# "It didn't feel right but I needed a job so desperately": Understanding People's Emotions & Help Needs During Financial Scams


Jake Chanenson*
Google
USA
jchanen1@uchicago.edu

Tara Matthews
Google
USA
taramatthews@google.com

Sunny Consolvo
Google
USA
sconsolvo@google.com

Patrick Gage Kelley
Google
USA
patrickgage@google.com

Jessica McClearn†
Google
USA
jessica.mcclearn.2021@live.rhul.ac.uk

Sarah Meiklejohn‡
Google
USA
s.meiklejohn@ucl.ac.uk

Abhishek Roy
Google
USA
abhishekroy@google.com

Renee Shelby
Google
USA
reneeshelby@google.com

Kurt Thomas
Google
USA
kurtthomas@google.com

Amelia Hassoun§
Google
UK
miahassoun@google.com



## Abstract

Online financial scams represent a long-standing and serious threat for which people seek help. We present a study to understand people's in situ motivations for engaging with scams and the help needs they express before, during, and after encountering a scam. We identify the main emotions scammers exploited (e.g., fear, hope) and characterize how they did so. We examine factors—such as financial insecurity and legal precarity—which elevate people's risk of engaging with specific scams and experiencing harm. We indicate when people sought help and describe their help-seeking needs and emotions at different stages of the scam. We discuss how these needs could be met through the design of contextually-specific prevention, diagnostic, mitigation, and recovery interventions.



## CCS Concepts

• **Security and privacy → Social aspects of security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**; • **Social and professional topics → Computer crime**.

## Keywords

Online financial scams, scams, help seeking, online safety, user states framework, at-risk users, digital safety, technology-facilitated abuse

**ACM Reference Format:**
Jake Chanenson, Tara Matthews, Sunny Consolvo, Patrick Gage Kelley, Jessica McClearn, Sarah Meiklejohn, Abhishek Roy, Renee Shelby, Kurt Thomas, and Amelia Hassoun. 2026. "It didn't feel right but I needed a job so desperately": Understanding People's Emotions & Help Needs During Financial Scams. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3772318.3790556


## 1 Introduction

Online financial *scams*[1] represent a long-standing and serious threat [1, 20, 23, 24, 36, 92, 116, 122]. Losses reported to the U.S. Federal Trade Commission (FTC) exceeded $12.5 billion USD in 2024 [61]. However, truly accounting for the impact of scams is challenging, as most incidents go unreported and many harms are not financial [6, 76]. Scammers' tactics are constantly evolving and growing in sophistication [20, 137] as they attempt to engage and exploit targets[2] [23, 24, 36, 69, 76, 93]. Targets span all ages, genders, and demographics [8, 20, 61, 76, 116, 122]. Understanding why and how people fall prey to scams, and what help they need in

*Also with University of Chicago.
†Also with Royal Holloway, University of London.
‡Also with University College London.
§Also with University of Cambridge.



*CHI '26, Barcelona, Spain*



ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790556


[1]Throughout this paper, we use *scams* to refer to *online financial scams*, which is synonymous with *online financial fraud*, unless otherwise specified.
[2]We use the term *targets* to refer to people a scammer attempts to engage, engages, or harms. We avoid the term *victims*, because it has been critiqued as being associated with negative attributes, such as powerlessness or weakness, that can be both stigmatizing and internalized [99].

critical moments before, during, and after encountering a scam, is necessary to mitigate this substantial harm.

Existing HCI and computer security research has investigated specific scam types—including romance [5, 27, 39, 40, 128], pig butchering [93], and e-commerce [14, 15], among others [10]—but relatively few studies have examined the experiences and needs of targets across a range of scam types and scammer tactics as scams unfold [17, 94]. Emerging research details how online communities provide emotional support and vetted guidance toward scam recovery, also identifying knowledge deficits that increase a target's susceptibility [17, 94]. Building on this work, we focus on targets' emotional states at key moments during a scam—such as when they are lured in (or "hooked" by the scammer), realize something is wrong, or ask for help. Our goal is to understand why targets engage with specific scams, why some targets experience elevated risk, and what types of help targets need at different stages of the scam to avoid, diagnose, mitigate, and recover from harm.

We examine 405 posts from Reddit that involve seeking help for a range of known and emerging scams. Posters commonly describe their encounters, providing rich descriptions of their emotions and needs at different stages of the scam. Our analysis builds on existing frameworks and research [10, 87, 113, 114, 126] to provide practical empirical insights. Systematically examining a range of scam types helps identify patterns in what motivates targets to engage and how scammers manipulate those motivations. To inform the design and development of effective scam interventions, we investigated the following research questions:

RQ1. What *motivates* people to consider engaging with scams and ultimately to comply with scammer requests?
RQ2. *When* during a scam do people seek help? What are their *emotions and help needs* at different stages of the scam?
RQ3. How do *contextual risk factors* augment scam susceptibility and harm?
RQ4. How might people's emotions and needs at different stages of the scam be used to *inform interventions*?

Our primary contribution is a qualitative analysis of the emotions and help needs people expressed while experiencing scams, especially the emotional motivations they had for engaging with scams. We found five main *emotional motivations* across 12 types of scams that scammers manipulated to engage targets: Fear, Guilt & Goodness, Trust, Hope, and Belonging. Understanding these underlying motivations (like the hope for a job in a difficult economy) helps explain why certain people (such as those who are financially insecure) experience an elevated risk of being targeted, engaging with, and harmed by [125] specific scams.

We also propose an incremental expansion of the User States Framework [87][3] for scams, adding nuance to the Active Event state. We use this framework and build on prior help-seeking research [126] to map users' help-seeking needs—Sensemaking, Guidance, Therapeutic, and External Action—to their emotional context and stage in the scam's lifecycle.

Our method enables us to contribute novel findings on targets' emotions and needs in the midst of an active scam. Overall, this work identifies opportunities for in situ scam interventions to help people effectively prevent, diagnose, mitigate, and recover from scams.

[3]The User States Framework [87] maps a user's expected needs and emotional state of mind before, during, and after technology-facilitated attacks into the states of Prevention, Monitoring, Active Event, and Recovery.

## 2 Related Work

We situate our work in the broader context of scam frameworks, the motivations known to affect how and why targets engage with scams, and online help-seeking patterns for scams.

### 2.1 Scam Frameworks

Previous research has produced scam frameworks reflecting different organizing principles. Some categorize scams by their structural or technical elements. Beals et al. [10] developed a five-level taxonomy that, at its highest level, distinguishes between fraud targeting individuals and organizations. Their sub-categories for individual fraud include consumer investment fraud, consumer products and services fraud, employment fraud, prize and grant fraud, phantom debt collection fraud, charity fraud, and relationship and trust fraud. Similarly, other frameworks classify scams by the channel through which they occur (e.g., web, mobile, telephone, physical) [98], the specific actions and deceptions involved in their execution (e.g., visceral appeals or pressure and coercion) [24], or the primary narrative used for persuasion, such as a threat, an offer, or a promise [43]. This structural understanding of scams is strengthened by research on human factors, with Levi [85] analyzing the fluid, networked organization of perpetrators, and Button et al. [24] synthesizing research on the characteristics and vulnerabilities of targets. Together, existing scholarship demonstrates that a comprehensive understanding of scams must integrate analyses of scam mechanics (including scammer tactics) and target experiences (including their motivations, differentiated risks, and support needs).

Scam impacts can extend beyond financial harm to inflict emotional, relational, and physical harm [23]. Targets often suffer intense emotional distress, including anxiety, depression, shame, and post-traumatic stress disorder (PTSD) symptoms [2, 37, 129], which can lead to erosion of trust [68] and social withdrawal [66, 72, 111]. The emotional toll is often felt more intensely than the financial harm [91, 129], can intensify existing health issues [25], and may result in suicidal ideation [42]. Consequently, effective interventions should be trauma-informed [49] and address scams' emotional dimensions. Absent from these scam frameworks is a perspective of the needs of targets across scam types, as scams unfold.

### 2.2 How and Why Targets Engage With Scams

We argue that scam susceptibility is a dynamic state influenced by targets' contextual risk factors [125] and scammer tactics [69]. Lack of digital literacy [45, 47, 88, 94], financial literacy [135, 136], and scam literacy [17, 94] all affect susceptibility. Timing [22, 86, 132], environmental contexts [64, 132], and misplaced trust in platform security features [94] further shape target engagement. Scammers exploit both universal cognitive biases, such as optimism bias and sunk cost fallacy [16, 47], and specific situational risk factors, such as financial need, life transition, or loneliness [26, 93, 120].

Social science research has analyzed psychological factors shaping scam susceptibility [21, 26, 30, 44, 69, 80, 92], using surveys to

find correlations between susceptibility and traits like impulsivity [75], high trust in others [57], or neuroticism [123]. Concurrently, computing literature has outlined the multi-stage mechanics of specific schemes like advance-fee fraud [48] and "pig butchering" scams [93] by detailing classic manipulation techniques like appeal to authority [90], foot-in-the-door [59], norm activation [115], and manufactured urgency [7]. Scammers apply these techniques by impersonating authority figures, escalating demands, invoking social obligations, and leveraging emotional manipulation to undermine rational decision-making [46, 83, 120].

While researchers importantly suggest that scam awareness, digital literacy, and emotional support interventions are needed [17, 94], existing work does not generally identify when, from a target's perspective, specific interventions would be effective. As Hassoun et al. [70] argue, deficit-based information literacy interventions often occlude the factors that most motivate people to engage online and must be informed by contextual understandings of their specific motivations and practices to affect change. Chen et al. [32] found, for example, that increased engagement with scam prevention communication did not affect migrant workers' ability to assess scam risks or decrease their victim-blaming beliefs—but a reduction in fear and increased sense of self-efficacy (i.e., confidence that they could respond effectively to a scam, even if they perceived its risk as severe) did improve scam prevention skills.

Building on these insights, we systematically explore how emotional motivations and scammer tactics drive target engagement with specific scams. Drawing on Roy et al.'s [113] scammer manipulation tactics, we describe the emotional motivations that "hook" targets to engage in scams. We mobilize Warford et al.'s [125] At-Risk Framework to understand what makes specific users more at risk of being targeted, hooked, and/or harmed by scams. We propose an expansion of the User States Framework [87] to map users' help-seeking needs to their emotional motivations and scam stage, identifying critical moments for interventions that respond to people's in situ needs.

## 2.3 Online Help Seeking For Scams

Formal scam reporting (e.g., to government agencies, support organizations, law enforcement or platforms) is one path available to scam targets seeking help. However, scam incidents are chronically under-reported [1, 94]. Studies highlight both personal motivations for justice and altruistic reasons for reporting [40, 89], but the majority of studies reveal persistent obstacles to formal help seeking. Research finds the most prominent obstacles are emotional, including shame, loss of trust, and self-blame [5, 38, 66, 91, 111, 128]. Victim-blaming norms and systemic issues like fragmented reporting channels and trauma-insensitive procedures isolate targets and dissuade them from reporting [6, 30, 41].

While these barriers to formal help seeking persist, the emotional safety and pseudonymity of online forums can reduce stigma and foster candid peer support [34, 121]. Within the computing literature, a small but growing body of work has examined scam-related help seeking in these spaces. Studies have categorized the types of help sought for image-based sexual abuse, including sextortion [126], documented how cryptocurrency communities educate users about scams [33], and identified common user knowledge gaps and peer support mechanisms in scam-focused subreddits [16, 94].

While prior work characterizes the types of help-seeking interactions that occur online, a systematic understanding of how a target's needs evolve throughout the course of a scam is still needed. In particular, many studies examine scams after they are over, with an emphasis on prevention and recovery support. Building on recent work examining the role Reddit communities can play in helping people who experience scams [17, 94], we contribute a detailed synthesis of help needs throughout scams, including a nuanced look at targets' experiences as scams unfold. We draw on the User States Framework [87] to map a target's in situ emotions and help needs onto their stage in a digital-safety (i.e., scam) event. This work contributes novel insights that can inform contextually-specific scam interventions.

# 3 Methodology

We derive our analysis of help seeking for scams from data publicly shared on Reddit. We focus on Reddit due to its large user base, diverse communities, and the relative anonymity it affords, which may encourage users to seek help [34, 121]. We adopt Wei et al.'s mixed-methods approach—previously developed to examine help seeking for image-based sexual abuse on Reddit [126]—to curate a dataset for in-depth qualitative analysis. Our goal in curating this dataset was to include a diverse range of known and emerging scams, not to seek a representative sample that covers all possible scams. We describe our approach to building a dataset for analysis, our coding process, ethical considerations, and limitations.

## 3.1 Defining Help Seeking for Scams

To be considered for inclusion, a post had to involve help seeking for scams. We considered a post to involve help seeking for scams if the poster sought information, advice, or support to cope with a scam-related issue for themselves or someone else. We interpreted such support broadly to include emotional or therapeutic needs, which posters might express, for example, through venting, helping others, or telling their story about scams. We use Beals et al.'s definition of financial scams [10]:

> *"Intentionally and knowingly deceiving the [target] by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain."*

Like Beals et al. [10], we excluded identity theft, account compromise, or malware, focusing on events where targets were persuaded to actively engage (rather than unknowingly stolen from). We also excluded related attacks like phishing, account compromise, or malware, which scammers used as part of their set of tactics to carry out a scam.

## 3.2 Curating a Reddit Dataset

*Filtering Reddit Data.* In our first step toward our goal to include a diverse range of known and emerging scam experiences in our dataset, we sought to filter Reddit data by sampling posts from relevant subreddits (Figure 1, ❶). To begin, we wanted to identify

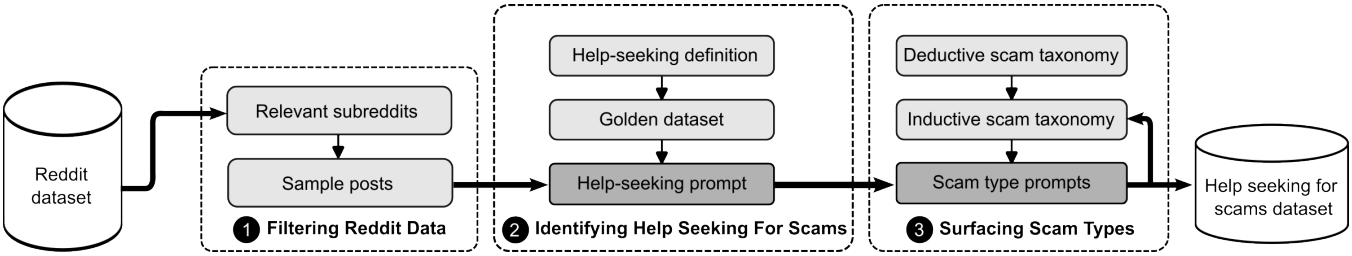


**Figure 1: Overview of our data curation pipeline. Steps involving an LLM are in dark shaded boxes. Steps informing LLM prompt creation are in the lighter shaded boxes above these darker shaded boxes. ❶ We began by sampling an initial dataset of 637,600 posts from relevant subreddits. ❷ We examined each of these posts using an LLM to identify 13,800 posts likely related to scam help seeking. ❸ We used manual review and LLM-assisted annotation to categorize posts into select scam types, sampling 500 posts across these scam types. We reduced this help-seeking dataset to a final set of 405 high-quality posts about 12 scam types after applying relevance and quality criteria in the qualitative analysis stage.**

Reddit communities—called *subreddits*—that were likely to have a high prevalence of help seeking for scams. To do so, we manually reviewed subreddits with more than 1,000 subscribers, accessing them via a site maintained by Reddit.[4] We examined each subreddit, focusing on its description and recent posts, and selected communities that had recent posts and content relevant to scams. We identified 134 subreddits with this method. These subreddits included those that were dedicated to platforms frequently targeted by scammers (e.g., *r/cashapp*, *r/facebookmarketplace*); that specialized in providing support related to scams (e.g., *r/scams*, *r/cryptoscams*); or that were about topics where scams were relevant, like digital safety or personal finances (e.g., *r/cybersecurity_help*, *r/povertyfinance*). Next, we sought to sample a diversity of scam-related data from these 134 subreddits. To do this, we randomly sampled up to 10,000[5] *original posts*—that is, the first post in a discussion thread[6]—from each of the 134 subreddits. We sampled these from an existing crawl of Reddit that adheres to robots.txt and crawler guidelines limiting to posts created between December 1, 2023 - December 1, 2024. Due to variations in community activity, not all subreddits had 10,000 posts within our analysis window. This resulted in a corpus containing 637,600 posts overall (with an average of 4,758 per subreddit).

*Identifying Scam Help-Seeking Posts.* To identify help-seeking posts for scams in this corpus of 637,600 posts, we utilized a large language model (LLM) (Figure 1, ❷). We first constructed a golden dataset of 698 examples, balanced with 50% positive examples (help seeking for scams) and 50% negative examples (i.e., not help seeking and/or not about scams). We created this golden dataset by randomly sampling 100,000 posts from the same 134 subreddits as the "Filtering Reddit Data" step, then used a keyword search (e.g., "scam," "fraud") to create a pool of candidate posts, and finally manually reviewed each post to select positive and negative examples of help seeking for scams. The golden dataset provided a ground-truth reference, allowing us to objectively iterate on prompts and measure how well the LLM identified help-seeking posts for scams. Our final classification prompt (Figure 2) achieved a recall of 98% and a precision of 68% on Gemini 1.5 Flash. We optimized for recall over precision to support our goal of including a diversity of scam types. In total, our model identified 13,800 potential help-seeking posts for scams. We used manual validation later in the process (described below) to ensure that posts in our final dataset met our definition of help seeking for scams.

*Selecting Posts for a Diversity of Scam Types.* Next, we performed a series of manual and LLM-assisted annotation passes to select 500 posts for in-depth analysis (Figure 1, ❸), reflecting the number of posts we needed to reach meaning sufficiency given our research questions [19]. To do so, we began with Beals et al.'s [10] taxonomy to include a diversity of known scams, and supplemented it by examining a subset of randomly sampled posts from the data to include posts describing emergent scam types not included in their taxonomy (e.g., cartel scams). Next, we used Gemini 1.5 Flash to annotate posts according to this initial set of scam types, and then drew a stratified random sample of 200 posts per scam type (2,000 total posts) from the 13,800 potential scam help-seeking posts. A single researcher examined the 2,000 posts to further refine scam types and confirm the posts were instances of scam-related help seeking suitable for in-depth qualitative analysis (i.e., detailed enough to determine (a) what kind of scam it likely was and (b) what kind of help the poster was seeking). The researcher then met with the rest of the research team to discuss post inclusion. We performed this iterative examination twice more to refine our selections. To make inclusion decisions during this process, we used our judgment, knowledge of scams, and experience reading many help-seeking posts (for this and other work). To exclude posts from scammers themselves [118], we especially scrutinized posts that mentioned specific individuals or services claiming to assist with scam recovery, or referenced potential scammer contact information. Finally, from the remaining posts we randomly selected 50 per scam type to produce the 500 posts. This set of scam types was not exhaustive of all possible scams.

[4]At the time of publication, Reddit lists its largest subreddits from most to least subscribers at this site: www.reddit.com/best/communities/1/.
[5]Setting a cap of 10,000 posts per subreddit provided a practical balance: it allowed for a broad coverage of active scam-related communities while still including smaller subreddits, supporting our goal of including a diverse range of scam-related help-seeking experiences.
[6]We include original posts because they focused on help seeking, and exclude comment threads which tended to focus more on help giving. For simplicity, we hereafter refer to original posts as *posts*.

You are a financial fraud detection specialist. Your task is to analyze the provided Reddit post to determine if the author is either seeking help because they are a victim of financial fraud, a scam, or financial exploitation, or if the user is offering help or advice related to these topics.

**Focus specifically on posts where users are discussing fraud, scams, and financial exploitation.**
This includes terms like "fraud," "scam," "identity theft," "phishing," "money laundering," "investment fraud," "financial abuse," "embezzlement," and similar terms.

**Ignore posts that are:**
- Requests for customer support related to cryptocurrency transfer issues or lost cryptocurrency coins.
- Account recovery requests.
- Questions about estate planning or money disbursement.

**Subreddit**: {{ subreddit }}
**Reddit post**: {{ text }}

**Task 1:** Does the post meet the definition of seeking or giving help related to scams and fraud? Answer Yes or No.
**Task 2:** Provide a concise reason for why a post is, or is not, seeking or giving help for scams and fraud.

**Figure 2: Prompt used to identify posts likely seeking help for scams. To favor recall over precision, the definition provided to the LLM goes beyond our definition of help seeking for scams. We relied on manual validation to remove imprecise or out of scope results.**

## 3.3 Qualitative Data Analysis

We used codebook thematic analysis (TA) to analyze the 500 posts, beginning with a deductive foundation from established frameworks and refining inductively based on emergent patterns in the data [55]. We used codebook TA primarily for its ability to enable teams of multiple researchers to combine deductive (theory-driven) and inductive (data-driven) analyses of complex datasets [55, 112]. Similar to Wei et al. [126], we used a five-stage codebook TA [112]: (1) initial code sourcing, (2) initial code development, (3) codebook design, (4) codebook application and reliability, and (5) interpretation.

*Initial code sourcing.* As part of the literature review covered in Section 2, we identified potential codes from existing frameworks relevant to our research questions. We drew from five frameworks to source an initial set of candidate deductive codes related to online harms [114], user states [87], scam types [10], help-seeking needs [126], and scammer manipulation tactics [113]. These candidate deductive codes would ultimately form the basic structure of our codebook (summarized in Appendix A), which we updated and expanded inductively.

*Initial code development.* We examined data to refine deductive codes and develop initial inductive codes throughout our data curating process (Figure 1, ❶ ❷ ❸). Three researchers read thousands of posts during this process and met to discuss impressions of the data and develop an early set of deductive and inductive codes. These three researchers applied these initial codes combined with open coding to 100 posts each (300 posts total). They then followed an iterative process of coding more posts, discussing, and updating codes, to ensure our codes were shaped by the data.

*Codebook design.* From our code development process, we designed a codebook with code labels, definitions, instructions on how to apply the codes, and examples. We revised our codebook through our iterative coding process—including into the next stage of applying the codebook. The final codebook is summarized in Appendix A and consisted of:

- *Scam characteristics.* Codes included scam type (informed by Beals et al. [10]), scammer tactics (informed by Roy et al. [113]), and harm type and details (informed by Scheuerman et al. [114]).
- *Help-seeking characteristics.* We refined the help-seeking types from Wei et al. [126] to focus on four different kinds of help posters indicated they needed: support in understanding something (Sensemaking), advice on actions to take (Guidance), emotional support (Therapeutic), or direct intervention from others (External Action).
- *User state characteristics.* We refined the user states from the User States Framework [87], splitting the Active Event category into distinct Diagnostic, Mitigation, and Denial substates (described in Section 4.2). We also noted posters' emotions, motivations, and practices tried.
- *Target characteristics.* Codes included target demographics, the target's relationship with the poster (when they were different people), and at-risk groups or risk factors involved, following definitions in Warford et al. [125].

*Codebook application and reliability.* Four coders iteratively applied the codebook to our dataset of 500 posts (Figure 1, ❸). For reliability, we used a consensus coding approach [28]. Three coders independently coded one-third of the dataset, while a fourth coder coded the entire dataset to improve consistency. During this process, all coders kept memos and iteratively discussed disagreements in weekly meetings and interim online chat. Based on discussions, one coder resolved clear or already-discussed disagreements and marked issues for further discussion. After all disagreements were resolved, two coders split the data and checked all posts to ensure codes were consistently applied (further discussing any issues that arose). In this way, the team iteratively reached agreement on codes across all posts. We sought intercoder consensus, a form of reliability in qualitative analysis [28], to support consistency of judgment among coders [18] for data that were nuanced and codes that were not mutually exclusive.

During this iterative analysis, as our understanding of scams grew, we removed or recategorized a subset of the 500 posts.[7] This process yielded a final dataset of 405 posts across 12 scam types (Figure 1's *Help seeking for scams dataset*).

[7]We removed posts with insufficient detail and posts that appeared to be written by scammers. We did not resample replacement posts when observations were removed; instead, we prioritized maintaining our original sampling frame to avoid introducing selection bias and to ensure consistency in our analytic approach.

*Interpretation.* Once the data were coded, we iteratively reviewed the coded data and notes taken as part of the coding process, and discussed themes. For example, we collated data by scam type, user states, emotions, and motivations. Over multiple discussions, we developed our five emotional motivation themes (Fear, Guilt & Goodness, Trust, Hope, and Belonging). Our development of themes around help needs through scam lifecycles was supported by examining and discussing relationships in the data between help seeking and user state codes.

## 3.4 Ethics

While Reddit data is publicly accessible, we recognize that the Reddit users whose posts we analyzed did not explicitly opt in to the study. Following established HCI guidelines [11, 107, 126, 127, 130] for quoted posts included in this paper, one researcher rephrased these quotes and systematically reverse searched each rephrased quote to ensure they did not return identifiable information. A second researcher reviewed the reworded data to ensure posts' original tone and meaning were preserved. To mitigate re-identification risk, we have chosen not to release the dataset. Although our institution does not mandate IRB review, we adhered to similarly strict ethical standards.

## 3.5 Limitations

Our study is limited to English-language posts on Reddit. Scam experiences discussed on other platforms or in other languages may differ. While data on Reddit language demographics is limited, a recent study found that over 97% of Reddit content was posted in English [74]. This indicates that the geographic distribution of Redditors posting in English likely resembles the overall distribution of active users. In Q4 2023, Reddit's Daily Active Unique (DAUq) user base was composed of 49.8% US (36.4 million) and 50.2% Rest of World (ROW) (36.7 million) users [108].

Our dataset reflected this diversity, containing references to numerous countries and regions—including the UK, India, Malaysia, Europe, and the US—though most posts did not indicate a specific region. The scam types in our study have been observed internationally. For example, Employment scams are a pervasive threat globally, with prior work demonstrating their high prevalence in countries like the UK [95] and India [62, 73]. Charity scams are also a recognized global crisis, with documented cases targeting local and diaspora communities in countries like Malaysia [12, 13].

While the geographic composition of Reddit's active user base is roughly split between US and ROW users, we do not know the location of the specific posters that make up our dataset. We therefore cannot make claims about the impact of sociocultural differences on online help seeking from this data. Follow-up studies that critically analyze sociocultural differences in scam experiences would help explore whether our findings apply across and in specific contexts. We further discuss these potential adaptations in Section 5.4.

As with other studies of scams [16, 17, 94], coverage of scams remains a key challenge and limitation of this work. In selecting scam-related posts for this study, we focused on including a diverse set of scam types and experiences rather than producing a representative sample of all scam-related help-seeking posts. These scam types included deductive and inductive types, as depicted in Figure 1, ❸, but did not include all possible scams (e.g., sextortion [126]).

We used a single LLM for our analysis. Our recall analysis, which measured the model's ability to find all relevant posts using a manually verified reference, demonstrates that our LLM prompt identified 98% of similar posts. To expand coverage of scams, we could add to the scam types we sought to find in Figure 1, ❸.

Because our analysis was focused on people's help-seeking behaviors and needs, we made inclusion and exclusion decisions based on self-reported accounts, which may contain technical inaccuracies, omit key details, or even be deceptive. Thus it is possible that posts were included that were not genuinely help seeking (e.g., scammer posts) or about actual scams (e.g., real debt collection or employment opportunities). Further, focusing on original posts misses help giving and interactions that might be present in comment threads—which have been explored in related work [17, 94] and could be further studied in future work. Finally, our scope was intentionally focused on financial scams based on definitions from prior work [10, 122], and thus our findings may not generalize to other forms of fraud, such as identity theft.

# 4 Results

Our analysis revealed how scammers exploit targets' emotions to initiate and sustain engagement, and when and what kind of help posters seek as scams unfold. First, we introduce five main *emotional motivations* scammers manipulated to engage targets. Second, we show *when* posters seek help (e.g., before or after a target engages with the scammer) and *what* they need at different critical moments of the scam, linking these needs back to the emotional context of the scam. Finally, we share how emotional motivations were intensified for at-risk users.

## 4.1 Emotional Motivations Across Scams

Across the 12 scam types that posters mentioned (see Table 1), our analysis identified five *emotional motivations* that scammers preyed upon in an attempt to overwhelm any initial skepticism on the part of a target and keep them engaged: (1) Fear, (2) Guilt & Goodness, (3) Trust, (4) Hope, and (5) Belonging. As one poster emphasized, these emotions strongly influenced their actions despite being generally security-savvy:

> *"The invalidation from people, even close friends, has been incredibly difficult. I'm not an idiot, and I've even studied cybersecurity. The issue here wasn't technical though, it was emotional. I made a stupid decision in the moment due to my judgment being clouded by urgency and fear. Scams like this are more about manipulating your fear and isolation than about what you know."* (Phantom Debt scam)

We discuss each of these emotional motivations below, synthesizing tactics across individual scam types, since designing effective interventions likely requires tailoring warnings and guidance to each. We provide a high-level overview in Table 1 of how four of these five emotions mapped to particular scam types as the *main* emotional motivation. We share evidence that Belonging was a main emotional motivation in certain scam types and strongly influenced engagement across scam types (as presented in 4.1.5), in

| Main EM | Scam Type | Description | Posts (N = 405) |
|---|---|---|---|
| **Fear** *N = 92* | Cartel | Scammer impersonates a cartel or organized criminal group, threatening to harm a target unless they pay to resolve a fabricated offense. | 47 |
| | Phantom Debt | Scammer impersonates a government agency or debt collector and intimidates a target into paying a fabricated or already paid debt. | 45 |
| **Guilt & Goodness** *N = 91* | Seller | Scammer deceives a target who is selling something online into providing the good without being paid (e.g., using a payment method that is later reversed). | 31 |
| | Accidental Payment | Scammer claims they inadvertently sent money to a target and requests the money be sent back. The original transaction is falsified or reversed. | 9 |
| | Charity* | Scammer impersonates a charity or otherwise seeks donations for a charitable cause from a target. | 51 |
| **Trust** *N = 69* | Authoritative Entity | Scammer impersonates a bank, service, platform, or public figure that a target nominally trusts to deceive the target into transferring funds. | 12 |
| | Romance* | Scammer romantically connects with a target online, manipulating the target's trust and desire for companionship to extract money (often repeatedly and over time). | 45 |
| | Personal Relation | Scammer is or impersonates a family member or friend who deceives a target into transferring funds. | 12 |
| **Hope** *N = 153* | Investment & Crypto Culture* | Scammer deceives a target into transferring funds or crypto into a fake investment opportunity, typically promising large gains and belonging in a community of investors. | 43 |
| | Employment | Scammer offers a fake employment opportunity to deceive a target into transferring some of their own funds, sharing personally identifiable information (PII), working without pay, or acting as a money mule. | 56 |
| | Prize & Grant | Scammer deceives the target into transferring funds to purportedly get access to a larger monetary payout (e.g., a giveaway, a lawsuit payout). | 30 |
| | Buyer | Scammer advertises a good on an online marketplace (that turns out to be fake or defective) that a target buys. | 24 |

*__Belonging__ was also a main emotional motivation in certain scam types marked by an * above.

**Table 1: Breakdown of the main emotional motivations (EM) manipulated by scammers, the different scams that hinge on these EMs, and the number of posts in our dataset.**

line with prior work indicating that it is an important driver for online engagement generally [70, 71].

*4.1.1 Fear.* Some scammers instigated and preyed upon fear, threatening targets with high-stakes consequences from powerful organizations or authorities. Examples included scammers who impersonated cartels, debt collectors, or government organizations (e.g., HMRC, ICE).[8] These scammers threatened targets with severe physical violence (e.g., murder), or escalating financial ruin (e.g., credit score damage, garnished wages, lost housing) unless the target paid the scammer:

> *"A random number started sending me my home address and names and photos of my relatives, and is threatening to kill them. They've been harassing me all night to send the money. I'm scared it's a scam and I'll be left holding the bag but also scared about what happens if I keep saying no."* (Cartel scam)

> *"This [medical company] is threatening my friend about a bill she allegedly owes. They are threatening to send the bill to debt collectors, even though we've sent so much evidence that she already paid the bill. It's been months of this. She's freaking out that this is going to mess up her credit score if it really does go to collection. What do we do?"* (Phantom Debt scam)

Scammers flooded targets with repeated messages to urgently transfer funds to avoid any consequences. Even if targets were

[8]HMRC is His Majesty's Revenue and Customs, the UK's tax, payments and customs authority; ICE is the United States' Immigration and Customs Enforcement.

suspicious of the authenticity of the messages, they expressed being at a loss for how the scammer might have obtained so much personal information, making the target fear the risks of not engaging:

> *"I messaged a few escorts on [website]. I then got a message to my phone saying that I had wasted the girls' time and money, and that I needed to pay $1500 or the organization has men tracking me and will come kill me. I've read posts here that seem similar but none that have this much info, like my cellphone and name and photo. I'm worried they'll find my address too. I just want to know if it is or isn't a scam. Please say I'm not alone in getting these messages – I'm feeling paranoid and can't sleep."* (Cartel scam)

Scammers' use of threats to impose urgency appeared to be a calculated attempt to overload and bypass the target's critical judgment. This tactic often weaponized existing anxieties about legal and financial authority, coercing immediate, irrational compliance. Scammers did not rely on any particular technical tactic to complete the scam transaction, seeming to trust that the emotional tactics eliciting Fear would compel some targets into complying.

Prior to seeking help, targets of Phantom Debt scams commonly discussed trying to verify the authenticity of a message, seeking proof from government institutions, credit bureaus, or their bank. However, many struggled with non-responsive customer service from these legitimate institutions. For Cartel scams, targets were often reluctant to involve law enforcement due to the perceived risk of disclosing how they came into contact with the scammer—which typically occurred after communicating with a sex work service.

*4.1.2 Guilt & Goodness.* Guilt & Goodness-based scams presented targets with emotionally wrought or otherwise personalized scenarios where the target could purportedly help someone in need. For example, scammers posed as charities supporting people in conflict zones (a Charity scam), buyers in online marketplaces who needed a refund due to challenging life circumstances (a Seller scam), or someone who accidentally sent money that critically needed to be refunded (an Accidental Payment scam):

> *"I see so many [social media] stories about people in [conflict zone] needing help and money. Someone added me but they never show their face or really their surroundings either. I know it's probably a scam, but what if it isn't? What if no one else believes them and I'm all they've got?"* (Charity scam)

> *"I was selling this item online and a guy said he'd give me $90 via [Payment App] to reserve it for him to come get next week. He messaged today saying sorry but he didn't want it anymore. He said he knew he'd wasted some of my time and that he was fine with me sending back whatever I thought was fair. My plan was to give it back, but I just wanted to ask whether if I did there was any way for that money to get rescinded by [Payment App]? I don't wanna be scammed but I also don't want to be an asshole."* (Seller scam)

Scammers appeared to use the emotional tactic of norm activation [84, 113, 115], which exploited the target's internal drive to uphold their moral identity as a "good person," overriding skepticism and compelling the target to complete the transaction. Various transaction tactics were then used to defraud the target; commonly in our dataset, the scammer directed targets towards using a peer-to-peer (P2P) payment platform[9] or making payments off-platform, effectively stripping away consumer protection and safety features of the original marketplace. In Seller and Accidental Payment scams, scammers often exploited a target's misunderstanding of complex financial systems and how funds might be processed or rescinded. Targets mentioned how funds from a payment appeared legitimately accessible in their accounts (which can occur when a scammer uses a stolen account or credit card to make the transaction). However, the scammer would request a "refund" (often via a different platform), after which the original transaction would be reversed (e.g., by an anti-fraud system).

Even if a target was suspicious of a scammer's request, they expressed a general concern they might be harming another person or that they could be someone's last line of support. To navigate this uncertainty, some targets reached out to their bank's fraud department or payment platforms for guidance. A few filed complaints with government agencies (e.g., the Internet Crime Complaint Center), seeking formal support. However, targets reported getting mixed guidance. For example, law enforcement and platforms instructed some targets to "work it out with the person," ignoring the risk of a scam.

*4.1.3 Trust.* Trust-based scams exploited a target's existing trust, such as in a reputed business entity or public figure (Authoritative Entity scams); by establishing trust through forming a new romantic relationship with the target (Romance scams); or by leveraging an existing relationship with the target (Personal Relation scam):

> *"My [mother-in-law] was trying to return something she bought online, and instead of signing into her account she looked up [retail company's] phone number and called it. Somehow the scammer got her to send $11,000 and her social security number. I just don't get how she could do this. I'm angry but I also feel so sorry for her. She cried when I told her she wouldn't get her money back and that really broke my heart."* (Authoritative Entity scam)

> *"My mentally unwell uncle has been scammed out of his life savings by someone pretending to be a celebrity. It's been going on for over two years and he has literally nothing left. The scammer kept promising things like if he just gives another ten grand they can fly together on his private jet."* (Romance scam)

Many of the posters seeking help for Trust scams were family members of the target, in part due to the target's unwillingness to reconcile that their trust was being abused. Attempts to intervene often caused relational harm:

> *"We've all tried to tell them that it's a scam and that it's fake but they won't believe any of us because their feelings are so strong."* (Romance scam)

[9] P2P payment apps are digital platforms that allow users to send and receive money directly to/from one another. Examples include Zelle, PayPal, Venmo, and Cash App.

> *"When my sister brought it up, my aunt got angry and refused to talk to her for days."* (Romance scam)

Sometimes scammers were (or appeared to be) a personal relation of the target and abused this access to drain the target financially:[10]

> *"My dad is being financially abused by multiple other family members. They control all his money and he is not even allowed his own bank account. I'm just trying to help him get out of there."* (Personal Relation scam)

> *"I got a request from my brother to send him $35 on [Payment App] and then he would send me the same amount of money on [Different Payment App]. Is this a scam? I don't really get it."* (Personal Relation scam)

Trust-based scams sometimes achieved high severity and long duration by constructing a deceptive relational or institutional bond that superseded the target's critical judgment. Scammers' primary tactic was impersonation, used to create a relationship of perceived credibility that drove targets to rationalize escalating financial demands. In Romance scams, the impersonation of a romantic interest appeared to exploit a deep-seated desire for companionship, causing targets to reject warnings from family members who attempted to intervene. In Authoritative Entity and Personal Relation scams, the scammer leveraged existing high-value trust—whether in an organization, public figure, family member, or friend—to circumvent skepticism and gain access to funds.

*4.1.4 Hope.* Hope-based scams presented targets with financial opportunities in the form of rapid investment gains,[11] employment, prizes, or goods in online marketplaces:

> *"This [Messaging App] group that I joined had over 10k members and we were all earning huge money using this crypto wallet. When I tried to take my funds out they said I had to deposit some small percentage before taking money out for the first time. I paid it, like an idiot, but then I still couldn't withdraw anything and they said I needed to deposit more due to some technical complication with my wallet."* (Investment & Crypto Culture scam)

> *"I'm new to the freelance life so I don't know much yet. I created an account on [Gig Work App], where I was contacted by a company. I communicated with them and ended up doing a transcription project for them. When I finished they told me I needed to pay $150 in tax before getting the $1600 for the job. Is this how it works or should I be worried?"* (Employment scam)

> *"I got a phone call saying the lottery chose random phone numbers and I won millions of dollars and a new car. I don't know if it's legit but – does this ever happen?"* (Prize & Grant scam)

Even if targets were skeptical, the potential financial upsides made them consider engaging:

> *"This person offered to help me pay off some medical bills. They said they'd transfer $1200 but the transaction would cost $30 so they'd need me to send them that upfront. This seems like a clear scam but I'm new to this and want to know for sure."* (Prize & Grant scam)

These scams appeared to leverage the cognitive bias to prioritize a desired outcome—a job, an investment, or a prize—over objective risk assessment, causing targets to rationalize red flags. Exploiting Hope, scammers used the primary tactic of offering something of value to lure targets. Often adding urgency as a secondary tactic, the scammer created a high-stakes, time-sensitive environment that drove the target to complete the scam transaction through a technical action like sending money through a P2P payment app [35, 113]. Scammers also convinced targets to accept the seemingly rational logic of paying a smaller upfront fee or withdrawal tax to receive a much larger promised reward [60, 113], or set up fraudulent employment schemes where targets might unwittingly become money mules.[12]

*4.1.5 Belonging.* Belonging was an emotional motivation which drove people to both engage with scammers and with other potential targets in their communities. People were drawn to scams by the need to Belong through personal companionship (especially common in Romance scams) and community membership (especially common in Investment & Crypto Culture and Charity scams):

> *"My dad knew this much younger woman was probably scamming him the whole time. But even the small chance that the relationship was real kept him going – he's just so lonely and keen to be with someone."* (Romance scam)

> *"A close friend is recently widowed from her (abusive) partner and seeking some purpose in her life. She joined a religious group that she's donating a lot of money to, and is also sending money to a group claiming that she's sponsoring a poor family overseas."* (Charity scam)

Uniquely, Crypto Culture targets often expressed low shame, as being scammed was a learning experience or rite of passage within the risk-tolerant community [29, 77, 97]. The act of (nonchalantly) sharing their experience to warn community members appeared to serve as a therapeutic function, supporting their need for Belonging:

> *"The scammers are probably laughing at me, and that's fine, I messed up and I'm laughing at myself too. This post is to remind y'all (and me) that it's crazy out there."* (Crypto Culture scam)

These scams appeared to manipulate an emotional need for connection, which informational anti-scam advice alone might not resolve. For certain cryptocurrency investment groups, the aforementioned community norm of accepting risk might have contributed to people prioritizing social validation within the group over personal security [29, 77, 97]. In Romance scams, the desire for connection and purpose could be so strong that targets who had been defrauded continued to engage with scammers despite warnings from social relations. For some targets, the emotional utility of belonging to a community or being loved outweighed the financial

[10] Some Personal Relation scams in our dataset described economic abuse, which is documented in literature on domestic and intimate partner abuse as one of many tactics abusers use to control survivors [103].

[11] While Trust scams may also present investment opportunities, their hook stemmed foremost from their trusted relationship with the target.

[12] According to [51], "A money mule is someone who transfers or moves illegally acquired money on behalf of someone else."

trauma of being scammed, leaving the target susceptible to the next risky shared investment or relationship. The underlying emotional need to Belong could remain unresolved even after being scammed, leaving targets susceptible to repeat abuse. Scammers seemed to take advantage of the target's desire to Belong through tactics focused on in-group signaling [29, 124] and love-bombing [40].

Across scam types, posters also informed others about particular scams or scammers, demonstrating a desire for Belonging through their concern for other community members. Many of these posts signaled Belonging to the community, using language and reflecting social norms common to that group. For example, this poster signaled their Belonging to the community of "animal lovers" in a post informing others about a particular scammer:

> *"Please stay alert and don't support any campaigns run by these horrible thieves. They're actively stealing from animal lovers and the actual charities are suffering as a result."* (Charity Scam)

## 4.2 Help-Seeking Needs Throughout Scams

Posters sought different kinds of help depending on *when* during the scam they turned to Reddit. We describe posters' experiences in two dimensions: their emotional state at different points throughout the scam, and the specific types of help they sought in each state.

We use the states from the User States Framework[13] [87] to map emotions and help needs to scam stages. This theoretical framework outlines people's likely emotions and needs before, during, and after technology-facilitated attacks. We expanded the framework and mapped these user states to scam stages that we identified as part of this analysis, as described in this section and depicted in Table 2.

We identified four cross-cutting help needs throughout these user states: Sensemaking (when the poster wanted to understand something), Guidance (when the poster wanted to know what actions to do next), Therapeutic (when the poster wanted emotional support or expression), and External Action (when the poster asked others to take an action, such as reporting a scammer). We present the intersection of user states and help needs below (see also Table 2). Table 3 summarizes our findings on common help needs throughout scams, indicating the user states when people especially needed certain types of help.

*4.2.1 Prevention Before (and After) the Scam.* The Prevention state involved protective actions in the period of time *before* a person encountered a scam. Prevention posts represented 19% of the posts in our dataset. The vast majority of these posters warned others about a scam or scammer to help others avoid the scam before they encountered it, limit the damage scammers could cause, and/or signal Belonging to their community (e.g., communities like a scam awareness group, crypto investors, online sellers/artists, etc.)—all Therapeutic purposes. For posters who did not indicate they had experienced the scam themselves, these posts seemed largely intended to *help others*[14] prevent being scammed. For example:

> *"Basically there's this content creator and I've seen a ton of people sympathizing with him but I just need to warn everyone about this guy. [Describes scammer tactics.] I know it's a lot but it just felt important to share this to protect people. Stay safe out there!"* (Charity scam)

Posters signaling Belonging to and concern for their community was also common, with phrases like *"Be safe, stay alert folks," "I hope sharing our experiences helps to protect others,"* and *"Y'all should be paid for your hard work and beautiful art."* Prevention with similar sentiments was also common *after* scam encounters, as a part of Recovery (covered in Section 4.2.4).

*4.2.2 During the Scam Active Event.* The vast majority of posters in our dataset requested help during an Active Event (72% of posts), starting immediately after they became suspicious or aware of an active scam and extending through the time they were trying to stop or limit initial harm, often expressing emotions of worry or distress.[15] We propose and describe three new substates below—Diagnostics, Mitigation, and Denial—to capture the nuanced help needs and emotions people expressed during an Active Event.

*Diagnostics: Considering whether to engage.* People in the Diagnostics substate were considering engaging with a scam based on the scammer's *hook* [113] or manipulative tactics intended to draw them in (such as a scary threat or enticing prize), but had yet to do so or experience significant negative consequences. They were often in the process of identifying dubious behavior as a scam, expressing emotions of confusion and suspicion, but the emotional motivations luring them to the scam could be strong enough that they would consider engaging despite their suspicions.

Sensemaking was the most common type of help people sought during Diagnostics, especially requests for help *identifying* whether something was a scam. In this example, the poster paused to consider a potential Employment scam, communicating the tension between their suspicions and hope of easing their financial need:

> *"Is this for sure a scam? I am desperate for work so I can't afford to miss out on an actual job opportunity, but I have that bad feeling in my stomach."* (Employment scam, Hope)

Posters also asked for *explanations* of particular tactics, trying to make sense of an unknown scenario before engaging (e.g., asking how it might be harmful to send a buyer a refund). They also commonly wanted to know if others had *experience* with the (yet to be confirmed) scam, seeming to use that experience as a proxy for understanding what might happen to them. When seeking Guidance in the Diagnostic substate, posters commonly asked *whether to engage* with the (yet to be confirmed) scam, communicating their hesitation and thought process. For example, this poster asked for

[13]The states in the User States Framework are **Prevention** (when a person wants to minimize their exposure to future tech-facilitated attacks; they're likely to feel low or typical stress, unless they feel threatened), **Monitoring** (when a person wants to watch for signs of attacks; they're likely to feel low or typical stress, unless they feel threatened), **Active Event** (when a person wants to stop or otherwise respond to an attack(s); they're likely to feel high stress to panic), and **Recovery** (when a person wants to fix damage from the attack(s), determine what happened, and cope with trauma; they're likely to feel moderate to high stress) [87].

[14]We use italics to highlight help-need theme identifiers that are listed in Table 3.

[15]The definition of Active Event in Matthews et al. includes that "users in this state are probably experiencing much higher than their normal amount of stress, even to the point of panic" [87]. While we could not directly assess stress, we considered expressions of emotion or distress during an event, together with other contextual clues in poster reports, when assessing the Active Event state.

| | **Scam Stage:** | Before | Hook | Some Harm | Ongoing Harm | | After | *Total posts* |
|---|---|---|---|---|---|---|---|---|
| | **User State:** | Prevention | Active Event | | | Monitoring | Recovery | |
| | | | Diagnostics | Mitigation | Denial | | | |
| **Help-Seeking Type** | Sensemaking | 12 | 71 | 136 | 13 | 7 | 23 | 251 |
| | Guidance | 9 | 13 | 80 | 24 | 15 | 17 | 136 |
| | Therapeutic | 65 | 7 | 47 | 8 | 11 | 72 | 149 |
| | External Action | 8 | 1 | 1 | 2 | 4 | 10 | 16 |
| | *Total posts* | 75 | 75 | 186 | 32 | 25 | 90 | 405 |

**Table 2: The number of posts per user state and per help-seeking type, and how they map to scam stages we observed.**

help *whether to engage* (as well as *identifying*) a potential Charity scam, motivated to consider it by a desire to help animals in need:

> *"Are these shelters in [country] a scam? I need advice on what to do, I'm worried that these poor animals are being starved. I don't know whether to help or not."* (Charity scam, Guilt & Goodness)

Posters in Diagnostics had paused to seek help identifying scams before engaging or being harmed—this is a substate in which people would likely be primed to consider scam interventions, especially those that identify and explain scams and address the emotions motivating them to consider it (Hope, Fear, etc.). Such interventions in Diagnostics could be impactful in preventing harm (discussed further in Section 5).

*Mitigation: Stopping further harm.* People in the Mitigation substate had experienced *some harm* and wanted to prevent further harm. At this stage in the scam, they had been partially impacted (e.g., given some money, shared some personal information, or experienced significant emotional harm) and there was potential for more. Emotions spiked in this substate, including worry, fear, or even panic. Help-seeking needs focused on stopping or escaping the scam, understanding its potential impact, avoiding further harm, and soothing painful emotions.

Some targets skipped the Diagnostic substate by quickly being harmed by an exploitative scam tactic—such as scary threats for scams that preyed on their Fear, or fraudulent monetary transactions targets felt obligated to cope with as in Accidental Payment and Seller scams (detailed in Section 4.1). These targets in Mitigation had the same Sensemaking needs as those in the Diagnostic substate—the most common still being requests for help *identifying* scams. For example, a purchase transaction was underway before this poster/seller realized there may be a problem:

> *"I sold something to this guy and he sent me a check. I deposited it a few days ago but now he contacted me saying he had an unexpected issue and wants to return the item for a refund."* (Seller scam, Guilt & Goodness)

Mitigation added new Sensemaking needs, especially for help *judging* the situation (e.g., *"should I be worried?"* or *"am I safe?"*). With such requests, posters sought help from others to subjectively assess their situation. Posters also needed help *predicting* the outcome of scams or related mediating actions. Common examples were posters who wanted to know if they might get their money back or what harm they might still face. For example, a poster asked for predictions about further harm from an Employment scam: *"I gave them a photo, my phone number, and email address. Am I just going to get a bunch of scam messages now?"*

Beyond Sensemaking, posters in Mitigation had a notable need for Therapeutic help when coping with harm experienced—and potentially still pending—from a scam. They commonly expressed their emotions and sought *reassurance* (e.g., *"Can anyone put my mind at ease?"* and *"I can't sleep."*). These needs were often expressed in posts that were emotionally intense—for example, if the poster was scared or had lost a large sum of money.

Posters in Mitigation also commonly sought Guidance on how to exit the scam and mitigate harm. These inquiries asked *how to* take an action (e.g., how to… respond, investigate, report, get my money back, cut ties), *whether to* take an action (e.g., should I… respond, ignore, pay them, report to the platform, call the police, hire a lawyer), and open-ended requests for advice (e.g., what are my options? what else can I do?). For example, this poster experienced an Accidental Payment—a scam type that immediately put people in Mitigation after unexpectedly receiving a fraudulent payment—and asked a mix of *open-ended* and *whether to* questions:

> *"Someone sent me close to $200, they asked me to send it back but I knew it was a scam and didn't respond. I didn't hear from them again but the money is still there a month later. Can I spend the money? Should I contact customer support? I don't know what to do."* (Accidental Payment scam, Guilt & Goodness)

*Denial: Harm continues unchecked.* The Denial substate describes targets who did not acknowledge or believe that they were experiencing a scam, often leading to *ongoing harm*. Denial is a psychological defense mechanism to protect against something that is threatening or emotionally painful [56]. In our dataset, Denial was associated with targets who were motivated by a need for Belonging, especially companionship—many targets in Romance scams were in Denial (51% of Romance scam posts). In these cases, the poster was typically a family member, friend, neighbor, or other relation of the target, who recognized or suspected the target was being scammed.

Posters coping with a target in Denial often expressed a desire to convince the target they were being scammed or otherwise help them, especially by asking for Guidance on *how to* convince them or that was *open-ended*. For example, one poster wanted to convince their mother that she was in a Romance scam, and asked for advice:

> *"My mom is being scammed by someone pretending to be a famous actor. He's taken literally every penny she*

| Help-Need Type | Help-Need Themes | Prominent User States |
|---|---|---|
| Sensemaking<br>*Wanting to understand something* | • Identifying scams *(Is this a scam?)*<br>• Explanations of scams or outcomes *(How do they scam me if I give a refund?)*<br>• Experiences with the scam *(Anyone seen this?)*<br>• Judging the situation *(Am I safe? Is this risky?)*<br>• Predicting the outcome *(What might happen?)* | Active Event>Diagnostics<br>Active Event>Mitigation |
| Guidance<br>*Wanting to know what actions to do next* | • Whether to *(Should I… respond? ignore? pay? report?)*<br>• How to *(How do I… respond? investigate? report? get my money back?)*<br>• Open-ended advice *(What else can I do?)* | Active Event>Mitigation<br>Active Event>Denial |
| Therapeutic<br>*Wanting emotional support or expression* | • Reassurance *(Should I be worried?)*<br>• Commiseration *(Has this happened to anyone else?)*<br>• Venting *(I just needed to share.)*<br>• Help others *(Don't fall for this scam. Stay safe.)* | Prevention<br>Active Event>Mitigation<br>Monitoring<br>Recovery |
| External Action<br>*Wanting help from a third party to perform an action* | • Report a scammer *(Help me report this scammer.)*<br>• Share info about a scammer *(Share this info to protect others.)*<br>• Vigilante behavior *(Let's get back at this scammer.)* | Recovery<br>Monitoring |

**Table 3: Summary of our findings on posters' help needs throughout scams. For each help-need type, we provide an overview of common help-need themes and the prominent user states when posters especially needed certain types of help (though these are not exhaustive).**

> *has. I tried showing her an article about other women falling for the same scam but I can't convince her that this guy isn't for real and I don't have the money to hire a lawyer or detective or anything. I don't know what to do and I'm so scared for her, would be grateful for any advice."* (Romance scam, Trust)

Posters sometimes sought Sensemaking (e.g., asking for *explanations* or *experiences*) or Therapeutic support by *venting*: expressing emotions of frustration, worry, or hopelessness as they told stories of the target being scammed, often over extended timelines:

> *"I just don't know how to support her anymore after a year of this and 500k gone. To anyone here who went through this [romance scam] themselves: what helped you figure out what was happening? "* (Romance scam)

*4.2.3 Monitoring Ongoing Scams.* The Monitoring state (6% of posts) involved watching for signs of scams or scammer behavior, which typically co-occurred with Active Events when a scammer continued to cause harm. Most Monitoring posts were posters watching a target (who was in Denial) being harmed by the same scammer over time, with help needs and emotions overlapping with Denial. For example, to protect their parent who was in Denial for repeated Authoritative Entity scams, one poster reported they *"have to manually block [scammers] every day"*, because if they did not, their parent *"gives his bank details to anyone pretending to be famous or rich or offering him money - all my educational attempts have failed."* Some Monitoring posts overlapped with Prevention to *help others* by informing a community about an active scammer, serving a Therapeutic need for the poster (as presented above for Prevention). Monitoring was involved when the poster had been watching and compiling evidence on the scammer over time.

*4.2.4 Recovery After the Scam.* After doing what they could to mitigate the damage of a scam and stop it, and after signs of emotional distress had calmed, people entered the Recovery state (22% of posts). In Recovery, posters' predominant concerns were to address lingering emotional harm, help others avoid the scam, and understand if anything they had lost was recoverable. They sought Therapeutic help for emotional harms, via *reassurance* (to soothe still-strong emotions), *commiseration* (to know they weren't alone), and *venting* (to share their story and feelings).

As part of Recovery, posters commonly told their story of encountering a scam to *help others* avoid it. Investment and Charity scam posts had a large portion that *helped others*, showing their Belonging in the community of risk-tolerant investors or those who care about a charitable cause. For example:

> *"I can't believe I was thinking about using my platform to help this awful person who is stealing money by using pictures from a real fundraiser for a family whose kid has cancer. I wanted to share to get the real family some money and spread the word about this scammer because they seem to have a lot of followers."* (Charity scam)

Another related form of help seeking was asking for External Action, which posters often did during Recovery. Common External Action requests included asking others to *report* a scammer, *share* information about a scammer, and engage in *vigilante behavior* (confirming results from Oak and Shafiq [94]).

## 4.3 Factors that Elevate Risk

Contextual risk factors are factors known to augment or amplify the chance that someone will experience technology-facilitated attacks or disproportionate harm from such an attack [125]. We identified four related factors—financial insecurity, legal precarity, gig work

& precarious labor, and neurodiversity & mental health—that influenced who experienced scams, their likelihood of experiencing harm at specific scam stages, and the types of help they needed.[16]

*4.3.1 Financial Insecurity.* Previous research has found that people experiencing financial and housing insecurity are vulnerable to scams [119]. In our data, this insecurity led targets to engage with scams, skipping the Diagnostic substate of Active Event out of intense Hope and desperation for a potential job or basic necessity like food and housing, regardless of the perceived risk involved:

> *"Someone from HR reached out and told me to send details to some random email address. It didn't feel right but the money was pretty good and I needed a job so desperately."* (Employment scam, Hope)

> *"My family have been really struggling with money but they found a [social media] page advertising free stuff. I was so excited to help so I entered all our details (email, phone number, birthday, etc.) but it was a scam and now my family is upset."* (Prize & Grant scam, Hope)

This insecurity also increased the impact of financial and emotional harm:

> *"The car he sold me stopped working almost immediately. He knew that money was all I had left, and that I'm homeless and was gonna live in this car. When I called to try to trade the car back for my money he told me his friends would come kill me."* (Buyer scam, Hope)

People who had prior experiences with debt had a hard time distinguishing Phantom Debt scams from potentially legitimate requests, requiring extra layers of verification compared to other potential targets: *"I'm getting calls about some debt that I paid ages ago. Am I being scammed? What if I can't find proof that I paid it back then?"*

Financially insecure targets often struggled to find the requisite time and mental space to diagnose and cope with scams (experiencing the "resource or time constrained" risk factor identified by Warford et al. [125]). Sleeper et al's [119] work highlights several circumstances that directly elevate the risk of harm for financially insecure individuals like those in our study: These individuals were vulnerable to engaging with suspicious low-cost online options (such as low-cost housing scams) out of urgent necessity, even when they suspected the deals were "too good to be true." Further, the need to use personal information actively for essential services (like applying for government benefits) meant they were habituated to providing sensitive data (like their social security number) to websites, which increased their overall risk of scams or phishing. When harm did occur, the impact was disproportionately severe; even small financial losses could affect basic necessities like food or rent, and limited resources made it difficult to recover from issues like identity theft, as they lacked the funds or standing with financial institutions to repair damaged credit.

*4.3.2 Legal Precarity.* Legal precarity—either due to immigration status, previous incarceration, or court judgments—also affected how people navigated scams, and could amplify Fear manipulated by some scammers. Prior work has suggested that migrant communities may be more vulnerable to scams, in part due to language barriers and regularly having to share sensitive personal information with authorities [117]. This was reflected in our data:

> *"My elderly parents got a letter saying they owe thousands from some medical procedures my dad got years ago. They don't speak English well enough to understand the letter or contest it themselves, but my mom thinks it's something to do with their insurance and my dad wants to just not pay. My reaction was to tell them to request a letter with the alleged charges rather than sending any money over the phone."* (Phantom Debt scam, Fear)

Similar to financial insecurity, prior legal charges made it difficult to distinguish scams from potentially legitimate judgments. Formerly incarcerated individuals faced significant employment barriers, increasing their financial insecurity, and risked experiencing elevated harm if they unknowingly participated in illegal activities like money muling. Many hesitated to seek formal help and were quicker to respond to scammers out of fear:

> *"I'm trying to help someone who is struggling to deal with fines from court charges that they thought they settled over a decade ago. They got a letter that looks like a legal summons but it said just their name and the state - there was no listed judge and it didn't say what the summons was for. This person responded right away by calling the number on the letter and money was taken out of their bank account days later. I need help finding information and figuring out the laws here."* (Phantom Debt scam, Fear)

Scammers impersonating legal organizations manipulated the perceived power differential between government entities and formerly incarcerated individuals to scare targets into engaging with scams. Language barriers also affected targets' ability to diagnose scams and contest scammer-inflicted issues. These barriers and risks have also been observed for undocumented immigrants [65], illustrating how "legal or political" risk factors like immigration status and "underserved accessibility needs" like language barriers can affect scam susceptibility and impacts [125].

*4.3.3 Gig Work and Precarious Labor.* Gig workers[17] face precarious labor conditions, including lack of legal protection and uncertain access to regular income [9, 81]. People applying for minimum wage jobs are more likely to be targeted by scams [117]. In our data, posters seeking general or informal labor found scams hard to distinguish from legitimate opportunities, increasing their risk of engaging with the scam. Those who primarily relied upon online sales for income risked experiencing more harm from scammers (in comparison to someone selling a one-off product online for supplementary income). Artists and sex workers who created online content were targeted due to their reliance on public-facing digital

[16] Our description of risk factors is by no means exhaustive; we aim to illustrate why contextual risk factors should be considered as part of designing effective interventions.

[17] Gig workers are workers who perform "task-based work conducted outside of a formal employment relationship, often paid per task and to various degrees governed by digital platforms" [81, 131].

platforms and because the precarious nature of their labor made institutional legal or financial recourse riskier:

> *"I'm just starting out as an adult content creator, and using social media to get followers. I'm really behind on bills. I get a lot of messages about being paid 3k a month if I just pay them a fee first. These are a scam, right?"* (Employment scam)

When scams made these targets lose trust in online platforms, it impacted their ability to find new jobs [106] or engage in online marketplaces and communities:

> *"After losing money because of a guy and now being harassed by him, I'm afraid to take custom requests because it could be him again, or some other scammer, and I don't want to put in all that work and money for nothing."* (Seller scam)

These online content creators were "prominently" visible to scammers and therefore susceptible to being targeted [125]. Sex workers encountered platform-enforced and legal barriers to safe employment practices [9]. Many precarious labor workers across employment types expressed being "resource or time constrained" [125], which meant scams could profoundly harm their ability to earn income [125].

*4.3.4 Neurodiversity and Mental Health.* Neurodiversity and mental health conditions affected how people reacted to scams and assessed risk. Targets who reported related conditions generally expressed intensified emotional harms (especially from scams that preyed on Fear or in a Mitigation state during an Active Event) and needed more Therapeutic support, even if they knew they were likely safe:

> *"I almost fell for the scam and I'm so scared that all my devices have viruses. I'm having panic attacks and my OCD means these thoughts won't leave my head even though I know they're irrational. Please don't say anything scary here since I'll just freak out more."* (Employment scam)

Some such targets expressed that they impulsively engaged with scams before thinking through the potential consequences:

> *"After looking at the posts and comments here I decided to send some messages to the scammer to mess with them a bit, but now I'm worried they might be able to find me. I have ADHD so can be a little reckless, I also have quite severe anxiety. Would appreciate any help."* (Cartel scam)

Prior traumatic experiences also exacerbated the harm targets experienced:

> *"The scammer has my address and sent me some really upsetting photos but also a video. I didn't see any other posts here mention a video so are you sure this is a scam? I have trauma from some stuff I saw as a kid so the photos that the scammer sent were really triggering, literally shaking right now."* (Cartel scam)

Mental health struggles stemming from abuse and isolation sometimes led targets to engage with scams:

> *"My abusive husband of 30 years died and I was in a horrible place and all alone. I needed a car so I found someone at a dealership to sell me one. He took advantage of my situation and stole tens of thousands of dollars from me for "investments." He lost his job at the dealership and vanished."* (Romance scam)

Such posters expressed both elevated anxiety about scammers attacking them and fears that they could not confidently protect themselves or recover from a scam's emotional effects, demonstrating "underserved accessibility needs" [125] which could increase their risk of experiencing harm.

## 5 Discussion

In this section, we discuss cross-cutting themes from our study and how our findings could inform the design of interventions that use the *right message*, at the *right time*, to address the *right need* for people targeted by scams—building on Intille's [78] concept of "just-in-time" messaging. Scam interventions are likely to be more effective when they deliver needed information using emotionally-sensitive messaging at key moments. For example, an intervention could diffuse the emotions scammers are attempting to manipulate (i.e., the *right message*), explaining a relevant common scammer tactic to give the person diagnostic support (i.e., the *right need*). The intervention could display this warning when a person encounters a potential scam online (such as a job seeking site or on social media) (i.e., the *right time*). We propose potential support strategies and indicate when and what kinds of interventions might be particularly useful.

### 5.1 Right Message: Emotional Motivations

Since emotions influence how information is received and processed [83, 132], we argue that scam interventions may be more effective if they deliver emotionally-sensitive responses to address the emotional components driving engagement. We identified five emotional motivations that scammers manipulated to hook and engage targets: Fear, Guilt & Goodness, Trust, Hope, and Belonging. Messaging in scam interventions should consider these emotional motivations when attempting to convince targets to avoid or stop engaging the scammer. Without addressing the underlying needs driving people's engagement with scams, interventions—particularly those focused on scam literacy, education, and other informational messaging—may not be effective. In particular, Belonging was a strong motivator for scam types in our data that involved Denial and extensive ongoing harm. It is unlikely that people motivated by Belonging would be responsive to primarily informational messaging, as we found with targets of Romance scams. Investment & Crypto Culture scam targets appeared to be partially driven by a desire to socially belong in a community that valued risk-taking and amused indifference to large losses [29, 77, 97], also suggesting that primarily informational messaging may not be effective.

Our findings support prior work on misinformation susceptibility that argues for addressing people's underlying motivations for engagement, which are often emotional and social [100]. This prior work finds that both youth [70] and adults [70, 82, 110] share misinformation to meet social and emotional needs. Like the scammers

in our research, misinformation creators explicitly target social and emotional needs to motivate people to engage [71]. Prior research has found that people also assess information and make credibility judgments together as members of communities [63, 70].

## 5.2 Right Time & Need: Help Seeking for Scams

Our findings detail people's help-seeking needs at key moments before, during, and after scams. Below, we suggest how these findings can be used to tailor interventions to help needs at different scam stages.

*Before a scam.* Posts related to the Prevention state demonstrated Reddit community members' interest in intervening to help others avoid scams and the important Therapeutic needs of Belonging and altruism this type of sharing supported. This community of helpers could be supported by their inclusion in scam prevention interventions (e.g., through reporting suspected scams to others or platforms).

*Hook.* Targets considering a scammer's emotionally manipulative hook in the Diagnostics substate (during an Active Event) needed help identifying and avoiding harm from the scam. In this critical pre-harm window, targets needed help to address the emotions motivating them to engage (e.g., Hope, Fear, etc.) and contextually-specific Sensemaking support to explain the scam mechanics.

*Some harm.* During a scam and after experiencing some harm in the Mitigation substate of Active Event, targets needed Sensemaking help to understand what was happening to them, Guidance on preventing further harm, and Therapeutic support to cope with escalated emotions like worry and fear.

*Ongoing harm.* Targets in the Denial substate of Active Event often experienced ongoing harm from scams and were not receptive to help. Family and relations described Monitoring these ongoing scams while feeling frustrated, worried, or hopeless, and expressed a need for Guidance on how to help the target mitigate harm and move toward Recovery; such help could be vital in stopping the severe harm often involved in these cases of repeated financial exploitation by scammers.

*After escaping a scam.* Posters in the Recovery state primarily needed Therapeutic support to cope with the emotional impact of the scam and to connect with others (such as by reporting the scam to help others avoid being hooked).

As outlined above, the three new Active Event substates we introduced for scams—Diagnostics, Mitigation, and Denial—enabled us to provide more granular break-down of a target's needs and emotions at key moments when they were facing an active scam.

## 5.3 Potential Interventions

Here, we bring together these findings to propose potential interventions that address the right need, at the right time, with the right message for scam targets.[18] We acknowledge that while our dataset captures a global user base, the predominance of English-language posts means that the help-seeking behaviors observed could reflect Anglophone cultural norms (e.g., specific expectations of institutional utility). Consequently, the interventions proposed below should not be viewed as universal solutions, but rather as strategies to be adapted to local sociocultural contexts (particularly regarding institutional trust, shame/stigma, and community support). We discuss these adaptations further in Section 5.4.

*Fear Interventions.* Fear-based scams often involved scary threats and were largely reported in our dataset as being carried out in direct messaging. Interventions could focus on mitigating fear with emotional reassurance and informing targets of red flags that suggest what they are experiencing could be (or even likely is) a scam that poses no real physical or financial danger. This sensemaking support could help demystify the threat and empower targets to disengage. Interventions could also give people clear guidance on how to verify potential scammer claims, like how to certify debt collection notices. Such interventions are likely most beneficial in the Diagnostics and Mitigation substates, when targets are actively receiving threats likely to elevate their distress.

*Guilt & Goodness Interventions.* For scams that manipulate a target's sense of Guilt & Goodness, interventions could help targets identify how scammers manipulate their desire to help others, explaining the emotional and technical tactics as they are encountering them. For example, within messaging platforms, especially those on P2P marketplace sites and apps, an intervention could detect conversational red flags,[19] such as a someone using emotionally manipulative language to compel an off-platform "refund," a common tactic in Seller scams. A just-in-time alert could intervene to discourage the platform switch, focusing on immediate information to explain how the scammer's tactic works both emotionally and technically. Such guidance may be most effective in the Diagnostic state, as people attempt to determine a solicitation's authenticity.

*Hope Interventions.* Targets of hope-based scam types could be dealing with financial insecurity, unemployment, and inexperience. Interventions could provide guidance sensitive to these vulnerabilities without discouraging legitimate opportunities. In the Diagnostic state, for example, just-in-time warnings about requests for upfront fees or personal data on job-seeking platforms could help prevent job-seekers from engaging with Employment scams. Many job-seeking posters in our study expressed both suspicion and hope (or even desperation) when asking about potential employers, suggesting that interventions could confirm red flags in job postings and support people in seeking further information to verify the legitimacy of the organization. Adaptations may be necessary for contexts where and people for whom the reliability of formal institutions (e.g., law enforcement, government agencies, banks) is low [67, 134]. In such circumstances, interventions might be more effective if they encourage sensemaking and verification through community-based organizations rather than institutional authorities.

[18] Please note that the design of effective digital-safety interventions is very challenging to get "right" in practice—something prior work has argued is a wicked problem [87]. Determining how to design scam interventions in privacy preserving, safe, and ethical ways that are effective on different platforms and for people world-wide, is an area for future work involving multi-disciplinary experts and communities. Our work can help inform starting points for evidence-based intervention explorations, but the ideas presented here should not be considered prescriptive or comprehensive.

[19] The privacy implications of such detection would need to be carefully considered.

In our data, most targets of these scam types reached Mitigation or Recovery, which suggests the value of interventions at these stages in places where targets seek help. This could include guidance on what to do if the target has already shared personal information with the scammer (in the Mitigation state), or support for navigating the legal or financial consequences of unwittingly participating in illegal activities (e.g., as a money mule) in the Recovery state.

*Trust Interventions.* For scams that rely on impersonation tactics, like Authoritative Entity scams, encouraging the target to pause and guiding them in verifying the identity of the scammer is critical. An emotionally-sensitive just-in-time intervention could specifically target the moment a scammer is attempting to exploit a user's faith in an organization or person. Many banking platforms have versions of these just-in-time messages, intervening at the moment of transfer. P2P platforms, which posters commonly mentioned scammers manipulating, could potentially benefit from similar messaging. In lieu of the platform itself implementing such messaging, a browser or app (with user consent) could provide this Diagnostic support.

While Romance scams are among the most widely researched in the HCI literature [5, 27, 39, 128] and targets engaging with them are deeply emotionally motivated [40], our research suggests they may be the least amenable to just-in-time interventions. The Denial state prevalent in Romance scams presents a unique challenge, as the targets themselves were largely not receptive to interventions and may have been socially isolated by scammers, making it important to direct Guidance and Therapeutic support towards their concerned family and friends. Our data indicated that targets of these scams had sometimes experienced repeat victimization, which might be because the underlying emotional motivations that initially led to engagement may have remained unresolved.

*Belonging Interventions.* While technical and educational interventions may help mitigate immediate financial harm, longer-term recovery from emotional harm often requires Therapeutic support. As discussed, while an emotionally-motivated desire for Belonging made some scams—like Romance, Investment & Crypto Culture, and Charity scams—seem more compelling to targets, the emotional need for community connection also appeared to motivate targets recovering from scams to offer Therapeutic support to others across scam types. This expression of Belonging in the form of help-giving served an important Therapeutic function for targets seeking Recovery, while providing educational help to those in Prevention.

Previous research [17, 94] already demonstrates the importance of online communities like Reddit in providing peer-to-peer therapeutic support and reassurance for targets. Platforms could contribute to this ecosystem by improving formal scam reporting mechanisms (a form of External Action). Enhancing these systems could potentially allow people, as part of their Recovery process, to anonymously tell their story through a publicly visible, scam-specific platform reporting function—a Therapeutic help-giving activity that could both aid their recovery and help warn others. Other research has found that people learn behavior-impacting lessons from digital security stories told by others, especially those which elicit an emotional response [104], suggesting that helping people tell their scam stories to others may serve a valuable preventative function. In sociocultural contexts where financial loss carries especially deep stigma or shame [50], interventions may need to prioritize anonymous, private, or one-way support channels rather than public forum participation.

## 5.4 Future Work

We propose that future work could investigate how our findings might apply to other types of scams not covered in our study, such as gambling scams, or beyond scams to other types of technology-facilitated attacks. We also discuss below how our work could inform future studies on automatic detection, user research, and the effects of sociocultural variation on help-seeking norms and interventions.

*Automatic detection and user research.* Automatic detection of potential scams could improve the timing and customization of just-in-time messages. Future work could examine whether our characterizations of scams by emotional motivations and user states could help inform such automatic scam detection. Any scam detection efforts would need to carefully account for user privacy and safety. In lieu of detection, designers could focus intervention efforts on functions that scammers misuse to manipulate targets, such as P2P sales, P2P payments, direct messaging, and more.

Translating this study's findings to the design of effective digital-safety interventions in practice will require extensive outreach efforts and rigorous applied research, as noted above. For example, researchers experimented for more than four years on just-in-time messaging and visual design for malware, phishing, and SSL warnings in Chrome to improve effectiveness [3, 4, 52–54, 109]. As a baseline, future work could compare and test user reactions to emotionally-sensitive anti-scam messaging versus purely informational ones to maximize protective efficacy across different scam stages. Likewise, future work is needed to iteratively design and evaluate just-in-time scam messaging to establish and improve effectiveness on specific platforms.

*Sociocultural variation.* Our findings and their implications for interventions are likely affected by sociocultural help-seeking norms, suggesting areas for future work to understand help seeking for scams in different geographies. For example, online help-seeking models based on data from the United States and the Philippines failed to generalize to students in Costa Rica, who engaged in significantly more offline, collaborative help seeking [96]. A study with Chinese first-generation college students found they preferred "one-way" rather than "interactive" online help seeking [50]. Another study with ethnic minority first-generation college students found they underutilized support services due to fear of relational damage [31]. These differences may affect online help seeking in ways that require further study. Some findings may generalize across contexts: anonymous support, for example, has been shown to reduce stigma and foster candid peer support in multiple cultural contexts [101, 102, 133].

The therapeutic value of public processing of trauma online likely varies based on cultural context, as evidenced by a study comparing Chinese Australian and European Australian trauma survivors [79] which found that cultural beliefs were associated with different

PTSD symptom outcomes. This suggests that a trauma-informed approach [49] to scam story sharing [104] requires "cultural humility" [105], as it is essential to first understand how potential recipients "understand and prefer to communicate about traumatic stress and the process of healing" [58].

Scam experiences and help-seeking behaviors are also influenced by socioculturally-mediated trust in institutions [67]. For many communities, institutions like law enforcement and banks have not historically been trustworthy [134]. Many Trust scams preyed on targets' trust in institutions, and falling prey to such scams decreased that institutional trust for some targets. Fear scams also preyed on targets who had prior negative experiences with institutions, like debt, incarceration, or legal issues. Such interactions between at-risk user status [87] and institutional trust [67] as they relate to scam susceptibility and help-seeking behavior merit further study, particularly toward improved intervention support.

## 6 Conclusion

This research, grounded in a user-centered analysis of posts on Reddit that sought help for scams, details how emotional motivations and scammer tactics interact to shape a target's susceptibility. We mapped help-seeking timelines and needs as scams unfold, highlighting when and why people reach out for support. We detailed implications for intervention design, including guidance on how user experience insights can inform timely, effective and empathetic scam prevention strategies.

Our findings indicate that scammers adeptly leverage targets' emotional motivations (including Fear, Hope, Guilt & Goodness, Trust, and Belonging), using both emotional and technical tactics. Targets predominantly seek help during the "Active Event" state—when they are actively trying to stop or mitigate immediate harm—though "Recovery" is also a significant phase for seeking support. The three new Active Event substates we introduced for scams—Diagnostics, Mitigation, and Denial—elucidate targets' different needs at key moments during an active scam. These help-seeking needs include Sensemaking (to understand the situation), Guidance (for next steps), Therapeutic (for emotional support), and External Action (for third-party intervention), underscoring the need for tailored support.

Notably, emotions were an important factor in scams—as motivators for engaging scams, part of the harm experienced, and dictating the help needed. Our findings further demonstrate that factors such as financial insecurity, legal precarity, platform dependent labor, neurodiversity, or mental health issues can heighten a target's risk and lead to more severe harms. These insights could inform the design of contextually sensitive interventions that move beyond technical scam detection, providing holistic support that addresses the real-life sensemaking, guidance, therapeutic, and external action needs of scam targets at specific critical stages of scams.

## Acknowledgments

We would like to extend a very big thank you to the many people who have supported this work, including Amanda Walker, Bryant Gipson, Luca Invernizzi, reviewers of this paper, and more.

## References

[1] AARP. 2025. Understanding Scams and Fraud. https://seniorplanet.org/scam-prevention/. Accessed August 26, 2025.

[2] Ron Acierno, Jordan Watkins, Melba A Hernandez-Tejada, Wendy Muzzy, Gabrielle Frook, Mara Steedley, and Georgia Anetzberger. 2019. Mental health correlates of financial mistreatment in the National Elder Mistreatment Study Wave II. *Journal of Aging and Health* 31, 7 (2019), 1196–1211.

[3] Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Proceedings of the 22nd USENIX Security Symposium*. USENIX Association, 257–272. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe

[4] Hazim Almuhimedi, Adrienne Porter Felt, Robert W. Reeder, and Sunny Consolvo. 2014. Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning. In *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS 2014)*. USENIX Association, 113–128. https://www.usenix.org/conference/soups2014/proceedings/presentation/almuhimedi

[5] Sima Amirkhani, Fatemeh Alizadeh, Dave Randall, and Gunnar Stevens. 2024. Beyond Dollars: Unveiling the Deeper Layers of Online Romance Scams Introducing "Body Scam". In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3613905.3651004

[6] Keith B. Anderson. 2021. To Whom Do Victims of Mass-Market Consumer Fraud Complain? https://papers.ssrn.com/abstract=3852323. https://doi.org/10.2139/ssrn.3852323 social science research network:3852323

[7] Dan Ariely and Dan Zakay. 2001. A Timely Account of the Role of Duration in Decision Making. *Acta Psychologica* 108, 2 (2001), 187–207. https://doi.org/10.1016/S0001-6918(01)00034-8

[8] Vimala Balakrishnan, Umayma Ahhmed, and Faris Basheer. 2025. Personal, Environmental and Behavioral Predictors Associated with Online Fraud Victimization among Adults. *PLOS ONE* 20, 1 (Jan. 2025), e0317232. https://doi.org/10.1371/journal.pone.0317232

[9] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. 2021. "Disadvantaged in the American-dominated Internet": Sex, Work, and Technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 563, 16 pages. https://doi.org/10.1145/3411764.3445378

[10] Michaela Beals, Marguerite DeLiema, and Martha Deevy. 2015. Framework for a Taxonomy of Fraud. *Financial Fraud Research Center* (2015).

[11] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil" Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–27.

[12] Bernama. 2024. Four Individuals, Including Social Media Influencer Couple, Held For Embezzling Public Donations. https://bernama.com/en/news.php?id=2316594 Accessed February 4, 2026.

[13] Bernama. 2024. Specific Law Needed To Monitor, Regulate Online Donations - Police. https://www.bernama.com/en/news.php?id=2272284 Citing statistics from Bukit Aman Commercial Crime Investigation Department (CCID) director Datuk Seri Ramli Mohamed Yoosuf. Accessed February 4, 2026.

[14] Marzieh Bitaab, Haehyun Cho, Adam Oest, Zhuoer Lyu, Wei Wang, Jorij Abraham, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupé. 2023. Beyond Phish: Toward Detecting Fraudulent e-Commerce Websites at Scale. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 2566–2583. https://doi.org/10.1109/SP46215.2023.10179461

[15] Eric Blancaflor, Harold Kobe S. Billo, John Michael P. Dignadice, and Philip T. Domondon. 2023. A Quantitative Case Study on Rampant Online Ordering Scams in the Philippines. In *Proceedings of the 2023 5th International Conference on Management Science and Industrial Engineering (MSIE '23)*. Association for Computing Machinery, New York, NY, USA, 185–191. https://doi.org/10.1145/3603955.3604029

[16] Elijah Bouma-Sims, Lily Klucinec, Mandy Lanyon, Julie Downs, and Lorrie Faith Cranor. 2025. The Kids Are All Right: Investigating the Susceptibility of Teens and Adults to YouTube Giveaway Scams. In *Proceedings 2025 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/ndss.2025.240342

[17] Elijah Bouma-Sims, Mandy Lanyon, and Lorrie Faith Cranor. 2025. 'Is this a scam?': The Nature and Quality of Reddit Discussion about Scams. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security* (Taipei, Taiwan) *(CCS '25)*. Association for Computing Machinery, New York, NY, USA, 2444–2458. https://doi.org/10.1145/3719027.3765030

[18] R.E. Boyatzis. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development*. SAGE Publications. https://books.google.com/books?id=_rfClWRhIKAC

[19] Virginia Braun and Victoria Clarke. 2022. Conceptual and Design Thinking for Thematic Analysis. *Qualitative psychology* 9, 1 (2022), 3.

[20] Casey Breen, Cormac Herley, and Elissa M. Redmiles. 2022. A Large-Scale Measurement of Cybercrime Against Individuals. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–41. https://doi.org/10.1145/3491102.3517613

[21] Tom Buchanan and Monica T. Whitty. 2013. The Online Dating Romance Scam: Causes and Consequences of Victimhood. *Psychology, Crime & Law* 20, 3 (2013), 261–283. https://doi.org/10.1080/1068316X.2013.772180

[22] Marcus Butavicius, Ronnie Taib, and Simon J. Han. 2022. Why People Keep Falling for Phishing Scams: The Effects of Time Pressure and Deception Cues on the Detection of Phishing Emails. *Computers & Security* 123 (Dec. 2022), 102937. https://doi.org/10.1016/j.cose.2022.102937

[23] Mark Button and Cassandra Cross. 2017. *Cyber Frauds, Scams and Their Victims*. Routledge, London. https://doi.org/10.4324/9781315679877

[24] Mark Button, Chris Lewis, and Jacki Tapley. 2009. *Fraud Typologies and the Victims of Fraud: Literature Review*. National Fraud Authority, London.

[25] Mark Button, Chris Lewis, and Jacki Tapley. 2014. Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families. *Security Journal* 27, 1 (2014), 36–54.

[26] Mark Button, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology* 47, 3 (Dec. 2014), 391–408. https://doi.org/10.1177/0004865814521224

[27] Elisabeth Carter. 2021. Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *The British Journal of Criminology* 61, 2 (Feb. 2021), 283–302. https://doi.org/10.1093/bjc/azaa072

[28] M. Ariel Cascio, Eunlye Lee, Nicole Vaudrin, and Darcy A. Freedman. 2019. A Team-Based Approach to Open Coding: Considerations for Creating Intercoder Consensus. *Field Methods* 31, 2 (2019), 116–130. https://doi.org/10.1177/1525822X19838237

[29] Dan Cassino. 2023. Crypto, Meme Stocks, and Threatened Masculinity. *Contexts* 22, 2 (May 2023), 18–23. https://doi.org/10.1177/15365042231172460

[30] Alyxandra Cazanis, Jao-Yue Carminati, Kimberly Chew, Cassandra Cross, Jennie Ponsford, and Kate Rachel Gould. 2025. "Falling into a Black Hole": A Qualitative Exploration of the Lived Experiences of Cyberscam Victim-Survivors and Their Social Support Networks. *Victims & Offenders* 0, 0 (2025), 1–20. https://doi.org/10.1080/15564886.2025.2481267

[31] Edward S. Chang, Chantal J. Hagerman, Y. Xu, S. J. Schwartz, and J. K. Hirsch. 2020. The complexity of cultural mismatch in higher education: Norms affecting first-generation college students' coping and help-seeking behaviors. *Cultural Diversity and Ethnic Minority Psychology* 26, 3 (2020), 280–294. https://doi.org/10.1037/cdp0000297

[32] Hongliang Chen, Yijin Guo, and Kexin Wang. 2025. Investigating Migrant Workers' Information-Seeking Behaviors on Scams: The Impact of Scam Prevention Communication and Victimization Experiences. *Journalism & Mass Communication Quarterly* 0, 0 (2025), 10776990251336383. https://doi.org/10.1177/10776990251336383

[33] Andrew Childs. 2024. 'I Guess That's the Price of Decentralisation… ': Understanding Scam Victimisation Experiences in an Online Cryptocurrency Community. *International Review of Victimology* 30, 3 (Sept. 2024), 539–555. https://doi.org/10.1177/02697580231215840

[34] Munmun De Choudhury and Sushovan De. 2014. Mental Health Discourse on Reddit: Self-Disclosure, Social Support, and Anonymity. *Proceedings of the International AAAI Conference on Web and Social Media* 8, 1 (May 2014), 71–80. https://doi.org/10.1609/icwsm.v8i1.14526

[35] Robert B. Cialdini. 2008. *Influence*. Pearson.

[36] Anna Coluccia, Andrea Pozza, Fabio Ferretti, Fulvio Carabellese, Alessandra Masti, and Giacomo Gualtieri. 2020. Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review. *Clinical practice and epidemiology in mental health: CP & EMH* 16 (2020), 24–35. https://doi.org/10.2174/1745017902016010024

[37] Anna Coluccia, Andrea Pozza, Fabio Ferretti, Fulvio Carabellese, Alessandra Masti, and Giacomo Gualtieri. 2020. Online romance scams: relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical practice and epidemiology in mental health: CP & EMH* 16 (2020), 24.

[38] Cassandra Cross. 2015. No Laughing Matter: Blaming the Victim of Online Fraud. *International Review of Victimology* 21, 2 (May 2015), 187–204. https://doi.org/10.1177/0269758015571471

[39] Cassandra Cross and Thomas J. and Holt. 2023. More than Money: Examining the Potential Exposure of Romance Fraud Victims to Identity Crime. *Global Crime* 24, 2 (April 2023), 107–121. https://doi.org/10.1080/17440572.2023.2185607

[40] Cassandra Cross, Molly Dragiewicz, and Kelly Richards. 2018. Understanding Romance Fraud: Insights From Domestic Violence Research. *The British Journal of Criminology* 58, 6 (Oct. 2018), 1303–1322. https://doi.org/10.1093/bjc/azy005

[41] Cassandra Cross, Kelly Richards, and Russell Smith. 2016. Improving Responses to Online Fraud Victims: An Examination of Reporting and Support. Final Report for Criminology Research Grant 29/13-14. (2016).

[42] Cassandra Cross, Russell G Smith, and Kelly Richards. 2014. Challenges of responding to online fraud victimisation in Australia. *Trends and Issues in Crime and Criminal Justice* 474 (2014), 1–6.

[43] Marguerite DeLiema, Yiting Li, and Gary Mottola. 2023. Correlates of Responding to and Becoming Victimized by Fraud: Examining Risk Factors by Scam Type. *International Journal of Consumer Studies* 47, 3 (2023), 1042–1059. https://doi.org/10.1111/ijcs.12886

[44] Marguerite Deliema, Doug Shadel, and Karla Pak. 2020. Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *Journal of Consumer Research* 46, 5 (Feb. 2020), 904–914. https://doi.org/10.1093/jcr/ucz020

[45] Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the 2006 CHI Conference on Human Factors in Computing Systems (CHI '06)*. Association for Computing Machinery, New York, NY, USA, 581–590. https://doi.org/10.1145/1124772.1124861

[46] Martina Dove. 2021. *The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable*. Routledge, Abingdon, Oxon ; New York, NY.

[47] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS 2006) (SOUPS '06)*. Association for Computing Machinery, New York, NY, USA, 79–90. https://doi.org/10.1145/1143120.1143131

[48] Alain Tambe Ebot. 2023. Advance Fee Fraud Scammers' Criminal Expertise and Deceptive Strategies: A Qualitative Case Study. *Information and Computer Security* 31, 4 (2023), 478–503. https://doi.org/10.1108/ICS-01-2022-0007

[49] Melissa Eggleston, Emily P Jones, Nashmia Khan, William A Romani, Kyle McQuillan, Jessica Otero, and Elizabeth Chen. 2025. A scoping review of trauma-informed care principles applied in design and technology. *Digital Health* 11 (2025), 20552076251360925. https://doi.org/10.1177/20552076251360925

[50] Yuying Fan and Jacob Oppong Nkansah. 2024. The exploration of online academic help-seeking behavior of first-generation college students in developing countries: evidence from China. *Frontiers in Education* 8 (2024), 1333824. https://doi.org/10.3389/feduc.2023.1333824

[51] Federal Bureau of Investigation. 2025. Money Mules. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules. Accessed November 14, 2025.

[52] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems*. ACM, 2893–2902. https://doi.org/10.1145/2702123.2702442

[53] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Emre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

[54] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at Scale with Google Chrome's SSL Warning. In *Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems*. ACM, 2667–2676. https://doi.org/10.1145/2556288.2557292

[55] J Fereday and E. Muir-Cochrane. 2006. Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods* 5 (2006), 80–92. https://doi.org/10.1177/160940690600500107

[56] Anna Feud. 1937. *The Ego and the Mechanisms of Defence*. Hogarth Press and the Institute of Psycho-Analysis, London.

[57] Peter Fischer, Stephen E. G. Lea, and Kath M. Evans. 2013. Why Do Individuals Respond to Fraudulent Scam Communications and Lose Money? The Psychological Determinants of Scam Compliance. *Journal of Applied Social Psychology* 43, 10 (2013), 2060–2072. https://doi.org/10.1111/jasp.12158

[58] Julian D. Ford, Damion J. Grasso, Jon D. Elhai, and Christine A. Courtois. 2015. Social, Cultural, and Other Diversity Issues in the Traumatic Stress Field. In *Posttraumatic Stress Disorder*. Elsevier, 503–546. https://doi.org/10.1016/B978-0-12-801288-8.00011-X

[59] Jonathan L. Freedman and Scott C. Fraser. 1966. Compliance without Pressure: The Foot-in-the-Door Technique. *Journal of Personality and Social Psychology* 4, 2 (1966), 195–202. https://doi.org/10.1037/h0023552

[60] Jonathan L. Freedman and Scott C. Fraser. 1966. Compliance Without Pressure: The Foot-In-The-Door Technique. *J. Pers. Soc. Psychol.* 4, 2 (1966), 195–202. https://doi.org/10.1037/h0023552

[61] FTC. 2025. New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024. Accessed July 7, 2025.

[62] Future Crime Research Foundation. 2024. *A Deep Dive into Cybercrime Trends in India*. White Paper. Future Crime Research Foundation (FCRF). Analyzes cybercrime data from Jan 2020 to June 2023.

[63] Christine Geeng, Savanna Yee, and Franziska Roesner. 2020. Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate. In *Proceedings*

*of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376784

[64] Kristen Greene, Michelle Steves, Mary Theofanos, and Jennifer Kostick. 2018. User Context: An Explanatory Variable in Phishing Susceptibility. In *Workshop on Usable Security (USEC) 2018*. Internet Society. https://csrc.nist.gov/pubs/conference/2018/02/18/user-context-an-explanatory-variable-in-phishing-s/final

[65] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3173574.3173688

[66] Umit G Gurun, Noah Stoffman, and Scott E Yonker. 2018. Trust Busting: The Effect of Fraud on Investor Behavior. *The Review of Financial Studies* 31, 4 (April 2018), 1341–1376. https://doi.org/10.1093/rfs/hhx058

[67] Markus Hadler et al. 2025. Generalized Trust as a Foundation for Online Trust: Findings From Austria, Greece, Poland, the Philippines, and South Africa. *Frontiers in Sociology* 9 (2025), 1504812. https://doi.org/10.3389/fsoc.2025.1504812

[68] LaToya Hall, Jennifer M Gómez, and Peter A Lichtenberg. 2023. Trust and betrayal in older adult financial exploitation. *Aging & Mental Health* 27, 12 (2023), 2466–2473.

[69] Yaniv Hanoch and Stacey Wood. 2021. The Scams Among Us: Who Falls Prey and Why. *Current Directions in Psychological Science* 30, 3 (June 2021), 260–266. https://doi.org/10.1177/0963721421995489

[70] Amelia Hassoun, Ian Beacock, Sunny Consolvo, Beth Goldberg, Patrick Gage Kelley, and Daniel M. Russell. 2023. Practicing Information Sensibility: How Gen Z Engages with Online Information. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3544548.3581328

[71] Amelia Hassoun, Gabrielle Borenstein, Katy Osborn, Jacob McAuliffe, and Beth Goldberg. 2024. Sowing "Seeds of Doubt": Cottage Industries of Election and Medical Misinformation in Brazil and the United States. *New Media & Society* 0, 0 (2024), 14614448241255379. https://doi.org/10.1177/14614448241255379

[72] LD Herrera. 2025. Romance Scam Victimization: A Survey-Based Examination of Financial, Psychological, and Reporting Factors. In *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*. 1–6. https://doi.org/10.1109/ISDFS65363.2025.11012081

[73] Hirect India. 2022. 56% of Indian Job Seekers Faced Scams During Their Job Hunt: Report. *The Economic Times* (29 Jul 2022). https://hr.economictimes.indiatimes.com/news/workplace-4-0/recruitment/56-of-indian-job-seekers-faced-scams-during-their-job-hunt-report/93199982 Data retrieved from Hirect India Recruitment Survey.

[74] Felipe Hoffa. 2021. The Most Popular Languages on Reddit after Analyzing 1M Comments. https://medium.com/data-science/the-most-popular-languages-on-reddit-analyzed-with-snowflake-and-a-java-udtf-4e58c8ba473c. Accessed February 4, 2026.

[75] Kristy Holtfreter, Michael D. Reisig, and Travis C. Pratt. 2008. Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology* 46, 1 (2008), 189–220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

[76] Mohamed Houtti, Abhishek Roy, Venkata Narsi Reddy Gangula, and Ashley Walker. 2024. A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries. *Journal of Online Trust and Safety* 2, 4 (Sept. 2024). https://doi.org/10.54501/jots.v2i4.204

[77] Gustavo Iamin. 2025. Are Crypto-Investors Overconfident? The Role of Risk Propensity and Demographics. Evidence From Brazil and Portugal. *The Journal of Risk Finance* 26, 1 (2025), 147–173. https://doi.org/10.1108/JRF-04-2024-0109

[78] Stephen S. Intille. 2004. Ubiquitous Computing Technology for Just-In-Time Motivation of Behavior Change. *Studies in Health Technology and Informatics* 107 (2004), 1432–1437. https://pubmed.ncbi.nlm.nih.gov/15361052/

[79] Laura Jobson et al. 2024. Cultural Differences in Appraisals of Control and Posttraumatic Stress Disorder Symptoms. *European Journal of Psychotraumatology* 15, 1 (2024).

[80] Rebecca A. Judges, Sara N. Gallant, Lixia Yang, and Kang Lee. 2017. The Role of Cognition, Personality, and Trust in Fraud Victimization in Older Adults. *Frontiers in Psychology* 8 (2017), 588. https://doi.org/10.3389/fpsyg.2017.00588

[81] Srujana Katta, Fabian Ferrari, Niels van Doorn, and Mark Graham. 2024. Migration, Migrant Work(ERs) and the Gig Economy. *Environment and Planning A: Economy and Space* 56, 4 (2024), 1102–1112. https://doi.org/10.1177/0308518X241250168

[82] Sang Jung Kim and Kaiping Chen. 2024. The use of emotions in conspiracy and debunking videos to engage publics on YouTube. *New Media & Society* 26, 7 (2024), 3854–3875. https://doi.org/10.1177/14614448221105877

[83] Jeff Langenderfer and Terence A. Shimp. 2001. Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology & Marketing* 18, 7 (2001), 763–783. https://doi.org/10.1002/mar.1029

[84] Stephen EG Lea, Peter Fischer, and Kath M Evans. 2009. The Psychology of Scams: Provoking and Committing Errors of Judgement. (2009).

[85] Michael Levi. 2008. Organized Fraud and Organizing Frauds: Unpacking Research on Networks and Organization. *Criminology & Criminal Justice* 8, 4 (Nov. 2008), 389–419. https://doi.org/10.1177/1748895808096470

[86] Ce Lyu, Shenghan Gao, and Qingqi Zhang. 2025. The Impact of Time Pressure and Type of Fraud on Susceptibility to Online Fraud. *Frontiers in Psychology* 16 (April 2025), 1508363. https://doi.org/10.3389/fpsyg.2025.1508363

[87] Tara Matthews, Elie Bursztein, Patrick Gage Kelley, Lea Kissner, Andreas Kramm, Andrew Oplinger, Andreas Schou, Manya Sleeper, Stephan Somogyi, Dalila Szostak, Kurt Thomas, Anna Turner, Jill Palzkill Woelfer, Lawrence L. You, Izzie Zahorian, and Sunny Consolvo. 2025. Supporting the Digital Safety of At-Risk Users: Lessons Learned from 9+ Years of Research and Training. *ACM Trans. Comput.-Hum. Interact.* 32, 3 (June 2025), 22:1–22:39. https://doi.org/10.1145/3716382

[88] Tim McGuinness. 2023. What Really Are Vulnerabilities That Lead To Scams? https://scampsychology.org/wp-content/uploads/2023/07/Vulnerabilities-A-SCARS-Whitepaper-.pdf.

[89] Wesley Meikle and Cassandra Cross. 2024. "What Action Should I Take?": Help-seeking Behaviours of Those Targeted by Romance Fraud. *Journal of Economic Criminology* 3 (2024), 100054.

[90] Stanley Milgram. 1963. Behavioral Study of Obedience. *The Journal of Abnormal and Social Psychology* 67, 4 (1963), 371–378. https://doi.org/10.1037/h0040525

[91] David Modic and Ross Anderson. 2015. It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy (SP)* 13, 5 (Sept. 2015), 99–103. https://doi.org/10.1109/MSP.2015.107

[92] Gareth Norris, Alexandra Brookes, and David Dowell. 2019. The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology* 34, 3 (Sept. 2019), 231–245. https://doi.org/10.1007/s11896-019-09334-5

[93] Rajvardhan Oak and Zubair Shafiq. 2025. "Hello, Is This Anna?": Unpacking the Lifecycle of Pig-Butchering Scams. *Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)* (2025). https://doi.org/10.5555/3767870.3767871

[94] Rajvardhan Oak and Zubair Shafiq. 2025. Victims, Vigilantes, and Advice Givers: An Analysis of Scam-Related Discourse on Reddit. *Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)* (2025). https://doi.org/10.5555/3767870.3767874

[95] Ofcom. 2023. *Online Scams and Fraud Research: Summary Report*. Technical Report. Office of Communications (Ofcom). https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-fraud-and-scams/online-scams-and-fraud-research-summary-report Research conducted by Yonder Consulting on behalf of Ofcom.

[96] Amy Ogan, Erin Walker, Ryan Baker, Ma. Mercedes T. Rodrigo, Jose Carlo Soriano, and Maynor Jimenez Castro. 2015. Towards Understanding How to Assess Help-Seeking Behavior Across Cultures. *International Journal of Artificial Intelligence in Education* 25, 2 (2015), 229–248. https://doi.org/10.1007/s40593-014-0034-8

[97] Dan Olson. 2022. Line Goes Up – The Problem With NFTs. YouTube video. https://www.youtube.com/watch?v=YQ_xWvX1n9g Channel: Folding Ideas. Accessed February 4, 2026.

[98] Cyril Onwubiko. 2020. Fraud Matrix: A Morphological and Analysis-Based Classification and Taxonomy of Fraud. *Computers & Security* 96 (2020), 101900.

[99] Brittany O'Shea, Rebecca Feicht, Marion Brown, and Matthew Numer. 2024. Rethinking Sexual Violence Labels: Exploring the Impact of 'Victim'and 'Survivor'Discourse. *European journal of psychotraumatology* 15, 1 (2024), 2296329.

[100] Shruti Phadke. 2025. Exit Stories: Using Reddit Self-Disclosures to Understand Disengagement from Problematic Communities. *Proc. ACM Hum.-Comput. Interact.* 9, CSCW2, Article 411 (nov 2025), 27 pages. https://doi.org/10.1145/3757592

[101] Julie Prescott, Terry Hanley, and Katalin Ujhelyi. 2017. Peer Communication in Online Mental Health Forums for Young People: Directional and Nondirectional Support. *JMIR Mental Health* 4, 3 (Aug 2017), e29. https://doi.org/10.2196/mental.6921

[102] Claudette Pretorius, Derek Chambers, and David Coyle. 2019. Young People's Online Help-Seeking and Mental Health Difficulties: Systematic Narrative Review. *Journal of Medical Internet Research* 21, 11 (2019), e13873. https://doi.org/10.2196/13873

[103] Domestic Abuse Intervention Programs. [n. d.]. Understanding the Power and Control Wheel. https://www.theduluthmodel.org/wheels/understanding-power-control-wheel/. Accessed November 14, 2025.

[104] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as Informal Lessons about Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS 2012)* (Washington, D.C., USA) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 6, 17 pages. https://doi.org/10.1145/2335356.2335364

[105] Noshene Ranjbar, Matt Erb, Othman Mohammad, and Francisco A. Moreno. 2020. Trauma-Informed Care and Cultural Humility in the Mental Health Care

of People From Minoritized Communities. *Focus* 18, 1 (2020), 8–15. https://doi.org/10.1176/appi.focus.20190027
[106] A.J. Ravenelle, S. Janko, and K.C. Kowalski. 2022. Good Jobs, Scam Jobs: Detecting, Normalizing, and Internalizing Online Job Scams During the COVID-19 Pandemic. *New Media & Society* 24, 7 (2022), 1591–1610. https://doi.org/10.1177/14614448221099223
[107] Joseph Reagle. 2022. Disguising Reddit Sources and the Efficacy of Ethical Research. *Ethics and Information Technology* 24, 3 (2022), 41. https://doi.org/10.1007/s10676-022-09663-w
[108] Reddit, Inc. 2024. Form S-1 Registration Statement. U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/1713445/000162828024006294/reddits-1q423.htm Accessed February 22, 2024.
[109] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 1–13. https://doi.org/10.1145/3173574.3174086
[110] Zhiying (Bella) Ren, Eugen Dimant, and Maurice E. Schweitzer. 2021. Beyond Belief: How Social Engagement Motives Influence the Spread of Conspiracy Theories. *Journal of Experimental Social Psychology* 104, 104421 (Sept. 2021). https://doi.org/10.1016/j.jesp.2022.104421
[111] C. A. Robb and S. Wendel. 2023. Who Can You Trust? Assessing Vulnerability to Digital Imposter Scams. *Journal of Consumer Policy* 46, 1 (March 2023), 27–51. https://doi.org/10.1007/s10603-022-09531-6
[112] Kate Roberts, Anthony Dowell, and Jing-Bao Nie. 2019. Attempting Rigour and Replicability in Thematic Analysis of Qualitative Research Data; A Case Study of Codebook Development. *BMC Med Res Methodol* 19, 66 (2019). https://doi.org/10.1186/s12874-019-0707-y
[113] Abhishek Roy, Narsi G, and Sujata Mukherjee. 2025. ShieldUp!: Inoculating Users Against Online Scams Using A Game Based Intervention. http://arxiv.org/abs/2503.12341. https://doi.org/10.48550/arXiv.2503.12341 arXiv:2503.12341 [cs]
[114] Morgan Klaus Scheuerman, Jialun Aaron Jiang, Casey Fiesler, and Jed R. Brubaker. 2021. A Framework of Severity for Harmful Content Online. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2 (Oct. 2021), 368:1–368:33. https://doi.org/10.1145/3479512
[115] Shalom H. Schwartz. 1977. Normative Influences on Altruism. In *Advances in Experimental Social Psychology*, Leonard Berkowitz (Ed.). Vol. 10. Academic Press, 221–279. https://doi.org/10.1016/S0065-2601(08)60358-5
[116] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the 2010 CHI Conference on Human Factors in Computing Systems (CHI '10)*. Association for Computing Machinery, New York, NY, USA, 373–382. https://doi.org/10.1145/1753326.1753383
[117] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. 2018. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/SP.2018.00023
[118] Gilberto Atondo Siu and Alice Hutchings. 2023. "Get a higher return on your savings!": Comparing adverts for cryptocurrency investment scams across platforms. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 158–169. https://doi.org/10.1109/EuroSPW59978.2023.00023
[119] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3290605.3300319
[120] Frank Stajano and Paul Wilson. 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Commun. ACM* 54, 3 (March 2011), 70–75. https://doi.org/10.1145/1897852.1897872
[121] John Suler. 2004. The Online Disinhibition Effect. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* 7 (July 2004), 321–6. https://doi.org/10.1089/1094931041291295
[122] Richard Titus and Angela Gover. 2001. Personal Fraud: The Victims and the Scams. In *Crime Prevention Studies*. Vol. 12. 133–151.
[123] Elisa Tjondro, Cherrylia Ester, Yovita Gisella Sardjono, and Adhityawati Kusumawardhani. 2025. Investment Scam Vulnerability among University Students: The Role of Personality Traits and Risk Tolerance. *Cogent Education* 12, 1 (Dec. 2025), 2464309. https://doi.org/10.1080/2331186X.2025.2464309
[124] Tamara van der Does, Mirta Galesic, Zackary Okun Dunivin, and Paul E. Smaldino. 2022. Strategic Identity Signaling in Heterogeneous Networks. *Proceedings of the National Academy of Sciences* 119, 10 (2022), e2117898119. https://doi.org/10.1073/pnas.2117898119
[125] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*. 2344–2360. https://doi.org/10.1109/SP46214.2022.9833643
[126] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. 2024. Understanding Help-Seeking and Help-Giving on Social Media for Image-Based Sexual Abuse. (2024). https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-understanding
[127] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 447–462. https://doi.org/10.5555/3563609.3563633
[128] Monica T Whitty and Tom Buchanan. 2016. The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial. *Criminology & Criminal Justice* 16, 2 (April 2016), 176–194. https://doi.org/10.1177/1748895815603773
[129] Monica T Whitty and Tom Buchanan. 2016. The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice* 16, 2 (2016), 176–194.
[130] Matthew L Williams, Pete Burnap, and Luke Sloan. 2017. Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, Online Context and Algorithmic Estimation. *Sociology* 51, 6 (Dec. 2017), 1149–1168. https://doi.org/10.1177/0038038517708140
[131] Jamie Woodcock and Mark Graham. 2019. *The Gig Economy: A critical Introduction*. Polity.
[132] Ryan T. Wright, Steven L. Johnson, and Brent Kitchens. 2023. Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection. *Management Information Systems Quarterly* 47, 2 (June 2023), 803–832. https://doi.org/10.25300/MISQ/2022/16625
[133] Heng Xu, Jun Zeng, Zheng Cao, and Huihui Hao. 2022. The Relationship between Intimate Partner Violence and Online Help-Seeking: A Moderated Mediation Model of Emotion Dysregulation and Perceived Anonymity. *International Journal of Environmental Research and Public Health* 19, 14 (2022), 8330. https://doi.org/10.3390/ijerph19148330
[134] David S. Yeager, Valerie Purdie-Vaughns, S. Y. Hooper, and G. L. Cohen. 2017. Loss of Institutional Trust Among Racial and Ethnic Minority Adolescents: A Consequence of Procedural Injustice and a Cause of Life-Span Outcomes. *Child Development* 88, 2 (2017), 658–676. https://doi.org/10.1111/cdev.12697
[135] Lei Yu, Gary Mottola, Lisa L. Barnes, S. Duke Han, Robert S. Wilson, David A. Bennett, and Patricia A. Boyle. 2021. Correlates of Susceptibility to Scams in Community-Dwelling Older Black Adults. *Gerontology* 67, 6 (2021), 729–739. https://doi.org/10.1159/000515326
[136] Yun Zhang, Qun Wu, Ting Zhang, and Lingxiao Yang. 2022. Vulnerability and Fraud: Evidence from the COVID-19 Pandemic. *Humanities and Social Sciences Communications* 9, 1 (Nov. 2022), 424. https://doi.org/10.1057/s41599-022-01445-5
[137] Xiaoqian Zhu, Xiang Ao, Zidi Qin, Yanpeng Chang, Yang Liu, Qing He, and Jianping Li. 2021. Intelligent Financial Fraud Detection Practices in Post-Pandemic Era. *The Innovation* 2, 4 (Oct. 2021), 100176. https://doi.org/10.1016/j.xinn.2021.100176

# A Codebook

## A.1 Scam characteristics

**Scam type** (informed by Beals et al. [10]): Select the code from below that best captures the type of scam (see Table 1 for descriptions of each scam type):

- Cartel
- Phantom Debt
- Seller
- Accidental Payment
- Charity
- Authoritative Entity
- Romance
- Personal Relation
- Investment & Crypto Culture
- Employment
- Prize & Grant
- Buyer

**Scam details** (informed by Roy et al. [113]): Notes on tactics and mechanisms of the scammer, focusing on how they interact with

the target to induce emotions, impel action, manipulate, deceive, and/or defraud them. Examples:

- Appeal to emotion
- Norm activation
- Make a threat
- Impersonate a person
- Impersonate an org/authority
- Offer something of value
- Urgency (to induce a concern, such as fear)
- Urgency (to indicate scarcity)

**Harm** (informed by Scheuerman et al. [114]): Select all codes from below that describe the type of harm self-reported by the poster, or take notes if they do not apply:

- Financial: "Financial harm is defined as material or financial loss, including the loss of digital assets like accounts." [114]
- Emotional: "Emotional harm ranges from an annoyance (at its least severe) to a stressful or traumatic emotional response (at its most severe), whether fleeting or long-lasting." [114]
- Relational: "Relational harm is defined as damage to one's reputation or their interpersonal, professional, or larger community relationships." [114][20]
- Legal: The poster reports harm related to legal issues.
- PII lost: The poster reports that the target lost personal information to the scammer.
- Time lost: The poster explicitly reports time lost to the scam as a hardship. (Do not interpret the time spent on the scam as a harm unless it is explicitly described as a hardship.)
- Stolen labor: The poster reports the scam involved performing uncompensated labor.
- None: The poster has not reported that the target has been harmed. This captures cases where the target catches the scam before the point of harm.

**Temporality**: For cases when harm has occurred, take notes on how long the target was involved with the scam or any other interesting time-relevant information, if explicitly described.
**Repeat victimization**: Indicate "Yes" and optionally take notes when a target has been victimized by more than one scam.
**Additional notes**: Notes on harm details, such as what was lost, monetary amounts, quotes describing emotional harm, etc.

## A.2 Help-seeking characteristics

**Help needs** (informed by Wei et al. [126]): Indicate the type of help the poster describes needing. Select any codes below that apply:

- Sensemaking: Expresses a need for help in trying to understand something related to a scam.
- Guidance: Expresses a need for help about what actions to take related to a scam.
- Therapeutic: Expresses a need for emotional support, such as reassurance, validation, self expression, etc. Includes cases when the poster has a strongly emotional tone, indicating a need to vent. Includes cases when the poster is helping others.
- External Action: Expresses a need for a third party to take direct action to help the poster/target.

**Help giving:** Notes on help given to others, such as informing others of a scammer and their tactics, explaining scams, sharing their story of a scam encounter, etc.

## A.3 User state characteristics

**States from User States Framework [87]**: Indicate the states during which the poster is seeking help. Select any state code below that applies. If Active Event is selected, also select only one Active Event substate code that best captures the substate:

- Prevention: When a person wants to minimize their exposure to future tech-facilitated attacks (or help someone else do so); they're likely to feel low or typical stress, unless they feel threatened. This tends to be done when a person is not actively coping with an attack.
- Active Event: When a person wants to stop or otherwise respond to an attack(s). This tends to include the period of time starting immediately after a person starts suspecting or becomes aware of the attack and extends through the time they are trying to stop or limit initial harm, often expressing worry or distress. If a person is unable to understand or stop an attack, or if attacks overlap, this could be an extended period of time.
  - Diagnostics: When a person is considering responding to a suspected scam, but has yet to do so or experience significant negative consequences. This tends to be when a person is in the process of trying to identify whether suspect behavior is a scam; they may feel confusion or suspicion, but also may feel motivated to engage. This also includes cases when the poster does not yet realize they are potentially experiencing a scam, but they worry something is wrong before engaging and a researcher can identify a likely scam from their description.
  - Mitigation: When a person has been partially impacted by the scam and there is potential for more harm. Emotions spike in this substate, including worry, fear, or even panic. A person likely wants to stop the scam, understand its potential impact, avoid further harm, and soothe emotions.
  - Denial: When a person targeted by a scam does not acknowledge or believe there is any fraudulent activity in their interactions with a scammer. Another person suspects or recognizes the Active Event and wants to help the target. The target may not seem worried or distressed, though others may express worry or distress due to the target's Active Event.
- Monitoring: When a person wants to watch for signs of attacks; they're likely to feel low or typical stress, unless they feel threatened. This can be done separately from an event or attack, but also in response to threats or attacks. Monitoring can commonly overlap with Active Event or Recovery—after a user is attacked, a typical response is to vigilantly monitor for more to occur.
- Recovery: When a person wants to fix damage from the attack(s), determine what happened, and cope with trauma; they're likely to feel moderate to high stress. This tends to

[20]The fourth harm type from Scheuerman et al. [114]—Physical harm—was not present in our data.

start after the acute stress or panic of the event has subsided (though people in this state may still express ongoing mental health challenges). This state can extend over a long time period, since resolving damage and coping with trauma from an attack can be lengthy processes.

**Emotion notes**: Notes on what emotions the poster is expressing.
**Motivation notes**: Notes on what motivations the poster is expressing.
**Practices tried**: Notes on previously attempted practices or remediation steps mentioned by the poster.

## A.4 Target characteristics

**Demographics**: Notes about the demographics of the target and poster (if different).
**Target's relationship to the poster**: Notes about the relationship between the poster and the target, if they are different people.
**At-risk user**: Notes about whether the target and poster (if different) mention an at-risk group or contextual risk factor in relation to the scam (following definitions in Warford et al. [125]).