Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy

Manya Sleeper, Tara Matthews*, Kathleen O'Leary†, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, Sunny Consolvo
Google, Mountain View, CA, USA
{manya,katieole,annaturn,jillwoelfer,martinshelton,anoplinger,aschou,sconsolvo}@google.com
*Independent, Pullman, WA USA
taramatthews@gmail.com
†Google, Seattle, WA, USA

ABSTRACT

Addressing digital security and privacy issues can be particularly difficult for users who face challenging circumstances. We performed semi-structured interviews with residents and staff at 4 transitional homeless shelters in the U.S. San Francisco Bay Area (n=15 residents, 3 staff) to explore their digital security and privacy challenges. Based on these interviews, we outline four *tough times* themes — challenges experienced by our financially insecure participants that impacted their digital security and privacy — which included: (1) limited financial resources, (2) limited access to reliable devices and Internet, (3) untrusted relationships, and (4) ongoing stress. We provide examples of how each theme impacts digital security and privacy practices and needs. We then use these themes to provide a framework outlining opportunities for technology creators to better support users facing security and privacy challenges related to financial insecurity.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; Usability in security and privacy; • **Human-centered computing** → *Empirical studies in HCI*;

KEYWORDS

Security; privacy; user study; financial insecurity; homelessness; optimistic user vision; qualitative study

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/3290605.3300319

ACM Reference Format:
Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, Sunny Consolvo. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland Uk.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3290605.3300319

1 INTRODUCTION

Many people worldwide face financial insecurity. For example, 41% of U.S. adults would not be able to easily access $400 [21]. Financial insecurity can contribute to "digital inequalities" [26] with wide-ranging effects on technology use. People with limited means might, for example, rely on older technology, have limited Internet access, and rely on mobile devices [1]. These limitations can have varied impacts. In this paper we focus on impacts to digital security and privacy (S&P), which has not been the focus of prior work.

Despite the challenges faced by many financially insecure users, technology affordances tend to focus on a techno-optimistic vision of the user and their ability to interact with technology [43]. Such an "optimistic user vision" (as we refer to this concept in this paper) can include the assumption that users have access to trusted personal devices, have reliable Internet access, and will benefit from increased technology. It can be tempting to focus on this optimistic user who can readily adopt new technologies. Unfortunately, however, affordances that focus on this type of vision might not fully account for the challenges associated with financial insecurity, which can limit the inclusivity of design [25, 43, 44]. Financially vulnerable users need the technology community to also understand and prioritize the (sometimes mundane) issues that can limit their digital inclusion.

In this paper we focus on how an intersecting set of challenges associated with financial insecurity (which we refer to as *tough times*) can uniquely impact digital S&P practices and needs. The consequences of S&P issues can be high, ranging from theft to stalking [16, 20, 39]. At the same time, addressing S&P issues can be particularly difficult for users who face challenging circumstances [20]. Our results include:

- ***Tough times* themes:** An outline of four types of challenging circumstances associated with financial insecurity, specifically (1) limited financial resources, (2) limited access to reliable devices and the internet, (3) the need to cope with untrusted relationships, and (4) ongoing stress.
- **S&P impact of *tough times*:** Examples of how these four challenges can uniquely impact digital S&P for financially vulnerable users.

To identify these themes and examples, we performed 18 semi-structured interviews with residents and staff of transitional homeless shelters. We explored the role digital S&P played in residents' lives, their S&P practices, and S&P issues they faced. We focused on financially vulnerable users in a developed region by interviewing participants living in the San Francisco Bay Area (U.S.). Our participants needed to use technology as part of their everyday lives, but also faced *tough times* challenges. Throughout the paper, when we refer to "financially vulnerable users," we refer to those who live in developed regions.

Through a qualitative exploration of these themes, we seek to both build empathy for, and understanding of the needs of, financially vulnerable users. We also consolidate the study results into a *tough times* framework, which we use to discuss ways to help the technology community prioritize design improvements to address a set of S&P issues financially distressed users experience.

2 RELATED WORK

We extend prior work on how financial insecurity impacts the ability to meet an optimistic user vision assumed by technology creators, as well as prior work focused on S&P experiences in specific circumstances (e.g., developing regions, among survivors of intimate partner abuse). Uniquely, we focus on how financial insecurity in developed, technology-rich areas can impact digital S&P experiences.

Financial insecurity and technology use

Broadly, financial insecurity can impact technology use, especially when technology creators focus affordances on a more optimistic user vision. This dynamic can contribute to a range of barriers to technology use [25].

Barriers to meeting an optimistic user vision. Financial insecurity is associated with a variety of barriers to meeting an optimistic user vision of technology engagement (i.e., the assumption that users have access to trusted personal devices, have reliable Internet access, and will benefit from increased technology). In the U.S., lower income levels tend to be correlated with lower rates of household Internet access and higher rates of mobile-only access [1]. For example, Yardi and Bruckman found that lower socioeconomic status (SES) users who became unemployed were forced to choose between a laptop, cell phone, or broadband Internet [47].

One area where these barriers can be particularly apparent is the use of employment and government benefits sites. Technology can play an important role in improving financial status, especially when job and government systems are digital [3, 25, 35]. However, lower resourced users can encounter barriers to these financial benefits when these systems' affordances assume a more optimistic user vision. Prior work has found, for example, a variety of skill and social barriers for users of job search sites who have low incomes [7, 14, 25, 41]. Similarly, users who lack reliable Internet access might have trouble accessing government benefits and job search resources [25, 47].

Technology use by people who are homeless. People who are homeless face financial insecurity, as well as many other challenges, which can prevent them from meeting the assumptions of an optimistic user vision. A variety of work has examined the technology use and needs of homeless populations. Like other groups, people who are homeless use technology in their everyday lives [15, 18, 23, 24, 28, 30, 43, 44] and can be disempowered and experience negative outcomes when they lose access to digital resources [18].

As in prior work, we study a sample of people experiencing homelessness, specifically who were housed in transitional shelter housing. We extend prior work by focusing on the challenges they face associated with financial vulnerability and specifically on their S&P experiences. To explore the intersection of financial vulnerability and S&P experiences we draw on a framework used by Woelfer and Hendry in work with homeless young people [43, 44] (details in Methods).

Digital S&P

S&P features can be critically important to online safety. Thus, it can be important for designers to consider the S&P challenges of financially insecure users both to design more inclusive S&P features and to increase overall digital equality. For example, S&P issues can reduce access to technology – users whose needs are not met sometimes abandon devices or accounts, or self censor content [16, 20, 39].

Challenges of S&P design. Research has broadly focused on increasing the usability of S&P features, typically focusing on general users [6]. However, Redmiles et al. [27] found that people with lower SES experience S&P events at similar rates to people with higher SES. Given that financially vulnerable users face a number of barriers to technology engagement, it is important to understand how the challenges they face can impact their S&P strategies and needs.

In a few cases, S&P-focused research has gone beyond an optimistic or general vision of the user to focus on specific populations. Dunphy et al. emphasize the value of this approach for S&P "to make more pronounced the needs that many of us have" [9]. We briefly summarize findings from such work with survivors of intimate partner abuse [11, 12, 20] and users in developing countries (ICT4D) [33, 38], to highlight both the valuable insights that can be gained from considering participants from specific populations and how our study extends prior research.

Prior work has explored S&P practices and risks demonstrated by survivors of intimate partner abuse. Survivors face many dangerous dynamics — such as online stalking, harassment, and control by their abusers — that can shape their S&P risks and strategies [11, 12, 20]. Design directions have been proposed to support survivors' needs, including an increased focus on usability to account for survivors' high stress levels and a focus on ways to provide transparency into account use [11, 20]. We extend this work by also exploring the impact of relations beyond intimate partners.

Digital S&P needs and practices can also be shaped by ICT4D dynamics. Vashinstha et al. [38] reviewed 10 years of S&P work in the ICT4D space and outlined how S&P practices and risks in developing countries can be shaped by cultural norms, knowledge gaps, device sharing, contextual reasons for technology use, and a strong need for usable low-cost technology. Technology might not be designed for these factors, which can contribute to ad hoc or culturally specific S&P strategies [33, 38]. More inclusive design for S&P in these contexts can, therefore, focus on accounting for culturally and contextually specific norms [33].

Our participants had some overlapping needs with users in ICT4D environments. For example, they also needed to prioritize low cost technology. However, we extend work in the ICT4D space by focusing on participants in a technology-rich region of the U.S. where technology use is expected for everyday activities. Participants also faced many of the same cultural norms as people who met an optimistic user vision. Working with these participants allowed us to focus on how challenges they faced due to financial vulnerability (in a technology-rich environment) impacted their S&P.

3 METHODS

To explore S&P challenges related to financial insecurity, we performed 18 semi-structured interviews with residents and staff at 4 transitional homeless shelter sites.

Shelter collaboration and participants

Participants were 15 residents (11 female, 4 male) and 3 staff members from 4 transitional housing shelter locations (1 serving adults, 3 serving families) run by 1 shelter network in the U.S. San Francisco (SF) Bay Area (California). The shelter network provided services to homeless adults and families at a variety of locations in the area. Residents were required to apply and meet a number of requirements (e.g., they needed to be homeless or facing eviction). They were then provided with housing on a temporary basis, typically a few months. Residents of family shelters (most of our participants) were provided with apartment-style housing.

We collaborated with the shelter network to co-create the study proposal, ask for advice on running study sessions (e.g., communication style), recruit participants, and determine appropriate incentives. Staff members recruited participants based on criteria provided by the researchers. Participants were over 18 years old, used the Internet, and self-reported having a technology-related security or privacy concern.

To protect participant privacy, we only collected limited demographics. Based on their residence in the shelters, we knew all participants had relatively limited financial means. However, because they were homeless in a relatively wealthy area, many had jobs and/or were in school. We recruited most participants from family shelters, and these participants also had children living with them.

Setting and context. The shelter network was in the SF Bay Area, which is a relatively wealthy, major metropolitan area with high housing costs. Similar to many locations in the U.S. [25], our participants lived in a technology-rich environment where they were expected to use the Internet regularly. These expectations arose partially from explicit shelter and government-driven requirements and processes. For example, the shelter organization sometimes required residents to use the shelter support services, which could include job and housing search. In the SF Bay Area, job and housing search often require Internet use. Participants also needed to interact with official government systems online. Several participants were veterans and needed to use online systems for veterans' job and benefits services. Government jobs and welfare systems in the state also tend to be digitized.

More generally, participants also needed to use the Internet for many everyday activities, including education, purchases, directions, running personal businesses, saving documents and photos, communicating with friends and family, and accessing entertainment. The need for digital access meant they tended to prioritize maintaining online access over other expenses. All participants also had access to at least one device, even if the device was older or shared.

Semi-structured interviews

We performed semi-structured interviews in the summer of 2015 (31-69 minutes long, median of 54 minutes) focused on participants' technology use and S&P experiences. Each interview was performed by two interviewers, audio recorded, and transcribed (with the participant's consent).

To start each session we reviewed our informed consent and gave the participant a $100 gift card. The amount was approved by the shelter organization and an ethics review process at Google. Participants were also provided with consent documents and given the opportunity to opt out before the study (and at any time during the study).

Shelter resident interviews. Resident interviews (n=15, referred to as P1...P15 in the paper) then used an experience-centered approach, focused on their experiences with technology and digital S&P [9]. The interview began with an "ice breaker" survey in which they outlined devices and accounts they used. We probed: (1) "Which of these devices are most important to you and why?" and (2) "Are any of these devices used by anyone else?"

We next asked participants questions about their digital S&P experiences: (1) "Can you tell me about a time when someone gained access to information about you that you did not want them to have?" and (2) "Can you tell me about a time when someone else gained access to one of your accounts or devices? Or tried to?" We followed up with probes: "What happened as a result?" "What did you do next?" "How has this affected how you use technology?" Finally, participants performed a card sort activity, in which they ordered statements about digital S&P features and strategies (e.g., "customize privacy settings," "use 2-factor verification," "delete an account") by how strongly they felt each was most or least like them. We used the sorted online safety features as additional prompts (e.g., "Why did you place this card here?" "Can you tell me a story about a time when you needed to do [strategy]?") and analyzed the results qualitatively.

Shelter staff interviews. We also interviewed 3 shelter staff members (referred to as SW1, SW2, and SW3) as they are important stakeholders in the residents' access to and use of technology [43, 46]. The staff members first described their roles and technologies the residents used. Next, we asked them to describe a specific situation during which a resident they worked with was attacked or threatened using digital means (without revealing personal information). We next asked them to describe the technology-related concerns the residents had ("What types of information are they concerned about?" "What are they worried about happening as a result?" "Who are they worried about?" "How are they addressing their concerns?"). Finally, we asked staff members to explain "What do you think your clients should be doing or using but are not, to protect themselves online?" Staff members also described their own technology use and S&P experiences, but we do not report on those results.

Additional study. Portions of four interviews were also included in a separate analysis for a study run concurrently on S&P experiences for survivors of intimate partner abuse [20]. We included the full interviews in this analysis as well, and report on experiences relevant to our *tough times* themes. We do so because the participants were part of the original sample, and the majority of the results related to financial insecurity do not overlap results reported previously.

Anonymization and well-being

We took several steps to protect participant privacy. We removed personally identifiable information from the transcripts (e.g., granular locations, names, workplaces, ages of children, etc.). In addition, we removed unique word choices or methods of speaking from quotes, for example filler words.

We also took steps to minimize potential harm to participants and researchers. We tried to protect participants from undue emotional distress by focusing the interviews on questions designed to elicit S&P and technology-related experiences, rather than on general experiences of homelessness or economic distress. Participants could also have an advocate join them for the interviews, although none chose to have one present. To protect participant and researcher well-being, we also worked with the shelter staff to make aftercare counseling available on request.

Analysis

To analyze the interviews, we performed iterative qualitative analysis that drew on a framework outlined by Woelfer and Hendry to understand the tensions inherent in designing for homeless youth in Seattle [43, 44]. This framework focuses on how societal expectations (e.g., for continuous internet access) can be in tension with the "exaggerated needs" experienced by the youth.

We focused on analyzing the forces (which we called *tough times* challenges) experienced by our participants, which might not align with an optimistic user vision. We first created a set of codes based on themes from a review of literature on homeless users' experiences with technology use, technology-related risks, and challenging circumstances [2, 10, 18, 24, 28–32, 36, 37, 42, 43, 45]. One researcher then used these initial codes to iteratively developed an initial codebook from the full set of interviews, over several rounds of coding and discussion with the other researchers.

We then narrowed the initial codebook to focus on (1) dynamics participants described that could impact S&P (resulting in the *tough times* challenges); and (2) the S&P impacts of these dynamics, including issues, perceived risks, and practices. One researcher, in discussion with others, including an expert on the sample population, selected the items to include. Two additional researchers each coded a subset of the items. After each round the researchers iteratively updated the codebook. A summary of the final codebook is in Table 1 (challenges) and Table 2 (impacts associated with these challenges).

4 RESULTS

We outline four themes that reflect *tough times* challenges participants faced. We provide examples of how these challenges impacted participants' digital S&P. These themes and impacts are summarized in Tables 1 and 2.

Challenge	Contrasting optimistic user vision
1. Limited financial resources	Financial flexibility to choose the safest option and have a safety net to recover from problems
2. Limited access to reliable devices & Internet	Access to up-to-date reliable devices and Internet
3. Untrusted relationships	Able to trust known people with access to devices & accounts
4. Ongoing stress	Mental energy to cope with S&P issues

Table 1: We identified four *tough times* challenges that contrasted with optimistic user visions.

Limited financial resources

Our first *tough times* challenge centers on participants' struggle to get by with limited financial resources. Our participants were unable to afford housing at the time of the study. Many shelter residents also received government benefits, and some participants described payday loans or debts. P14 explained, for example:

> *"I'm the type of person that lives paycheck by paycheck...if somebody were to take...$20 from me that could feed my family for a week."* (P14)

We outline how participants' limited financial resources could (1) lead to the need to provide personal information to websites, (2) make it difficult to give up options they knew might be *too good to be true*, and (3) slow recovery after digital S&P issues.

Providing personal info. Limited finances meant participants needed to perform online activities using personal information to meet basic needs. For example, participants had to use online benefits websites, job search sites, and housing sites, which tend to ask for personal information. One shelter worker explained:

> *"[They] use their personal information more actively in terms of applying for benefits or resources. You know getting help from shelters, going to human services agencies. They're using things like their social security number a lot more actively. So that makes them more vulnerable."* (SW2)

Similarly, because participants were struggling financially they greatly valued free or discounted services, such as grocery store loyalty card discount programs. These types of services tend to require personal information, but providing this information sometimes led to spam or unwanted ads. P15 explained, *"You go to a store, and they're like, you can get 15 percent off, just give us your e-mail."* Beyond potential for spam, frequent use of services that ask for personal information might habituate participants to providing information online, increasing their risk for scams or phishing.

Increased risk of scams. Participants also sometimes found it difficult to bypass unsafe choices online even when they knew the options might be risky. Digital security features, such as SSL indicators, warnings, and phishing alerts and education usually rely on users understanding and avoiding unsafe choices. For example, phishing education teaches users different signals, to watch out for suspicious emails or websites. Users are then expected to avoid clicking on untrustworthy links on their own [40].

However, participants' limited means sometimes made it difficult for them to bypass low-cost online options, even when they knew those options were suspicious. Participants desperately needed very low cost housing and extreme online deals, which carry a high risk of scams [22]. A staff member described, for example, how residents were particularly vulnerable to housing scams, because they desperately wanted affordable housing:

> *"...I've had clients get really excited...They'll see a three bedroom house in [city] for $1,000 [USD]...it's at a price range that's like well maybe that could be reasonable, but in this area that's completely not realistic. But then it's at that cusp where it's like, 'Should I contact them? Should I give them my personal information?'...that's just kind of that desperation."* (SW2)

Difficult to recover. Participants described how their limited means made it difficult to recover from scams, identity theft, or other problems that could result from digital S&P issues. This meant a resulting financial setback could impact their basic needs, for example the ability to buy food or pay rent. P4, for example, discovered that someone had stolen money from her bank account when her rent check bounced and assumed that someone had gotten access to the online account. She could not recover the money for several weeks.

Challenge	Sample impacts on participants' digital S&P experiences	Participant count
1. Limited financial resources	• Difficult to quickly recover after an issue	9
	• Habituated to provide personal info to websites (may be difficult to opt out)	7
	• Vulnerable to scams (difficult to give up deals that are *too good to be true*)	4
2. Limited access to reliable devices & Internet	• Need to use public & shared devices (despite increased risk of accidental data sharing)	16
	• Difficult to use 2FA (because of unreliable device setups)	2
3. Untrusted relationships	• Vulnerable to untrusted insiders (e.g., friends, family, acquaintances)	11
4. Ongoing stress	• Use drastic coping strategies for S&P threats (that can have negative impacts)	17
	• Difficult to make decisions or take action (due to higher levels of stress)	3

Table 2: We describe sample impacts the four *tough times* themes had on participants' S&P experiences. This table outlines the impacts identified in our interview codebook, as well as counts of residents and staff who described examples of each (residents described the impact on themselves, staff described the impact on residents)

Some participants described struggling to recover from identity theft for extended periods of time, due to a lack of funds. One staff member explained that most residents had a hard time repairing damaged credit after identity theft:

> *"A lot of times [residents] don't [recover from identity theft], because...a lot of the agencies that will help with fixing credit issues cost money. Our clients don't have money to pay for that."* (SW2)

P5 described how this struggle to recover had impacted him. He had fallen prey to identity theft several years earlier but still felt long-term emotional and financial impacts:

> *"All I know is [they] took money from me...I had to spend money that I couldn't afford to spend to try and get all this stuff taken care of, and finally I just said, 'You know what? I'm tired...I can't keep fighting these people...I don't have the resources to prove that this is not me.'"* (P5)

Participants also sometimes struggled to recover when their devices broke, because they could not afford to replace or fix devices. P14 explained that she could not afford to replace the computer she had broken several years earlier:

> *"I messed up my computer and now I don't have a computer anymore...I have a phone, and that's basically what I use."* (P14)

Limited access to reliable devices and Internet

Because of their limited means, participants also had limited access to reliable, personal, up-to-date devices and reliable Internet — our second *tough times* theme. All participants had access to at least one device, typically a mobile phone. However, these devices tended to be outdated, limited, and often shared. P3 explained, for example, that she had stopped texting, because her phone ran out of memory: *"I have to keep deleting messages and deleting pictures and deleting apps, just to receive a text message."* Some participants described feeling they could not justify the cost of replacing older or limited devices. P9 explained, *"I don't need it, it's a want."*

Participants also tended to have limited access to reliable Internet. Some shelters did not to provide Wi-Fi, and only provided limited Internet access through shelter computers, for example only for job and housing search. Some participants, therefore, needed to rely on personal Wi-Fi hotspots and mobile data for personal Internet. However, relying on these methods meant that participants had limited online data and had to carefully ration use or could lose access. For example, P9 purchased a mobile hotspot. Without her realizing it, her son used up all the data playing games, and she could not afford to refill it. She explained:

> *"I [got a mobile hotspot]. There was a limit to the amount [of data], and my son ended up using the whole thing to play games, and I didn't even know. So [the hotspot] is sitting in the drawer."* (P9)

This lack of reliable devices and Internet access (1) led participants to rely on shared and public devices, increasing the potential for accidental data sharing; and (2) could make it difficult to use authentication methods tied to accounts, devices, or phone numbers.

Shared and public devices. Despite having limited access to personal Internet and lacking reliable personal devices, participants still required the Internet for everyday needs. To get online they described sharing devices with family members and using public computers and Wi-Fi, for example at the library or at fast food restaurants. This reliance on shared and public devices for Internet access is typical for users with lower incomes [25, 47].

Using shared and public devices, and public Wi-Fi, can increase the risk of accidentally sharing account information or other data [19]. Some participants realized this was a risk but did not feel they had a choice, because they needed to get online and could not afford to do so on private devices. P9 explained, for example, that when she needed to check her email, she would use her father's computer, even though it was shared with family members:

> *"...sometimes I use my dad's laptop to get into [my email], and my password is saved on there...and a lot of people use his laptop, like my sister, my brother...it's like the house laptop."* (P9)

Similarly, P5 relied on free public Wi-Fi even though he felt it was risky:

> *"I know the risks of public Wi-Fi, but I really don't have the option not to use that...I have to go after the free stuff because I can't afford the other side of it."* (P5)

Difficult to use 2FA. Unreliable access to Internet and older devices can make it more difficult to use authentication methods in which identity is tied to a device, account, or phone number. Our participants' experiences with two-factor authentication (2FA) provide an example of this. 2FA is a commonly recommended tool that can help provide users with an additional layer of security for verifying their identities by using a secondary source of authentication, such as a phone or a hardware token. It can be especially useful for users who are moving between shared or public devices [16]. But, 2FA requires a user to have reliable access to a second factor on which to receive a code, such as a text message sent to a phone, a security key, or an app — things our participants sometimes did not stably have.

Two participants described losing access to second factors they had set up. For example, P13 was unable to pay his mobile phone bills, so he could no longer receive text messages from the phone number he had set up for 2FA. This led him to get locked out of his email account. He explained:

> *"I had two-step verification on my phone...and I stopped paying my phone bill because it was too expensive...so I can't get into my account without the two-step verification [code]."* (P13)

Untrusted relationships

Our third *tough times* theme focuses on the fact that participants also sometimes found it difficult to avoid threats from people they were close to but did not trust for a variety of reasons. These people included abusive partners and a wide variety of other types of relationships.

Intimate partner abuse. Some participants were experiencing, or had experienced, intimate partner abuse. Intimate partner abuse can contribute to financial insecurity [49]. Participants who were survivors of intimate partner abuse described dangerous dynamics, including harassment, surveillance, and fear of physical violence, all of which reflected dynamics described in prior work [8, 11, 12, 20].

Other untrusted relationships. Beyond the abusive partners considered in prior work, participants also needed to interact with a variety of other types of untrusted people to whom they had ties. Some participants described romantic partners, and partners' associates, who were not abusive, but who also were not trustworthy. For example, P15 was in the process of divorcing her husband. She explained that she did not trust his new girlfriend and was worried the girlfriend might have access to any emails sent to her soon-to-be-ex husband.

Participants also described untrusted former friends and family members who behaved maliciously. For example, P4 had a family member who stole money from her. Similarly, P9 had a restraining order against a former friend who had harassed her online.

A few participants were also in recovery for addiction. They faced the additional challenge of deciding how to deal with people they may have trusted before they got sober. P12, for example, had been sober for about a year and a half. But, before she got sober, she had given a variety of people access to her computer, *"People that I would get drugs from and stuff like that."* After she got sober, she changed her passwords, but still worried they might have access to her accounts.

These types of untrusted relations could present a particular threat of account or device compromise because they had physical access to participants' devices and knowledge of participants. P10, for example, was fairly sure that her cousin had been able to maliciously change information in her social media account using knowledge about her:

> *"I'm thinking it might have been my cousin...at the time my password was my son's name and his birth date...she might have been able to figure that out pretty easily."* (P10)

Ongoing stress

Exacerbating other challenges, participants also needed to cope with ongoing stress from a variety of sources — our fourth *tough times* theme. They had ongoing financial need, which is associated with a variety of negative stressors [13]. In addition, some participants faced mental health issues, such as Post Traumatic Stress Disorder, adding to the stressors they faced. Many participants also described relatively low levels of tech savviness. We outline how these stressors could lead participants to deprioritize S&P issues or use broad coping strategies with potentially negative impacts.

Difficult to make decisions or take action. Coping with S&P issues can require mental energy. The design of S&P assistance and features may assume, for example, that a user has the mental energy to make well-thought-out choices, find available options, and follow detailed advice. A user trying to address an issue may need to find and follow instructions, review warnings or notices, reset a password, or contact a service provider [16].

However, when people are under stress, thoughtful actions can become difficult [17, 34]. Participants' ongoing stress could make S&P issues more difficult to address and lower in their priorities, and could contribute to participants taking drastic actions to try to cope with perceived threats. One shelter worker explained how important preventative actions can be deprioritized in the face of other necessities:

> *"When you have all these other things you're dealing with...trying to feed your kids and figure out where you're sleeping that night and looking for work and applying for benefits...even the simple process of contacting your phone company to get your number changed [to prevent harassment]...goes way down the list on your priorities."* (SW2)

Coping strategies. Fear of mistakes, as well as general stress, could also lead participants to take drastic measures to try to cope with perceived or actual risks, even if those coping strategies could have negative impacts.

Participants sometimes reset or abandoned devices or accounts, even if this meant they lost access to saved content, like photos, resumes, or contacts saved in an account. In one case, P10 abandoned an entire email provider when she believed that her account may have been compromised:

> *"When I had email [at Provider] I believe...that somebody had tried to access my information or tried to get into my account. And so by then I was just over the whole [Provider] and I moved to [other Provider]."* (P10)

Similarly, P14 was so scared after her computer had a virus that she asked her bank to freeze her bank account. She worried the virus would lead to identity theft, and she could not afford to lose any money: *"[I was afraid] for the little bit I had in my name to be removed and put in someone else's account."* Participants also sometimes avoided particular services or features that felt risky. Some tried to avoid online banking or shopping. For example, P4 explained that she only did banking face-to-face.

Some participants generally tried to avoid technology, because they feared it might cause harm. After P15's computer had a virus, she was scared to use technology. She explained *"I'm scared, so then I just only do the minimal of what I need to do on the computer."* More narrowly, some participants sometimes turned off, or only selectively turned on, settings they felt were risky. For example, P1 explained that she kept her GPS off *"unless I'm just GPS'ing myself somewhere."*

5 LIMITATIONS AND FUTURE WORK

We provide exploratory results from a study performed with a relatively small sample of participants from SF Bay Area transitional homeless shelters. This work is not intended to generalize to the needs of all people experiencing *tough times* or homelessness. This study also had the standard limitations of self-reported data, for example recall and observer bias. We hope future work can expand on our findings. For example, it could focus on developing specific technology solutions to help support people experiencing *tough times* (e.g., people in transitional housing). Or, it could provide a deeper understanding of how S&P experiences of people facing specific challenges might be impacted in different environments, for example through a broader sample of financially vulnerable participants or a sample recruited for more specific attributes associated with financial vulnerability.

6 DISCUSSION

We seek to help technology creators prioritize and focus on S&P issues that can impact financially vulnerable users. In this section, we use the *tough times* challenges to provide a framework that consolidates and clarifies how to think beyond an optimistic user vision. Based on our participants' experiences (Table 2), Table 3 lists how each challenge (first column) could impact financially vulnerable users (second column), and sample design considerations technology creators can think through as they create or update S&P features (third column). This can be used as an analysis tool in early-stage planning and later-stage evaluation to help ensure S&P features are sensitive to challenges faced by financially insecure users. In this section we also expand on some of the design considerations.

Consider impacts and costs of S&P

Based on our participants' experiences, technology designers can focus on supporting inclusive design by considering the practical costs financially distressed users may encounter when they experience, or try to address, S&P risks (see row 1, col 2 of Table 3). For example, limited resources can increase the practical costs of some protective actions. Freeing up space for security updates can be "costly," if it requires a user

Challenge	Sample practical issues that can impact S&P	Sample design considerations
1. Limited financial resources	***Impacts and costs of S&P*** • Difficulty of replacing devices • Impact of recovering from financial issues (or monetary and emotional costs of not recovering) • Cost of storage (e.g., need to delete content to free space) • Cost of making risky choices (e.g., strong needs may make giving up options that are *too good to be true* difficult) • Disproportionate impact of issues (e.g., even if a scam is eventually addressed, the impact can still be high if money is needed in the interim for necessities)	• How to reduce data and storage required to install S&P critical updates • How to educate and train agency and shelter staff on how to help others identify and recover from risks
2. Limited access to reliable devices & Internet	***Device and Internet setups*** • Lack of a trusted personal device (e.g., devices shared with untrusted people, use of public computers) • Limited and/or unreliable personal Internet • Unreliable personal devices (e.g., old or broken)	• Whether and how to draw on "bandwidth sensitive design" principles [4] to provide indicators and tools to help users manage and prioritize personal data • How to provide users with, and direct users to, S&P help content and options tailored to their device and operating systems (even for older technology) • How to build redundancy into security critical flows (e.g., ensure S&P features work independently of Internet access or a reliable phone number) • When it's appropriate to "stress test" designs against different device and Internet configurations
3. Untrusted relationships	***Ties to a variety of untrusted people*** • Account & device sharing w/ malicious relations • Attackers with knowledge of the individual • Varied types of untrusted relationships (e.g., friends, family, acquaintances, partners, people known during addiction)	• How to provide notifications about account access and sensitive actions • How to allow users to easily revoke undesired account access and ameliorate undesired actions when they occur (e.g., change password) • How to design for secure multi-user access to devices that may be shared (e.g., multi-account, guest accounts, hidden apps)
4. Ongoing stress	***Sources of stress*** • Ongoing, stressful life circumstances (e.g., financial, mental health, etc.) • Stress from tech use while lacking tech savviness • Stress arising from short or long-term S&P issues	• How to design S&P features for usability under chronic stress (e.g., easy reading levels, directed flows, automation where possible) • What secure defaults to chose for stressed, vulnerable users who might not make changes

Table 3: We provide a framework, with examples of how each *tough times* challenge (first column) can impact financially vulnerable users (second column), and sample design considerations that technology creators can think through as they create S&P features (third column).

to delete frequently used apps or valuable content. Similarly,

for users who desperately need low-cost housing leads, it may be difficult to give up even suspicious low-cost options. In many cases, reducing these types of costs or impacts can require users to carefully consider tradeoffs or be able to quickly find ways to fix issues. This may be particularly difficult for financially vulnerable users, as they might be stressed and overwhelmed. They may look to shelter workers or other resource providers for advice, but agency staff may not have this type of expertise [12].

Table 3 (col 3) provides sample considerations a designer can think through to support these challenges. For example, the technology community could help users seeking advice by considering how to create educational materials and training for shelter workers and other community resource providers (e.g., libraries, schools, etc.) on common scams and risks. Educating resource providers could help them advise people desperately looking for resources or who have fallen victim to scams.

Consider device and Internet setups

As demonstrated by our participants, it can also be important to consider users' varied device and Internet setups, in particular users with limited access to trusted devices and reliable personal Internet (see row 2 of Table 3).

To help provide these users with digital S&P, technology creators can draw from "bandwidth sensitive design" principles created for areas where limited data is more common (e.g., South Africa). Designers could help users make reasoned choices about data use by providing clearer indications of how much data is being used and when data might be running low [4]. Making these types of indicators easily available to users in regions where bandwidth limitations are less typical could help financially vulnerable users maintain access to trusted devices for online activities.

For security critical tasks, technology creators can also focus on designing features that work for users even absent reliable access to a personal device or phone number. For example, designers could "stress test" authentication methods by imagining how the system might work for a user who only has access to a public computer, suddenly loses access to their personal devices, or who loses access to their phone number. Designing a system with redundancy for these types of situations, and encouraging users to set up multiple recovery pathways (e.g., secondary emails, phones, etc.) could help users maintain access to accounts.

Consider ties to untrusted people

As our participants described, we also should consider how financially vulnerable users might need to interact with varied untrusted relations including untrusted friends, acquaintances, family members, and people from previous life stages (see row 3 of Table 3). To help account for these untrusted relations, technology creators can consider how to help users monitor accounts and devices that people who are untrusted might have access to, for example by providing notifications when sensitive or suspicious activities occur (e.g., after unusual account accesses, financial transactions, changes to account information, etc.). When it becomes apparent that someone is untrusted, either because of a life event (e.g., divorce, moving out of addiction) or after a notification, designers can focus on directing users to clear methods for revoking access to accounts and devices, and follow-up methods to minimize harm, for example by changing a password to revoke access to the account.

Because untrusted relations can be friends or family members who have physical access to devices, or with whom the user might share a device, either purposefully or accidentally, technology creators can also focus on designs that allow easy multi-user access to devices without full account sharing. Examples include allowing for multiple accounts or guest accounts on a device [19, 33]. Similarly, drawing insights from work in ICT4D environments, designers can focus on easily allowing users to hide or lock sensitive applications on mobile devices they might need to share [33].

Consider stress levels

Finally, our participants experienced chronic stress (see row 4 of Table 3), which can make even simple tasks harder. In the face of chronic stress, technology creators should consider how to make security critical tools, such as account hijacking flows or warnings, as usable as possible. Designers should focus on simple reading levels and, where possible, using highly directed or automated flows [5].

7 CONCLUSION

We found that four *tough times* challenges associated with financial insecurity impacted our participants' digital S&P practices and needs, specifically: (1) limited financial resources, (2) limited access to reliable devices and Internet, (3) untrusted relationships, and (4) ongoing stress. Technology creators can use our *tough times* framework to consider these challenges when designing S&P features, to offer a more inclusive set of options for users facing *tough times*.

8 ACKNOWLEDGEMENTS

We thank the many people at Google and the shelter organization for their support and ideas during this work, our reviewers for their insightful feedback, and, most importantly, our participants for sharing their experiences.

REFERENCES

[1] Monica Anderson. 2017. Digital divide persists even as lower-income Americans make gains in tech adoption. *Pew Research Center* (2017).

[2] Kimberly Bender, Stephanie Begun, Anne DePrince, Badiah Haffejee, and Sarah Kaufmann. 2014. Utilizing technology for longitudinal

communication with homeless youth. *Social Work in Health Care* 53, 9 (2014), 865–882.

[3] Stevie Chancellor and Scott Counts. 2018. Measuring employment demand using internet search data. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 122.

[4] Marshini Chetty, Richard Banks, AJ Brush, Jonathan Donner, and Rebecca Grinter. 2012. You're capped: Understanding the effects of bandwidth caps on broadband use in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3021–3030.

[5] Lorrie Faith Cranor. 2008. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. USENIX, 1.

[6] Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and usability: Designing secure systems that people can use*. O'Reilly Media.

[7] Tawanna R Dillahunt, Nishan Bose, Suleman Diwan, and Asha Chen-Phang. 2016. Designing for disadvantaged job seekers: Insights from early investigations. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, 905–910.

[8] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interacting with Computers* 23, 5 (2011), 413–421.

[9] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*. ACM, 83–94.

[10] Karin M Eyrich-Garg. 2011. Sheltered in cyberspace? Computer use among the unsheltered 'street' homeless. *Computers in Human Behavior* 27, 1 (2011), 296–303.

[11] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 667.

[12] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 46.

[13] Carol Graham. 2000. The High Costs of Being Poor in America: Stress, Pain, and Worry. *Brookings Institution Social Mobility Memo* (2000).

[14] Anne E Green, Yuxin Li, David Owen, and Maria De Hoyos. 2012. Inequalities in use of the Internet for job search: Similarities and contrasts by economic status in Great Britain. *Environment and Planning A* 44, 10 (2012), 2344–2358.

[15] Rosanna E Guadagno, Nicole L Muscanell, and David E Pollio. 2013. The homeless use Facebook?! Similarities of social network use between college students and homeless young adults. *Computers in Human Behavior* 29, 1 (2013), 86–89.

[16] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one can hack my mind": Comparing expert and non-expert security practices.. In *Proceedings of the Symposium on Usable Privacy and Security*, Vol. 15. USENIX, 1–20.

[17] Kathleen M Kowalski-Trakofler, Charles Vaught, and Ted Scharf. 2003. Judgment and decision making under stress: An overview for emergency managers. *International Journal of Emergency Management* 1, 3 (2003), 278–289.

[18] Christopher A Le Dantec. 2008. Life at the margins: Assessing the role of technology for the urban homeless. *Interactions* 15, 5 (2008), 24–27.

[19] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. She'll just grab any device that's closer: A study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 5921–5932.

[20] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.

[21] Board of Governors of the Federal Reserve System. 2017. Report on the Economic Well-Being of U.S. Households in 2017.

[22] Affordable Housing Online. 2018. Don't Become a Victim! Learn how to identify common online rental housing scams. https://affordablehousingonline.com/housing-scam-prevention-guide

[23] David E Pollio, D Scott Batey, Kimberly Bender, Kristin Ferguson, and Sanna Thompson. 2013. Technology use among emerging adult homeless in two US cities. *Social work* 58, 2 (2013), 173–175.

[24] Lori Ann Post, Federico E Vaca, Kelly M Doran, Cali Luco, Matthew Naftilan, James Dziura, Cynthia Brandt, Steven Bernstein, Liudvikas Jagminas, and Gail D'Onofrio. 2013. New media use by patients who are homeless: The potential of mHealth to build connectivity. *Journal of Medical Internet Research* 15, 9 (2013).

[25] Alison Powell, Amelia Bryne, and Dharma Dailey. 2010. The essential Internet: Digital exclusion in low-income American communities. *Policy & Internet* 2, 2 (2010), 161–192.

[26] Elissa M Redmiles. 2018. Net benefits: Digital inequities in social capital, privacy preservation, and digital parenting practices of US social media users. In *Twelfth International AAAI Conference on Web and Social Media*. AAAI.

[27] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide?: A survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 931–936.

[28] Eric Rice and Anamika Barman-Adhikari. 2014. Internet and social media use as a resource among homeless youth. *Journal of Computer-Mediated Communication* 19, 2 (2014), 232–247.

[29] Eric Rice, Seth Kurzban, and Diana Ray. 2012. Homeless but connected: The role of heterogeneous social network ties and social networking technology in the mental health outcomes of street-living adolescents. *Community Mental Health Journal* 48, 6 (2012), 692–698.

[30] Eric Rice, Alex Lee, and Sean Taitt. 2011. Cell phone use among homeless youth: Potential for new health interventions and research. *Journal of Urban Health* 88, 6 (2011), 1175–1182.

[31] Eric Rice, Norweeta G Milburn, and Mary Jane Rotheram-Borus. 2007. Pro-social and problematic social network influences on HIV/AIDS risk behaviours among newly homeless youth in Los Angeles. *AIDS Care* 19, 5 (2007), 697–704.

[32] Jahmeilah Roberson and Bonnie Nardi. 2010. Survival needs and social inclusion: Technology use among the homeless. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*. ACM, 445–448.

[33] Nithya Sambasivan, Garen Checkley, Amna Batool, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in South Asia. In *Proceedings of the Symposium on Usable Privacy and Security*. USENIX.

[34] Jennifer Sheehy-Skeffington and Jessica Rea. 2017. *How Poverty Affects People's Decision-making Processes*. Joseph Rowntree Foundation York.

[35] Aaron Smith. 2015. Searching for work in the digital era. *Pew Research Center* 19 (2015).

[36] Tony Sparks. 2010. Broke not broken: Rights, privacy, and homelessness in Seattle. *Urban Geography* 31, 6 (2010), 842–862.

[37] Sanna J Thompson, David E Pollio, Karin Eyrich, Emily Bradbury, and Carol S North. 2004. Successfully exiting homelessness: Experiences of formerly homeless mentally ill individuals. *Evaluation and Program Planning* 27, 4 (2004), 423–431.

[38] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. ACM, 25.

[39] Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith Cranor. 2011. I regretted the minute I pressed share: A qualitative study of regrets on Facebook. In *Proceedings of the Symposium on Usable Privacy and Security*. ACM, 10.

[40] Rick Wash and Molly M Cooper. 2018. Who provides phishing training?: Facts, stories, and people like me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 492.

[41] Earnest Wheeler and Tawanna R Dillahunt. 2018. Navigating the job search as a low-resourced job seeker. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 48.

[42] Jill Palzkill Woelfer. 2014. Engaging homeless young people in HCI research. *Interactions* 21, 1 (2014), 54–57.

[43] Jill Palzkill Woelfer and David G Hendry. 2010. Homeless young people's experiences with information systems: Life and work in a community technology center. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010). ACM, 1291–1300.

[44] Jill Palzkill Woelfer and David G Hendry. 2011. Designing ubiquitous information systems for a community of homeless young people: Precaution and a way forward. *Personal and Ubiquitous Computing* 15, 6 (2011), 565–573.

[45] Jill Palzkill Woelfer and David G Hendry. 2012. Homeless young people on social network sites. In *Proceedings of the 2012 CHI Conference on Human Factors in Computing Systems*. ACM, 2825–2834.

[46] Jill Palzkill Woelfer, Amy Iverson, David G Hendry, Batya Friedman, and Brian T Gill. 2011. Improving the safety of homeless young people with mobile phones: Values, form and function. In *Proceedings of the 2011 CHI Conference on Human Factors in Computing Systems*. ACM, 1707–1716.

[47] Sarita Yardi and Amy Bruckman. 2012. Income, race, and class: Exploring socioeconomic differences in family technology use. In *Proceedings of the 2012 CHI Conference on Human Factors in Computing Systems*. ACM, 3041–3050.