 2022. Recruiting stigmatised populations and managing negative commentary via social media: a case study of recruiting older LGBTI research participants in Australia. *International journal of social research methodology* 25, 2 (2022), 157–170.
- [28] Rania Wasfi, Zoe Poirier Stephens, Meridith Sones, Karen Laberee, Caitlin Pugh, Daniel Fuller, Meghan Winters, and Yan Kestens. 2021. Recruiting participants for population health intervention research: effectiveness and costs of recruitment methods for a cohort study. *Journal of medical Internet research* 23, 11 (2021), e21142.

A APPENDIX

A.1 Nextdoor User Interface



Settings
Help Center


A.2 Flyer for Recruitment

HAVE YOU BEEN THE TARGET OF SCAMS OR FRAUD?

OLDER ADULT PARTICIPANTS NEEDED

The University of Michigan is looking for older adults (65+) who have recently experienced fraud or scams (online, over the phone, or in person). This research will help inform how we collectively understand the personal and social impacts of fraud and scams, as well as how systems may be designed to better remedy situations after a fraud or scam has occurred. If interested, please take the survey, linked below.

TAKE THE SURVEY:



Or go to:
tinyurl.com/2kr5zbky


Or call me to schedule a phone survey:
(734) 330-2085

REQUIREMENTS:

- 65 years and over
- Live in Michigan
- Experienced scam(s) or fraud in the recent past

THANK YOU!

For questions or concerns, please contact:
samank@umich.edu



SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN