Experiences with Digital Scams Post-Incarceration in the U.S.

Yael Eiger
University of Washington

Candice Baughman
Interaction Transition

Rory Andes
Communities of Belonging

Bryan Glant
Project Rise

Franziska Roesner
University of Washington

Abstract

When people are released from prison in the United States, they reenter into a highly digitized world that they have little to no experience with or preparation for. This lack of experience makes them potentially vulnerable to digital scams and phishing attempts upon release. Towards addressing this digital divide, we ran a workshop to teach and learn about digital security and privacy needs unique to the formerly incarcerated community (in our area of the U.S.). At this workshop, we deployed a survey to both participants (N=20) and volunteers (N=12). We later followed up with a more targeted survey specifically asking about scams and scam susceptibility among formerly incarcerated people (N=20, 4 of whom also attend the workshop). We additionally include personal narratives from three formerly incarcerated researchers (co-authors on the paper) about their experiences with scams. Combining all of this data (N=48 unique respondents), we find that scam exposure and victimization in this community is common, and we document a variety of risk factors: digital literacy challenges, heightened coercive potential of scams which purport to be from law enforcement or governmental bodies, loneliness during incarceration, financial instability post-incarceration, and a fear of stigmatization and repercussions from reporting. At the same time, we find that participants recount some mitigating factors, including belonging to a community that faces common challenges and therefore builds strong community networks to turn to for help. We close by identify gaps between best practices to avoid scam victimization and the realities of being currently or formerly incarcerated in the U.S., and making recommendations.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

1 Introduction

Each year in the United States, more than half a million people are released from prison [5]. One difficult aspect of this reentry process is adapting to a digital world which may have changed drastically over the course of someone's incarceration, while they had little to no digital access to learn and prepare. Prior work has described the impacts of this immense learning curve for formerly incarcerated people, particularly when digital skills are necessary to secure employment, housing, and social services post-release [3, 45, 78, 92, 99, 101, 102, 114, 115, 121].

People reentering society post-incarceration also struggle with widespread information exposure [52] which may increase scam targeting. For example, currently and formerly incarcerated people's history, demographics, address, and phone number are largely available via public lookup tools (plus some run by private companies [120, 138, 142]), and their medical records, case histories, financial data, and communications are subject to public records requests [52, 58, 97, 137]. Some formerly incarcerated people are also court-mandated to supply personally identifying information (e.g fingerprints, ID, address, employment, phone number, family, relationships, whereabouts) to public registries [31, 42, 98].

Previously unexplored in research (to our knowledge) is how this digital divide and sensitive information exposure impacts scam susceptibility and targeting. Thus, this work investigates:

- **RQ1:** What are the **experiences** of people released from incarceration in the U.S. with respect to scams?
- **RQ2:** What **unique aspects of incarceration and post-incarceration life** impact scam susceptibility, reporting, and remediation?

This paper is a collaboration between two computer security researchers at an academic institution and three formerly-incarcerated researchers and community members in our area. To answer our research questions, we combine four sources of data that we collected from formerly incarcerated people in our geographic area of the U.S.

Specifically, we deployed a survey related to technology and digital privacy for formerly incarcerated people (N=20) at a workshop we ran to learn and teach about digital security and privacy with people reentering society. Volunteers at the workshop also provided individualized technology help to reentrants, and these volunteers were surveyed about the technology challenges and needs they assisted with (N=12). After the workshop, we conducted a follow-up survey with formerly incarcerated people specifically related to scams (N=20, 4 of whom also attended and responded to the workshop survey). We combine these results with personal narratives of three formerly incarcerated (co-author) researchers.

Overall, we find that falling for a scam was relatively common among our participants. Participants felt that they received more scams – and were more susceptible to them – when they had only recently been released from prison. Moreover, these scams are experienced in the context of a habitual lack of privacy: participants felt a desire for digital privacy that they did not have access to, in part due to court-mandated reporting requirements and broader surveillance.

Participants confirmed that digital skills gaps play a large role in scam susceptibility, especially if they were incarcerated for much of the 21st century. We also heard that scams impersonating the government and threatening criminal or legal action were perceived as particularly coercive. Moreover, financial instability caused by incarceration [18,62,139] played role in the curiosity of our participants towards job-related scams or "get rich quick" schemes. Despite these struggles, our participants also felt a sense of confidence in identifying misleading and manipulative behavior, and were successful at building and utilizing close family and friend networks to support them in navigating these challenges.

Based on our findings, we highlight gaps in common best practices for scam avoidance and the realities of reentering society as a formerly incarcerated person, including gaps in education and technical interventions, fear of reporting, and the inability to protect one's privacy as much as desired. We conclude with lessons for future privacy and scam-related workshops and recommendations for the research community to close these gaps.

2 Related Work

2.1 Scams & Susceptibility

Previous work has characterized specific scams/attack vectors [2,12,28,53,57,67,71,72,76,81,89,91,94,95,123,136,149], and specific educational [27,43,69,113,119,144] or technical tools [16, 75, 91, 109, 124, 152] for scam prevention. Prior scam research has also studied specific communities' susceptibility [25,48,125] including children [13,70,105,153], multilingual people [127], people who are blind/low vision [66] and elderly adults [20,105,151,153], and found that, for every population, across multiple scam surfaces and vectors, technical prevention tools and education were helpful but not a panacea, and must be joined by other holistic, context- and community-specific methods. We expand on how this literature applies to formerly incarcerated people in Section 5.1. Past research on scams has not (to our knowledge) studied the experiences or susceptibility of people who have been incarcerated; moreover, the recommended technical and educational interventions are currently, to our knowledge, not available to incarcerated people in the U.S.

2.2 Digital Literacy & Incarceration

Prior work has discussed the lack of technology and technology education in prisons and the impact this has on digital literacy, job, and housing search [3, 50, 99, 100, 102]. For example, Reisdorf et al. [114, 115] highlighted the scarcity of computer literacy programs in U.S. prisons, noting that even existing programs rarely cover essential skills like navigating the internet. To rectify this digital literacy gap, some recent HCI papers have proposed applications and workshops for incarcerated people to learn digital skills like coding and virtual reality [46, 79, 93].

Prior work on digital technologies in a reentry context has also shown that privacy concerns often lead formerly incarcerated people to avoid or limit their engagement with digital technologies, and many people cite surveillance concerns in particular [52,101,107]. Seo et al. [121] examine women transitioning from incarceration and note that post-incarceration discomfort with the internet often stems from its association with the surveillance they experienced in prison. As such, online privacy concerns often make people, in particular under served populations, hesitant to acquire new skills and engage with technology [122].

In this paper, we confirm the findings of prior work regarding the hindrances to digital literacy for incarcerated people and the impact when they re-enter an increasingly digitized society. We extend these findings by investigating how this digital divide affects scams in particular, both scams that are explicitly targeted towards formerly incarcerated people, or more generic scams which they may be more susceptible to.

2.3 Digital Privacy for Vulnerable Groups

Prior work explored security and privacy risks for marginalized and/or vulnerable groups [8, 11] such as refugees and migrants [51, 126, 134], as well as journalists [85, 86]. Prior work has also focused on victims of interpersonal violence (IPV) and stalking, including orgainzing workshops and clinics to aid these issues [7,24,44,135]. Prior work by Owens et al. has explored security and privacy issues, like surveillance, of formerly incarcerated people and migrants [106–108]. We strengthen these findings (e.g. electronic monitoring stress), but build on them by contributing an understanding of scam experiences and susceptibility post-release.

3 Methods

To answer our research questions, we combined several methods for the collection of different types of data.

3.1 Post-Incarceration Workshop

In collaboration with local community groups led by and in advocacy of formerly incarcerated people, we co-designed an in-person workshop related to digital literacy and digital privacy. It was called "Computer Basics for Reentry" and involved 20 minute presentations in parallel with 1:1 technology help by volunteers staffed to answer personalized questions. The presentations included information related to resume creation, finding job opportunities, how to set up and navigate email inboxes, identify scams, and implement online privacy tips (e.g. password management). These topics were chosen by the team of collaborating community organizers and researchers to maximize the pairings of expertise with community needs. The 1:1 volunteers were available to answer personalized technology questions for individual attendees. The workshop took place in a conveniently located local church, and attendees of the workshop were given catered lunch, beverages, a $35 Walmart gift card for attending, and reimbursement for any travel costs to the workshop. We also had a few other community groups present at the workshop, including a group to help enroll formerly incarcerated people in college courses, and subsidized social services in our city.

3.2 Surveys

Participants of the workshop were asked to fill out a survey while they were there related to computer access, education, scams, and how to improve subsequent workshops (N=20). We also asked the 1:1 volunteers to fill out a survey about the technology questions and needs they were assisting with, and how to improve subsequent workshops (N=12).

To learn more about scam susceptibility specifically, we then co-designed another survey, this time more directly related to scams and scam education during incarceration, that was sent out to the community networks of our local community partners. We received N=20 responses to this survey, 4 of whom also attended the workshop and are included in the sample size of the workshop survey, and 16 new respondents. As compensation for this follow-up survey, we held a raffle of five Walmart gift cards ($35).

We acknowledge two survey design limitations: (1) We did not ask about the details regarding incarceration history and technology usage in the follow up survey; (2) Question 2 of our follow-up survey read "Have you ever fallen for or experienced a scam?" which means that unless the survey taker responded to later questions about the specific scams they have fallen for, we are unable to differentiate "experiencing" versus "falling for" a scam.

3.3 Personal Narratives

Inspired by autoethnography work [22, 26, 33, 38, 40, 54, 64, 65, 77, 104, 110, 130, 131, 148], we combined our survey data with personal narratives from three formerly incarcerated researchers. We chose to do so because we concur with prior work in HCI that considers this method an impactful research tool for "producing meaningful, accessible, and evocative research grounded in personal experience, research that would sensitize readers ... to experiences shrouded in silence, and to forms of representation that deepen our capacity to empathize with people who are different from us." [38]. Concretely, as technologists intending to improve digital systems, we also agree with Cunningham et al [33], and Hughes et al [55], that autoethnography can help system designers understand "user behavior as it actually exists, rather than idealized pictures of how the user 'ought' to approach a task." In the same vein, HCI researchers have described autoethnography as "allow[ing] practitioners to capture some of the subtleties and nuances of the contexts that can influence the adoption and use of a device not easily achieved without experiencing them" [104]. This methodological choice reflects a belief in what social scientists refer to as "standpoint theory" [128].

Specifically, three formerly incarcerated researchers wrote a personal narrative detailing their experience with digital scams during their reentry transition (provided in Appendix A). The co-authors who did not write the personal narratives then qualitatively coded these them as data alongside the collated survey data (which all authors analyzed), and iteratively refined the codebook to synthesize themes across all three surveys and the personal narrativves.

3.4 Data Analysis

In line with prior qualitative work, authors used a collaborative, qualitative open coding technique [133], where four researchers (including the three formerly incarcerated co-authors) separately examined both the participant and volunteer survey data from the workshop and drew up initial codes. These codes were then combined and further refined collaboratively in discussions among the authors. This led to the creation of codebooks for both the participant surveys and volunteer surveys. We then analyzed the union of this data and combined it into a single codebook (see Appendix C).

Based on these findings, we wanted to further investigate scam experiences, susceptibility, and reporting, and thus ran our follow-up survey. Based on the results of the follow-up survey, co-authors used the same open-coding techniques to create a codebook (see Appendix C.

We used inductive thematic analysis [15] to uncover overarching themes and identify the union of the separate codebooks through open discussion among all researchers. This was then analyzed to identify overlaps with the autoethnographies (the co-authors who wrote the personal narratives did not code the

personal narratives; they were coded by the remaining two authors who did not write personal narratives). These overlaps were identified by the lead author, who did not write a personal narrative and does not belong to the population under study. This process resulted in our final themes in Table 1.

3.5 Positionality

In line with the lessons from social science and standpoint theory [128], we believe that as authors and researchers we are not inherently objective. In fact, we believe that our positionality can enhance our ability to interpret and analyze the data we collect (this is part of the reason we chose to add personal narratives). Because of this subjectivity, we believe it is important to disclose our motivations and positionality in this work, and be upfront about the unique perspectives we are bringing to the research.

This research team is made up of three formerly incarcerated researchers, and two researchers who are not formerly incarcerated but who have experience in the computer security and privacy research community. Many of the authors have spent years teaching in prisons and community organizing for educational access and other rights for incarcerated people. The authors come from a diverse range of educational, geographic, and socioeconomic backgrounds. They were all motivated to do this research to explore the security and privacy needs of currently and formerly incarcerated people, an often underserved and overlooked group. We believe that community-engaged and community-driven research is ultimately the best path forward to create better research, and to create better societal impact for our research.

3.6 Ethical Considerations

Given the sensitive nature of incarceration history (including trauma), we took great care to ensure this research was conducted ethically. All of our research activities were approved by our institutional IRB, and we took the following steps:

Together with community members, we decided upon the best compensation package to balance the needs of formerly incarcerated people with the needs of research best practices (i.e., not compensating too much or too little to influence the self-selection or confirmation bias of certain groups and responses) — this resulted in a $35 Walmart gift card. We believe that our surveys gave the participants a chance to articulate their experiences without causing any trauma from re-telling, etc. We also believe that the educational access and technology help available at the workshop was a positive tradeoff for participants. There have been calls for us to organize another workshop, from both participants and volunteers, and we are planning the next one currently.

We did not collect name or demographic information with either survey. We acknowledge the limitation in being unable to analyze our data according to demographic measures, but chose to prioritize privacy given the sensitive nature of data regarding incarceration history. We included a question on the follow-up survey asking if the respondent attended our workshop. As such, we know that 4 participants in the follow-up survey attended the workshop, and thus overlap with the workshop survey participants, but we don't know *which* participants these are.

We protected the respondents' privacy by keeping all data in access-controlled directories only accessible to the research team. We explained the research process and privacy considerations, and left space for questions/concerns both in the surveys and in person at the workshop.

For volunteers and presenters, we held a training and orientation prior to the workshop to review best practices for trauma-informed engagement and research, as well as guidance on respectfully socializing and interacting with formerly incarcerated individuals, recognizing the unique life circumstances and experiences they may carry. Throughout this process, we partnered with professionals in the field (of reentry) to further ensure the workshop and subsequent survey were a positive experience. We believe the workshop was a safe, happy, and positive environment for all present, but we also took preventative steps to plan for the alternative: we had certified peer support specialists and reentry specialists present for any deescalation, emotional, or individual needs (these services were offered but not used). Since this research was conducted, we have continued to nourish these community and collaboration partnerships.

4 Findings

We now turn to our findings, drawing on all of our data sources to support our conclusions. We first report on general experiences with scams and digital privacy among our participants and co-authors (Section 4.1), then discuss the risk factors for formerly incarcerated people with respect to scams (Section 4.2), and finally highlight several mitigating factors that may reduce risk (Section 4.3). Table 1 summarizes the themes that we distilled from our data.

We refer to workshop survey respondents as P1 ... P20. We refer to our volunteers at the workshop as V1 ... V12. We refer to the respondents to our scam follow-up survey as SF1 ... SF20. When a follow-up survey respondent also attended the workshop, we add a * to their designation (e.g., SF9*). We refer to our autoethnographic narratives as A1 ... A3.

4.1 Experiences with Scams and Privacy

We begin by reporting on our participants' experiences with scams, as well as their experiences with digital privacy in general post-release (answering RQ1).

Respondents mentioned...	Workshop survey (N=20)	Volunteer survey (N=12)	Follow-up survey (N=20, 16 unique)	Auto-ethnography (N=3)
Experiences:				
Experienced a scam	12	-	13	3
Experienced government scam	-	-	7	2
Experienced relationship scam	-	-	5	1
Experienced job scam	4	-	8	-
Phone/internet monitoring post-release	4	1	-	2
Risk Factors:				
Digital skills gap	17	11	4	-
No digital educational opportunities	8	-	2	-
Outdated or restricted digital educational opportunities	5	-	-	-
Flurry of new credentials	-	2	-	-
Fell for relationships scam due to loneliness	-	-	2 (of 5)	1 (of 1)
Fell for job scam due to financial need	-	-	2 (of 8)	-
Didn't report / so as not to interact with law enforcement	-	-	11 / 5	-
Mitigating Factors:				
Close relationships	8	-	-	1
Confidence due to life experiences	-	-	11	-

Table 1: **Findings Summary.** This table summarizes the themes in our findings, and reports on the number of respondents in each survey who mentioned the theme listed in the first column. These numbers are a **lower bound**, limited by what we asked and what was explicitly, verbatim, mentioned in the survey responses; we did not specifically ask about each theme in each survey. For example, we asked about specific scams (e.g., government, relationship, job) and risk factors in the follow-up survey, but not in the workshop survey or the volunteer survey. We emphasize that this work is largely qualitative, and we do not intend the numbers to be read as generalizing to a broader population or even representing all of our participants' experiences; instead, we aim to give the reader a sense of our codebook and data.

4.1.1 Experiences with scams were common

As such, our follow-up survey specifically focused on scams and scam suceptibility. Thirteen out of 20 respondents reported that they had experienced and/or fell for a scam. Seven out of 20 reported that they had experienced and/or fell for a scam claiming to be from the government, authorities, law enforcement, a judge, etc, and eight out of 20 reported that they had received a scam which threatened arrest, fines, warrants, or other legal punishment if they did not comply. Five of 20 said they had experienced and/or fell for a scam claiming to want a sexual or romantic relationship, and eight out of 20 had experienced and/or fell for a scam claiming to offer a job or financial opportunity.[1]

Participants mentioned that they felt more susceptible to scams, and more frequently a target of scams, when they had only recently been released from prison. One participant at the workshop said that they "fell for a couple scams at first, had to cancel my bank card several times in last 2 years" (P3).

When asked how frequently they receive scams, one participant said "Not as often as I did when I was first released into the community" (SF5). Another participant articulated a similar chronology, where they experienced more scams early on in their reentry transition: "The first 3-4 months after release, I had 4-5 FTR [Failure to Register] scams [2] that contacted both myself and multiple members of my family, threatening them as well if they didn't help them. I haven't heard from any for several months now" (SF7).

In response to the question about scam frequency, participants additionally responded that they receive scams in a range from daily (SF1), weekly (SF6*, SF12, SF13, SF17), to monthly (SF3, SF8, SF10, SF11) as well as "occasionally" (SF9*), "lots" (SF14), and "frequently" (SF16).

In our workshop survey, 12 participants answered yes to the question "Do you ever get unsolicited phone calls, texts, or emails, from sources you don't know or trust? Do they ever ask for money or personal information?" And in response to the question "What do the calls/texts/emails try to convince you of?", participants reported "they'll get me to do something on my computer that sets off an alarm + freeze my screen, and try to get me to buy gift cards for payments" (P3), "send funds/money" (P5, P16), "I've got a great job opportunity LOL" (P7), "free money, qualifying" (P9), "mostly to provide

[1] We caution that these numbers emerged from qualitative work, not nationally representative measurements or surveys, and that it is also possible, for instance, that formerly incarcerated people who have fallen for a scam were potentially more likely to take a survey related to scam experiences.

[2] An example of this scam was released by one state's Bureau of Investigation [96], warning formerly incarcerated people who have been convicted of sex related offenses about a Failure to Register scam. In this scam "the scammer uses a specific officer's name associated with a specific law enforcement agency, which in many cases is the name of a real officer... The caller then informs the registered sex offender that they are non-compliant with their registration requirements and will be arrested or a warrant will be issued if they fail to pay a specific fine." In addition to money, the scammer sometimes requests forms to be faxed to them that has "all of their personal information ... and a DNA swab...[if they do not] a warrant will be issued for their arrest."

personal information" (P11), "buying insurance" (P18). One participant mentioned that these solicitations "are all scams" (P16), and another said that "since the day I bought my phone, soliciters have called" (P18).

After describing a scam that they fell for, A2 describes how "this happens to so many people coming home. We don't always know what's real, what's required, or who to ask. And scammers know that fear is loud."

4.1.2 Broader privacy concerns

Scams are experienced in the context of broader concerns and vulnerabilities with respect to digital privacy, which we discuss in this subsection. Indeed, our initial workshop was framed broadly as "Computer Basics for Re-Entry" and our initial survey questions were more broadly about technology and privacy (our focus on scams in this paper came out of the data, in which scams were prevalent).

Workshop participants were broadly worried about digital privacy and how to protect it. When asked, "Do you have any worries when using technology?" they mentioned: "scams + inexperience" (P3), "yes, got my identity stolen" (P1), "controlling my footprint and information" (P11), "scams" (P20), and "data breaches, password management" (P19).

When workshop participants were asked who they were worried about having access to their information, they reported "anybody" (P1), "hackers" (P2, P20), "scam artists" / "scammers" (P3, P7), "law enforcement"/DOC/"the government" (P1, P5, P13). One participant said that they were worried about "AI" accessing information about them (P16).

One participant in the workshop mentioned that one of the most surprising things to them when they were released compared to when they entered prison was "how much privacy [the] public has abandoned" during that time period, and gave an example of how commonplace/expected "allowing integrated sources (e.g., Samsung + Google on phone) permissions" had become (P10).

Ultimately, participants had many worries about their digital privacy beyond scams, with a recognition of the privacy vulnerabilities which come from the now-ubiquitous mobile phones that they previously did not need.

4.1.3 Shameware and mandated Electronic Monitoring

When we asked participants about who might have access to their personal information currently, multiple participants mentioned that their Community Corrections Officer (CCO) monitors the entirety of their internet, computer, and mobile phone usage. This compliance is court-mandated and participants face re-arrest if they do not comply.

In additional to post-incarceration electronic monitoring apps [106], this surveillance may take the form of mandated "shameware" [87] apps like Accountable2You [1], EverAccountable [39], and CovenantEyes [32], which some formerly incarcerated people must install on their personal devices. These apps are created by religious organizations and marketed around "accountability" for users to help them "Quit Porn" [1, 39, 82, 87] but for formerly incarcerated people with sex-related convictions, they are court mandated. To use these apps, a subject must grant root certificate and VPN access on their phone. These apps then monitor all network traffic, take screenshots of all activity (including messages, banking, password managers, doctors' portals, and other sensitive information), and send automated reports to the CCO about their internet usage and behavior. These apps also send automated reports to the CCO if the app detects an "infraction" during internet use — for example, if someone tries to download social media when their release conditions forbid it (common for people with sex-related convictions).

This monitoring was identified by a volunteer (V3) when answering questions for a participant about how to use Google Maps in a way that would satisfy their CCO reporting requirements (for instance, the need to share an ETA which includes unforeseen traffic, because missing a meeting due to traffic may constitute a custody violation).

Beyond mandated apps installed by the CCO, one participant said that their monitoring simply takes the form of: "my CCO goes through my phone" (P18).

One participant articulated the fear and distrust this monitoring amplifies in them: that "DOC monitors all [my] device usage. 80% of [my] mental bandwidth is spent hesitating, wondering how DOC will frame usage or interfere." (P19) The fear of monitoring wasn't due to actual infractions being discovered, but how DOC will "frame" benign usage, and how this misrepresentation would penalize them and further revoke the limited access they do have to the internet.

For the author of Personal Narratives 3, this fear of misrepresentation has a direct relationship with their likelihood to comply with a scam: "Authority will have a different or jaded view of something I'm doing while free... Not that I've done anything wrong, but anything can be misconstrued, and that's where the danger of the scams really does come in" (A3).

4.2 Risk Factors and Challenges

We now turn to risk factors and other challenges that our participants reported increasing their susceptibility to scams or hinder their ability to report or respond (answering RQ2). These themes are also summarized in Table 1.

4.2.1 A digital skills gap plays a large role

Confirming prior work [99–101, 103, 114, 121], we confirm that formerly incarcerated people face an uphill battle when adapting to a world filled with digital tools that they have little to no experience with. Table 2 summarizes our workshop participants, highlighting the length of their incarceration and the new technologies they were confronted with after release.

	Which years were you incarcerated?	What technology did you use regularly before you were incarcerated?	What technology do you use regularly now?
P1	7 years	Phone, iPod	*Smartphone now* with these class computers
P2	1994 - 2023 (29 Years)	Landline, phone	*iPhone*
P3	1990 - 2022 (32 years)	Landline	*Laptop, cell phone* - but not to their full abilities
P4	2012, 2011, 2020 - 2024 (4 years)	Cell phones, computers	Cell phones, computers
P5	1998 - 2025 (27 years)	Pager	*iPhone X, laptop!*
P6	2015 - 2018 (3 years)	Phone, computer, iPod, iPhone	Computer
P7	-	-	-
P8	2021 - 2025 (4 years)	Cell phone	Cell phone
P9	2004 - 2025 (21 years)	There weren't smartphones. Camera phones were becoming popular	*Smartphone, iPhone/Macbook.* I consider myself tech savvy and can quickly learn or adapt.
P10	2018 - 2025 (7 years)	All of it.	All of it.
P11	1989 - 2023 (34 years)	Landline telephone	*Laptops, PC, desktop, smart phone*
P12	2023 - 2025 (2 years)	Cell phone	
P13	2015 - 2025 (10 years)	Phone, computer	Phone
P14	1986 - 2025 on and off	Cell phone, computer	Cell phone
P15	2017 - 2018, 2024 - 2025 (2 years)	Landline, cell phone, computer, iPod	*Chat GPT*
P16	2000 - 2003, 2004 - 2015, 2016 - 2019, 2019 - 2020, 2023 - 2025 (21 years)	Landline, AOL	*Cell phone*
P17	2017 - 2025 (7 years)	Computer, Android phone	*iPhone, iPad*
P18	2012, 2013, 2014, 2016, 2017, 2020, 2021, 2022, 2023 (9 years)	Cell phone	*iPhone, laptop*
P19	2018 - 2025 (6 years)	Cell phone, computer (laptop + gaming desktop)	Laptop, *smartphone*
P20	2014, 2017 - 2018, 2019, 2023 (5 years)	Landline telephone, cell phone, computer, iPod, iPhone	Landline telephone, cell phone, computer, iPod, iPhone

Table 2: **Workshop Participants.** This table reports workshop participants' verbatim survey responses about when they were incarcerated, what technology they used regularly before incarceration, and what technology they regularly use now, post-incarceration. Highlighted in blue and in parentheses are the number of years the participant was incarcerated. Highlighted in red and underlined are technologies used only before incarceration (not now). Highlighted in *green* and italicized are technologies that they use now, but not before incarceration.

One participant in our workshop said that "at almost 3 years out, I'm still not proficient" (P3). This has a grave impact when digital literacy is needed to apply for jobs, housing, and social services. We hypothesize that this is why so many participants asked for help with these issues: applying for jobs, scholarship, creating resumes, and sending emails, as we discuss in Section 4.3.3 and Section 5.

Digital literacy is also required to comply with some release requirements and court-mandated electronic monitoring via smartphone app (as described in Section 4.1.2 and prior work [106]). Participants in our workshop also expressed that the most difficult changes in society to adapt to post-release included "getting used to the fact that everything includes technology" (P17), "the chronic need for a cell phone" (P11), and that now "everythings on the web" (P10).

In addition to already well-documented impacts of digital literacy gaps for formerly incarcerated people (Section 2.2), this issue can also increase scam susceptibility. One survey respondent articulated that "Digital and technological illiteracy definitely has a huge influence on those who 'fall' for scams post incarceration" (SF7).

The volunteers at the workshop assisted participants with several digital skills that may have an impact on scam susceptibility and identification. For example, one volunteer mentioned that the person they were assisting "had many apps installed on their phone that it seemed like they did not install themselves" and that they "didn't understand how apps showed up on their phone - whether they were first-party on Android, first-party from their hardware provider, first-party from their carrier, or third-party. They also had some alt app stores installed" (V9). This is particularly concerning given that recent scams have specifically directed victims to down-

load a malicious app [36] which may contain malware [83], as can apps installed via alternative/third party app stores [90].

A related digital skill which may impact scam susceptibility, especially if the scam is presented through ads or popups, is identifying and navigating UI elements on a webpage. One volunteer said that "It seemed like the participant was struggling with 'vertical depth' in UIs... where you can scroll, what a button is, etc" (V9). Indeed, one respondent in our follow-up survey fell for a scam like this: "The one scam I fell for was installing Fire Stick on my phone. In the install app it had a click here to install - that was an ad/scam" (SF20).

Participants also had trouble filtering through spam and scams in a crowded inbox. One volunteer described how a participant "had been put on several listservs that sent out multiple emails every day (e.g., package delivery notifications, utility payments, public services, etc.) that distracted them, and drowned out the messages that they did want to see" (V11). To sort through this noise filled with potential junk, spam, and scam emails, together the volunteer and participant "walked through how to unsubscribe from email lists, how to block specific addresses, and how to create filters in their email inbox that could help declutter their inbox" (V11).

Teaching these digital skills may not be a complete solution for preventing scams, but the ability to sort through popups without clicking on them, close windows and tabs, avoid downloading apps unintentionally, and create spam filters in an inbox helps to ensure that someone is navigating through the internet that they want to see.

4.2.2 Limited educational opportunities and technology exposure while incarcerated

The digital literacy gap is due in part to limited technology educational opportunities while incarcerated. None of our participants received education about scams in particular during their incarceration, and even general technology exposure (let alone education) was limited: eight out of 21 workshop participants reported that they had *no* access to any computers, computer skills, or computer education while incarcerated. For the nine workshop participants who reported that they did have computer access, this access was available solely because they were enrolled in education courses (mostly at their own expense), for which only a small fraction of incarcerated people are eligible [29, 88, 111, 118, 129, 145]. One participant summed up computer education as "anemic and sporadic but it existed" (P11). Despite this, they add that "One of the biggest problems of being release[d] from prison is that little to nothing is done or allowed to prepare for release. Especially with regard to technology" (P11).

Additionally, the little computer access they did have was outdated. Despite being incarcerated until 2022, one participant said the only computer access they had was on Windows 95 (P3). Another said they only had "little [access], windows, word access, powerpoint, excel" (P6).

One participant mentioned that the most difficult adaptation post-release was how "the world has become very 'mobile-first' which is a big mindset shift" (P19). Despite this global shift away from desktop/laptop computers and towards smart phones, no participant had access to a mobile phone or mobile phone education while incarcerated, yet the introduction of mobile phones (particularly smart phones) into the lives of our participants post-release was common (see Table 2). This dearth of education for the most commonly used tools upon release is also true of internet access and web browsing.

More broadly, and also observable in Table 2, was that participants were familiar with many technologies before they were incarcerated that they no longer use or are now obsolete (e.g. pagers, AOL messenger). And vice versa, they now use many technologies which were completely new to them upon release (e.g. ChatGPT, iPhones). Computers were the only technology which people could learn to use while incarcerated. Thus, the rest of these technologies had to be mastered once they had already reentered society. Thus, people need to try to detect and avoid scams at the same time as familiarizing themselves with device form factors, UX conventions, and in an abundance that they do not have prior experience with.

4.2.3 Participants felt primed to offer credentials

To reestablish themselves, people recently released from prison are in a unique position where they must create many different accounts in a very short period of time, and account creation becomes a routine gateway to access a resource. The failure to create an account or download an application when instructed often means a denial of a crucial need: employment, housing, identification, social services. The formerly incarcerated co-authors on this paper hypothesize that this habit of entering in new credentials over and over, and encountering many new credential portals during their reentry, prime formerly incarcerated people to enter their credentials into new portals without thinking twice.

One volunteer mentioned that they were surprised about "How many listservs you get added to when first (re)establishing your identity online. There are so many services that ask for your email address. Getting them all is overwhelming" (V11).

Another volunteer reported that the person they were helping was struggling with multi-factor authentication (MFA) when establishing an important new credential: "[they were] stuck in an MFA loop where their authenticator app required a different MFA device. We weren't able to resolve this; I told them to reach out to their institution's MFA provider." In post-workshop reflection, the volunteer reported that "The MFA loop was extremely frustrating: the app flow to recover didn't work, and it didn't seem like they had their MFA recovery codes. I am extremely sympathetic for this since I think the participant could not have fixed this themselves" (V9).

Multiple volunteers mentioned having to help participants

with email spam filters that came from entering in their (email) credentials into various services, and sorting through their email inboxes for actually important communications (V1, V9, V11). Indeed, one workshop participant experienced a scam in exactly this way. They recounted a scam where "I accidentally clicked an accept when I went to close and delete the email - it cost me $100.00 to have my computer cleaned"(P11).

4.2.4 Scams that impersonate law enforcement or authority are particularly coercive

We heard many anecdotal reports about scams in our workshop. Job-related scams, for example, were mentioned by workshop participants when asked what unsoliticed phone calls and text messages were trying to convince them of (quoted in Section 4.1.1). Additionally, in deciding upon the topics of our intial workshop, our community partners mentioned that information about how to identify scams would be helpful. As such, we conducted a follow-up survey specifically asking about scams and scam susceptibility.

In our follow-up survey, we asked about scams in three buckets: scams claiming to be from the government/law enforcement, scams claiming to want a sexual/romantic relationship, and scams claiming to have a job opportunity.

The type of scam which our participants experienced most commonly were those claiming to be from the government or law enforcement. Such scams can trigger trauma-informed fears of re-arrest for formerly incarcerated people. Six out of 13 respondents who engaged with a law enforcement or government scam reported that they engaged with it specifically because it threatened financial penalties if they did not (e.g., fines). Three respondents (of the seven who experienced a government related scam) reported that they engaged with the scam specifically because it threatened legal action if they did not. (The only justification for engaging with the scam which was more common was not knowing or identifying that it was a scam and simply complying — seven participants.)

In Personal Narrative 2 (included in Appendix A), the researcher describes how an authoritative-appearing letter demanded money for a "business license" renewal that ended up being a scam. They describe how it had "logos, warnings, deadlines..." which made it convincing. They continue:

> "Prison teaches you to question everything, but reentry expects you to trust things you don't understand. That makes people like me easy targets." (A2)

The risk calculus when deciding to comply with a scam is different for formerly incarcerated people in this position. Because of the high stakes of re-arrest, participants sometimes complied with a scam even if they suspected it might be a scam. For example, Personal Narrative 3 describes the impact of the threat of missing a purported highway toll:

> "I know for me, part of the idea of scams in and of itself is the fact that they use authority in which to execute the scam... All it's going to take is the one scam that says, 'Hey, a camera caught you going through an intersection after the light turned red,' and I, like most people in my circumstance, would just simply panic long enough to think, 'I don't want to go back to prison. Whatever this is, I'll do whatever it takes to make it go away, to include payment.' ... especially when under the directives of community corrections. " (A3)

In other words, people may comply with possible scams that threaten fines or re-arrest because the consequences of noncompliance in the case that it may not be a scam are so stark. A3 describes that "I know for me, every rogue parking charge or Good-to-Go [toll] pass charge all comes with some level of danger. What happens if I don't pay? ... My fears become a scammer's best target" (A3).

Finally, a few times in our research, when asking participants about scams they had fallen for online, they mentioned government entrapment schemes or "sting operations" set up by (real) law enforcement entities. Some of these tactically resemble phishing and scams online; sometimes they appear as romantic or sexual opportunities on dating sites, or job opportunities on gig forums. We believe further work is needed to understand the tactics of government entrapment schemes online, and to question the efficacy, ethics, and privacy implications of law enforcement strategies that may mimic the tactics of scammers which law enforcement entities themselves criminalize.

4.2.5 The loneliness from incarceration impacts relationship scam susceptibility

Five respondents in our follow-up survey had engaged with a sexual/relationship scam. Four of the five reported that they didn't know or expect it to be a scam. The fifth respondent engaged with the scam "long enough to troll the scammer and waste their time" because they were able to "tell it's a scam very early on or from the get go" (SF12).

Two of the five who engaged with the relationship scam said explicitly that they engaged because they were lonely and starved for connection post-incarceration.

Personal Narrative 1 explores this feeling of loneliness and scam susceptibility as well: "When I was incarcerated, I was lonely. Extremely lonely. I had friends of course, but no matter how close I became with friends and family, nothing could make up for the lack of a romantic connection....8 years is a really long time to go cut off from romance and intimacy [...] This is the emotional state that most men in prison are constantly in: lonely and longing for connection" (A1).

The personal narrative explains how female-coded names started appearing on their email contact lists.[3] These email

[3]In order for an incarcerated person to communicate with someone, they have to be contacted first; they are unable to reach out to someone on their own. This communication is often done through the telecommunications company Securus (formerly known as JPay), who sells tablets to incarcerated

contacts would send them messages, talking about how lonely they were, too, and forming emotional connections. Ultimately, the author received a letter from a police department in another state that they were conducting a fraud investigation. The narrative describes the fear of even being associated with a potential crime (and the consequences of this for the sentence they were serving, and the role of loneliness in relationship scam vulnerability:

> "Prisoners, much like myself at the time, are emotionally vulnerable, facing long sentences, and often do their entire sentence completely alone. Some have friends and family, but few actually have romantic partners or other intimate connections. I, like so many others, was susceptible to that kind of manipulation and tactic because not only was it easy to believe, but I wanted to believe that someone reached out to me, was interested in me. It made the scam that much more powerful." (A1)

4.2.6 Financial instability post-release impacts financial scam susceptibility

Due to limited employment opportunities and an urgent need for money to establish themselves, some participants mentioned using get-money-quick apps. One participant said that they use the app "freecash" where they "earn money by playing games" (P17). This app has been investigated for being deceptive, manipulative, a scam, and violating user privacy (even TikTok removed Freecash ads for violating "its rules on financial misrepresentation") [4, 17, 117]. Another participant said they often get scam calls advertising that they have "got a great job opportunity" (P7). These opportunities may be particularly appealing for formerly incarcerated people, because they are often barred or discriminated against in many employment opportunities [29, 30, 80, 116, 140].

In our follow-up survey, eight out of 20 participants had engaged with a scam claiming to have a job or financial opportunity available. Two of these eight explicitly mentioned having engaged because they "really needed money" (and five said they engaged because they were curious).

One participant in our follow-up survey said that "When I was first released trying to figure out how to get my feet under me, it seemed reasonable to engage with doors that (seemed to open) but were actually scams. Such as rental properties, possibly employment" (SF5). As they "got their feet under them" over time, the urgency, desperation, and tradeoffs around income and employment balanced out so that they could be more discerning when presented with (scammy) financial opportunities.

We hypothesize that this is the reason so many participants wanted more education and help regarding job applications, resumes, how to contact employers, etc, as we discuss in Section 4.3.3 and 5.

4.2.7 Hesitation to report scams, especially to police

Of 16 follow-up survey respondents who had fallen for a scam, 11 had never reported one. Of those who had never reported a scam, five articulated that one reason they did not report was because they "didn't want to interact with law enforcement," one said they "didn't want to get anyone in trouble," and eight "didn't know who to report to." Four respondents said that they didn't report because they felt "ashamed or embarrassed."

In the workshop survey, when asked who participants were worried about having access to their information, they reported "CCOs" (P1), "law enforcement" (P5), "the government" (P13) and "DOC" (P19). When A1 was contacted by law enforcement to investigate the scam that they were a victim of, they were " terrified at first because I didn't know why I would be involved in their investigation." Similarly, A3 describes how receiving a scam purporting to be from a governmental entity takes advantage of formerly incarcerated peoples' fear of authorities. They articulate that "the last thing [a formerly incarcerated person] need[s] is somebody faking the thing they hate the most or fear the most, and that's the punishment and the idea of going back to prison" (A3).

We hypothesize that this discomfort and distrust with law enforcement makes reporting scams to those same crime-related entities undesirable for formerly incarcerated people.

4.3 Mitigating Factors

Finally, while acknowledging the many challenges and risk factors, we emphasize that formerly incarcerated people are not helpless: indeed, some of our data suggests that there are unique factors that can help *mitigate* risks from scams. We discuss these factors next (continuing to answer RQ2).

4.3.1 Close relationships and community ties help

In line with previous work [47, 84, 143], when marginalized and vulnerable groups are left out of institutional and systemic services, they often turn to strong family, friend, peer, and social networks to navigate digital challenges. When asked where they turn for help with digital needs, participants responded that they seek out family (P2, P7, P9, P13) and friends (P2, P3, P8, P9, P12). These strong community ties directly prevented scam victimization in Personal Narrative 2. After receiving a fake letter to pay for a business license fee, A2 called a friend and claims that "without their support, I would have sent in the money immediately" (A2). The author goes on to describe the importance of these social connections during a stigmatizing experience. "It showed me how much support matters during reentry. It reminded me that asking for help isn't weakness. It's survival. It's protection. It's community" (A2).

people, and allows them to send e-messages (for a price) to people in the outside world who have a Securus messaging account.

4.3.2 Confidence in identifying scams

In our follow-up survey, we asked participants if they think think they are better or worse at identifying scams than people who have not been incarcerated.[4]

Most participants felt they were better at identifying scams than people who had not been incarcerated, specifically because of their history. One participant said that they "used to con a lot of people in my addiction, [so] I feel like I can spot a con a mile away" (SF1). Another participant said that "after being incarcerated/ past criminal you can kinda tell when things are off especially with ones threatening arrest or warrants because you've had experience with the real thing" (SF13). Others mentioned that they can "tell when someone is trying to work me" (P8). Others believed that they received practice identifying misinformation while in prison, as one participant says "I'm sure being in prison helped - with all of the things people tried there" (SF20) and another recommended that people in their position shouldn't "believe anything, always be skeptical, verify everything, check sources, and if it seems fishy or too good to be true, it is. You learned to trust your gut and your feelings on the inside, use those same instincts on the outside" (SF11).

Conversely, and as mentioned in Section 4.2.1, other participants said that they felt worse at identifying scams because they had not been exposed to them while incarcerated. For example: "It makes it worse because I was incarcerated for thirty two years. So I missed everything to do with technology" (SF3). Others simply expressed that they've gotten better over time, the longer they've been out of prison. Two participants in the follow-up survey mentioned getting better at identifying scams, and more discerning, specifically after falling for scams a few times upon reentry.

In line with prior work, three follow-up survey respondents also said that upon identifying a scam as a scam, they engaged with it specifically *to* gather evidence on the scammer or to scam-the-scammer (sometimes called "scambaiting" [10]).

4.3.3 Participants desire more technology education

Finally, though education is not the only solution — and indeed, avoiding scams should not just be the responsibility of users alone — participants were eager to take active roles in their own education and security. They were hungry for more educational programming and felt that education around scams was important for incarcerated people and people reentering society. They wanted to learn about computers and coding (P1, P4, P9, P11), digital services like when applying for scholarships (P7, P19, V4, V5, V7), using file management and calendar tools (P3, P10), resumes and cover letters (P17, P19, V8, V10), and AI (P13, P15, P18). In the follow-up survey, respondents asked for more digital literacy education, especially during the reentry process.

In our follow-up survey, one participant wrote that "Often times our information is sold and we need to be educated as previously impacted by incarceration about scams and how to identify them so we can spread the word" (SF12). Our workshops are a preliminary attempt to fill this gap, and we discuss such opportunities further in Section 5.

[4]We acknowledge that self-reported confidence is not the same as an actual measure of how well people do in practice, but we sought to understand whether participants felt that their unique history was only a hindrance to digital experience, or if it provided benefits as well.

5 Discussion

Incarceration presents a unique case study to understand the experience of being excluded from learning about and accessing a society's tools for years at a time, and then being suddenly thrust back into it. This isolation and exclusion creates several gaps between the best practices of privacy education and scam prevention on the one hand and the lived experience of incarceration and reentry on the other. We discuss a few ideas to mend these gaps, as provoked by our findings.

5.1 Inadequacy of Best Practices for Scam Avoidance

Our findings reveal gaps between the current best practices for scam avoidance, and the realities of being formerly or currently incarcerated in the U.S. Specifically, these gaps are:

- **Education:** Scam research [2, 6, 14, 21, 27, 43, 48, 49, 68, 70, 73, 76, 95, 105, 113, 119, 125, 132, 141, 144, 147, 149] emphasizes early intervention, education and training to bolster one's ability to identify scams, which none of our participants had access to.
- **Technical detection tools:** Scam research has created a myriad of technical tools to detect scams and limit the reliance on human detection [16, 34, 73, 75, 91, 109, 124, 132, 152]. The systems which incarcerated people use (e.g., for communication), to our knowledge, do not deploy these types of technical detection tools, and furthermore, incarcerated people do not have control over the implementation of those tools in the digital devices available to them. Once outside, the challenges with tech literacy make it hard to use additional tools.
- **Data privacy:** Scam research [14, 25, 63] suggests that one should protect their data privacy by limiting publicly accessible information (e.g., phone number, email address, and physical address), which our participants had limited agency over because personal information about formerly incarcerated people is often publicly available [120, 138, 142].
- **Reporting:** Some scam research [2, 14, 20, 94, 95] encourages collaboration with law enforcement entities to report scams [19, 41] and arrest the people responsible, which our participants were unlikely to do given previous (traumatic) encounters with law enforcement.

5.2 Lessons and Recommendations

Digital literacy is important but not a panacea. Firstly, it is clear to us that digital literacy education and scam training is important and achievable for currently and formerly incarcerated people. While the prison may have certain concerns about incarcerated people having access to technology, it is possible to do this training without creating any vulnerabilities (even with pen and paper, for example). There is already a growing amount of digital literacy education being implemented in prisons including computers and internet access [79, 93]. We firmly believe that someone being in prison does not mean they should be excluded from educational opportunities, and in fact, education is the leading vehicle for decreasing recidivism, lowering crime, and making communities safer [9, 37, 61, 146]. Furthermore, as 95% of incarcerated people will be released one day [56], they will be released into a society which increasingly necessitates digital literacy.

We believe more workshops and educational opportunities are needed while people are still incarcerated and once people return to society. We are currently planning a second workshop, based on feedback from our first one (as expressed in Section 4.3.3). This will involve continued support for digital skills related to job search, educational attainment and scholarships, in addition to scam prevention, digital privacy education, and the tradeoffs of AI.

Despite this recommendation for digital literacy training, we echo what the nonprofit Data & Society have argued [150] regarding digital literacy as a systemic and not individual problem. In response to vague, insufficient pushes toward "AI literacy," they write that: "...the concept of AI literacy has been leveraged to market a simplistic solution to the very complex problem of job displacement..." and that the push for individual "AI literacy faults workers for failing to garner gainful employment rather than a wider socioeconomic environment that normalizes precarity." We agree that digital literacy and AI literacy will not solve the overwhelming unemployment rates for formerly incarcerated people [30, 140], or provide a panacea for the discrimination, poverty, and inequality which they experience [35, 59, 60, 80].

Limitations of relying on law enforcement for fighting scams. We note above that some scam research recommends collaboration with law enforcement vis-a-vis identifying and stopping scammers. However, in our findings, we report that people with a history of incarceration are unlikely to report or collaborate with law enforcement, so another avenue is clearly needed. We furthermore believe that to the extent that scammers are themselves motivated by financial need, and financial need is both a frequent outcome and predictor of incarceration [18, 35, 62], incarcerating scammers and perpetuating this cycle may not be the most effective approach for fighting scams. We believe this extends to crime generally, which is largely a function of social vulnerability and necessity, and that incarceration only exacerbates these conditions for the individuals and society at large.

Consumer protection for incarcerated people. We also echo an increasing push in academic and legal literature to extend consumer rights to people in prison, many of which they are carved out of despite being a literal "captive market" [18, 74, 112]. Related to scam victimization specifically, the National Consumer Law Center details [23] how being incarcerated creates "prime targets for financial exploitation." They further explain how incarcerated people are left out of scam reporting processes because federal agencies "encourage consumers to report violations of the laws they enforce online. But most incarcerated consumers lack access to the open internet... preventing incarcerated people from submitting a fillable form" [23]. To change the state of consumer protection rights for incarcerated people, a UC Law review article concludes: "Accomplishing meaningful change will thus require concerted effort by advocates and a willingness on the part of policymakers to see incarcerated people and their families as consumers entitled to the same protections that are enjoyed by most people every day" [112].

5.3 Opportunities for Future Work

There are many opportunities for future work. Firstly, future work could quantitatively measure whether there is a substantive difference in the number of scams formerly incarcerated people receive compared to others, and whether their online information exposure plays a role in this. We also believe more work is needed to understand the true societal causes of scams as simply finding and incarcerating scammers may not produce desired results. We also believe a direction for future work could investigate the adoption of AI tools; one respondent mentioned Perplexity.ai, and another mentioned ChatGPT when asked where they go to for digital help. Finally, we believe further work is needed to understand the tactics, efficacy, ethics, and privacy implications of government entrapment schemes online, which some participants felt were similar to scams.

6 Conclusion

In this work, we investigated the relationship between scams, digital literacy, and (post-)incarceration in the United States. We conducted three surveys with a total N=48 unique respondents, and coupled this with personal narratives from three formerly incarcerated researchers. Our participants were unable to gain experience or intuition with new digital tools or new digital scams while they were incarcerated, and they frequently fell for and were targeted by scams. We investigate contributing factors to scam susceptibility and scam mitigation techniques. We concluded by offering lessons from this research to better protect currently and formerly incarcerated people (and help them protect themselves).

References

[1] Accountable2You. Home — accountable2you.com. https://accountable2you.com/. [Accessed 18-02-2026].

[2] Sharad Agarwal. 'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom.

[3] Oghenemaro Anuyah, Karla Badillo-Urquiola, and Ronald Metoyer. Characterizing the technology needs of vulnerable populations for participation in research and design by adopting maslow's hierarchy of needs. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2023.

[4] Pieter Arntz. Get paid to scroll TikTok? The data trade behind Freecash ads — malwarebytes.com. https://www.malwarebytes.com/blog/news/2026/01/get-paid-to-scroll-tiktok-the-data-trade-behind-freecash-ads, 2026. [Accessed 19-02-2026].

[5] ASPE. Incarceration & Reentry — aspe.hhs.gov. https://aspe.hhs.gov/topics/human-services/incarceration-reentry-0, 2026. [Accessed 19-02-2026].

[6] Aurélien Baillon, Jeroen de Bruin, Aysil Emirmahmutoglu, Evelien van de Veer, and Bram van Dijk. Informing, simulating experience, or both: A field experiment on phishing risks. *PloS One*, 14(12):e0224216, 2019.

[7] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. "so-called privacy breeds evil": Narrative justifications for intimate partner surveillance in online forums. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW3), January 2021.

[8] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. SoK: Safer Digital-Safety Research Involving At-Risk Users . In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 635–654, Los Alamitos, CA, USA, May 2024. IEEE Computer Society.

[9] Kathleen Bender. Education Opportunities in Prison Are Key to Reducing Crime — americanprogress.org. https://www.americanprogress.org/article/education-opportunities-prison-key-reducing-crime/, 2018. [Accessed 19-02-2026].

[10] Manon Berney, Jan Ondrus, and Adrian Holzer. Navigating the shadows of cyber vigilantism: A preliminary analysis of social dynamics and activities of scambaiting. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery.

[11] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M. Redmiles, and Angelika Strohmayer. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 546–553, 2022.

[12] Marzieh Bitaab, Alireza Karimi, Zhuoer Lyu, Adam Oest, Dhruv Kuchhal, Muhammad Saad, Gail-Joon Ahn, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, and Adam Doupé. SCAMMAGNIFIER: Piercing the Veil of Fraudulent Shopping Website Campaigns. In *Proceedings 2025 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2025. Internet Society.

[13] Elijah Bouma-Sims, Lily Klucinec, Mandy Lanyon, Julie Downs, and Lorrie Faith Cranor. 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*, San Diego, CA, USA, 2025. Internet Society.

[14] Nick Bourke. Stopping Scams Against Consumers: Roadmap for a National Strategy, July 2024.

[15] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[16] Paolo Buono, Giuseppe Desolda, Francesco Greco, and Antonio Piccinno. Let warnings interrupt the interaction and explain: designing and evaluating phishing email warnings. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI EA '23, pages 1–6, New York, NY, USA, April 2023. Association for Computing Machinery.

[17] Better Business Bureau. Freecash | BBB Complaints | Better Business Bureau — bbb.org. https://www.bbb.org/us/fl/orlando/profile/online-gaming/freecash-0733-90711835/complaints, 2026. [Accessed 19-02-2026].

[18] CONSUMER FINANCIAL PROTECTION BUREAU. Justice-Involved Individuals and the Consumer Financial Marketplace. https://files.consumerfinance.gov/f/documents/cfpb_jic_report_2022-01.pdf, 2022. [Accessed 19-02-2026].

[19] Consumer Financial Protection Bureau. I think I or someone I know was the victim of a scam or financial exploitation. Who can I contact for help? | Consumer Financial Protection Bureau — consumerfinance.gov. https://www.consumerfinance.gov/ask-cfpb/i-think-i-or-someone-i-know-was-the-victim-of-a-scam-or-financial-exploitation-who-can-i-contact-for-help-en-1777/, 2025. [Accessed 19-02-2026].

[20] Mark Button, Vasileios Karagiannopoulos, Julak Lee, Joon Bae Suh, and Jeyong Jung. Preventing fraud victimisation against older adults: Towards a holistic model for protection. *International Journal of Law, Crime and Justice*, 77:100672, June 2024.

[21] Deanna D. Caputo, Shari Lawrence Pfleeger, Jesse D. Freeman, and M. Eric Johnson. Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1):28–38, 2014.

[22] Doga Cavdir, Dillion Simone, Myles de Bastion, Shawn Trail, and Nate Hergert. Sonic Agency: A Group Autoethnography of Technology-mediated Performance Practice by Deaf and Hard of Hearing Musicians. In *Proceedings of the 27th International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '25, pages 1–15, New York, NY, USA, October 2025. Association for Computing Machinery.

[23] National Consumer Law Center. Captive Concerns: Incarcerated People Face Obstacles to Reporting Consumer Abuses — nclc.org. https://www.nclc.org/resources/captive-concerns-incarcerated-people-face-obstacles-to-reporting-consumer-abuses/, 2024. [Accessed 19-02-2026].

[24] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458, 2018.

[25] Hongliang Chen, Christopher E. Beaudoin, and Traci Hong. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70:291–302, May 2017.

[26] Si Chen, James Waller, Matthew Seita, Christian Vogler, Raja Kushalnagar, and Qi Wang. Towards Co-Creating Access and Inclusion: A Group Autoethnography on a Hearing Individual's Journey Towards Effective Communication in Mixed-Hearing Ability Higher Education Settings. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, pages 1–14, New York, NY, USA, May 2024. Association for Computing Machinery.

[27] Xiaowei Chen, Sophie Doublet, Anastasia Sergeeva, Gabriele Lenzini, Vincent Koenig, and Verena Distler. What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory.

[28] Grace Ciambrone and Shomir Wilson. Creation and Analysis of a Corpus of Scam Emails Targeting Universities. In *Companion Proceedings of the ACM Web Conference 2023*, WWW '23 Companion, pages 24–27, New York, NY, USA, April 2023. Association for Computing Machinery.

[29] Lucius Couloute. Getting Back on Course: Educational exclusion and attainment among formerly incarcerated people — prisonpolicy.org. https://www.prisonpolicy.org/reports/education.html, 2018. [Accessed 19-02-2026].

[30] Lucius Couloute and Daniel Kopf. Out of Prison & Out of Work — prisonpolicy.org. https://www.prisonpolicy.org/reports/outofwork.html, 2018. [Accessed 19-02-2026].

[31] King County. Sex offender registration - King County, Washington — kingcounty.gov. https://kingcounty.gov/en/dept/sheriff/courts-jails-legal-system/sheriff-services/sex-offender-registration, 2026. [Accessed 19-02-2026].

[32] CovenantEyes. Screen Accountability™ | Covenant Eyes — covenanteyes.com. https://www.covenanteyes.com/, 2025. [Accessed 18-02-2026].

[33] Sally Jo Cunningham and Matt Jones. Autoethnography: a tool for practice and education. In *Proceedings of the 6th ACM SIGCHI New Zealand chapter's international conference on Computer-human interaction: making CHI natural*, CHINZ '05, pages 1–8, New York, NY, USA, July 2005. Association for Computing Machinery.

[34] Avisha Das, Shahryar Baki, Ayman El Aassal, Rakesh Verma, and Arthur Dunbar. Sok: A comprehensive reexamination of phishing research from the security perspective. *IEEE Communications Surveys & Tutorials*, 22(1):671–708, 2020.

[35] Saneta deVuono Powell, Chris Schweidler, Alicia Walters, and Azadeh Zohrabi. Who pays? the true cost of incarceration on families. *Oakland, Calif.: Ella Baker Center, Forward Together, Research Action Design. Accessed July*, 23(2021):221–43, 2015.

[36] Zak Doffman. FBI Warning—Do Not Install This App On Your PC Or Smartphone. Section: Cybersecurity.

[37] DOJ. Prison reform: Reducing recidivism by strengthening the federal bureau of prisons. https://www.justice.gov/archives/prison-reform, 2025. [Accessed 19-02-2026].

[38] Carolyn Ellis, Tony E. Adams, and Arthur P. Bochner. Autoethnography: An Overview. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 12(1), 2011.

[39] EverAccountable. Quit Porn Today Through the Power of Accountability | Ever Accountable — everaccountable.com. https://everaccountable.com/. [Accessed 18-02-2026].

[40] Matthias Fassl and Katharina Krombholz. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15, Hamburg Germany, April 2023. ACM.

[41] FBI. Financial Crime and You | Federal Bureau of Investigation — fbi.gov. https://www.fbi.gov/file-repository/vsd/financial_crime.pdf/view, 2018. [Accessed 19-02-2026].

[42] FBI. Sex Offender Registry Website. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/sex-offender-registry, 2026. [Accessed 18-02-2026].

[43] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. SoK: Still Plenty of Phish in the Sea — A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research.

[44] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "is my phone hacked?" analyzing clinical computer security interventions with survivors of intimate partner violence. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[45] Aakash Gautam, Khushboo Gandhi, and Jessica Sendejo. Enhancing reentry support programs through digital literacy integration. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, pages 2882–2896, 2024.

[46] Aakash Gautam, Khushboo Gandhi, and Jessica Sendejo. Enhancing Reentry Support Programs Through Digital Literacy Integration. In *Designing Interactive Systems Conference*, pages 2882–2896, Copenhagen Denmark, July 2024. ACM.

[47] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium*

(USENIX Security 22), pages 305–322, Boston, MA, August 2022. USENIX Association.

[48] Sanjay Goel, Kevin Williams, and Ersin Dincelli. Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, 18:22–44, 01 2017.

[49] Roderick Graham and Ruth Triplett. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, 38(12):1371–1382, 2017.

[50] Monika Grierson, Delvin Varghese, Mitzi Bolton, and Patrick Olivier. Design considerations for a digital service to support prison leavers. In *Proceedings of the 2022 ACM Designing Interactive Systems Conference*, pages 504–516, 2022.

[51] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 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, page 1–15, New York, NY, USA, 2018. Association for Computing Machinery.

[52] Susila Gurusami. The carceral web we weave: Carceral citizens' experiences of digital punishment and solidarity. *Punishment & Society*, 21(4):435–453, 2019.

[53] Grant Ho and David Wagner. Detecting and Characterizing Lateral Phishing at Scale.

[54] Sarah Homewood. Self-Tracking to Do Less: An Autoethnography of Long COVID That Informs the Design of Pacing Technologies. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, pages 1–14, New York, NY, USA, April 2023. Association for Computing Machinery.

[55] John Hughes, Val King, Tom Rodden, and Hans Andersen. The role of ethnography in interactive systems design. *interactions*, 2(2):56–65, April 1995.

[56] Timothy Hughes and Doris James Wilson. Reentry Trends in the United States.

[57] Phuong Duy Huynh, Son Hoang Dau, Nicholas Huppert, Joshua Cervenjak, Hoonie Sun, Hong Yen Tran, Xiaodong Li, and Emanuele Viterbo. Serial Scammers and Attack of the Clones: How Scammers Coordinate Multiple Rug Pulls on Decentralized Exchanges. In *Proceedings of the ACM on Web Conference 2025*, WWW '25, pages 1016–1033, New York, NY, USA, April 2025. Association for Computing Machinery.

[58] Prison Policy Initiative. A guide to public records requests for advocates seeking reform of the criminal legal system.

[59] Prison Policy Initiative. Poverty and debt.

[60] Prison Policy Initiative. Public health.

[61] Vera Institute. Back to School: A Common-Sense Strategy to Lower Recidivism — vera.org. https://www.vera.org/news/back-to-school-a-common-sense-strategy-to-lower-recidivism, 2019. [Accessed 19-02-2026].

[62] Vera Institute. Fines and Fees — vera.org. https://www.vera.org/ending-mass-incarceration/criminalization-racial-disparities/fines-and-fees, 2026. [Accessed 19-02-2026].

[63] Danesh Irani, Steve Webb, Kang Li, and Calton Pu. Large online social footprints–an emerging threat. *2009 International Conference on Computational Science and Engineering*, 3:271–276, 2009.

[64] Dhruv Jain, Audrey Desjardins, Leah Findlater, and Jon E. Froehlich. Autoethnography of a Hard of Hearing Traveler. In *Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '19, pages 236–248, New York, NY, USA, October 2019. Association for Computing Machinery.

[65] Daye Kang, Jingjin Li, Gilly Leshed, Jeffrey M Rzeszotarski, and Xi Lu. Towards Hormone Health: An Autoethnography of Long-Term Holistic Tracking to Manage PCOS. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–20, New York, NY, USA, April 2025. Association for Computing Machinery.

[66] Emaan Bilal Khan, Emaan Atique, and Mobin Javed. Investigating Phishing Threats in the Email Browsing Experience of Visually Impaired Individuals. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, pages 1–11, New York, NY, USA, May 2024. Association for Computing Machinery.

[67] Platon Kotzias, Michalis Pachilakis, Javier Aldana Iuit, Juan Caballero, Iskander Sanchez-Rola, and Leyla Bilge. Ctrl+Alt+Deceive: Quantifying User Exposure to Online Scams. In *Proceedings 2025 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2025. Internet Society.

[68] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Trans. Internet Technol.*, 10(2), June 2010.

[69] Daniele Lain, Yoshimichi Nakatsuka, Kari Kostiainen, and Gene Tsudik. URL Inspection Tasks: Helping Users Detect Phishing Links in Emails.

[70] Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. How Effective is Anti-Phishing Training for Children?

[71] Xigao Li, Amir Rahmati, and Nick Nikiforakis. Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms. In *Proceedings 2024 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2024. Internet Society.

[72] Xigao Li, Anurag Yepuri, and Nick Nikiforakis. Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams. In *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2023. Internet Society.

[73] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 2075–2084, New York, NY, USA, 2011. Association for Computing Machinery.

[74] Aaron Littman. Free-World Law Behind Bars. *Yale Law Journal*, Vol. 131(5):1385–1482, March 2022.

[75] Gang Liu, Guang Xiang, Bryan A. Pendleton, Jason I. Hong, and Wenyin Liu. Smartening the crowds: computational techniques for improving human verification to fight phishing scams. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 1–13, New York, NY, USA, July 2011. Association for Computing Machinery.

[76] Mingyi Liu, HyungSeok Han, Jaehyuk Lee, Jihae Ahn, and Frank Li. I Experienced More than 10 DeFi Scams: On DeFi Users' Perception of Security Breaches and Countermeasures.

[77] Andrés Lucero. Living Without a Mobile Phone: An Autoethnography. In *Proceedings of the 2018 Designing Interactive Systems Conference*, DIS '18, pages 765–776, New York, NY, USA, June 2018. Association for Computing Machinery.

[78] Richard Martinez and Kurt Squire. Engaging recently incarcerated and gang affiliated black and latino/a young adults in designing social collocated applications for mixed reality smart glasses through community-based participatory design workshops. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2024.

[79] Richard Martinez and Kurt Squire. Engaging recently incarcerated and gang affiliated Black and Latino/a young adults in designing social collocated applications for mixed reality smart glasses through community-based participatory design workshops. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–17, Honolulu HI USA, May 2024. ACM.

[80] Tara García Mathewson. Licensing barriers keep people with criminal records from education and training. https://archive.is/27SLP, 2023. [Accessed 18-02-2026].

[81] Gibson Mba, Jeremiah Onaolapo, Gianluca Stringhini, and Lorenzo Cavallaro. Flipping 419 Cybercrime Scams: Targeting the Weak and the Vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion*, WWW '17 Companion, pages 1301–1310, Republic and Canton of Geneva, CHE, April 2017. International World Wide Web Conferences Steering Committee.

[82] Andy McAdams. An Uncomfortable Look at the Use of Surveillance App Covenant Eyes by Law Enforcement — bytesizedethics.io. https://www.bytesizedethics.io/p/an-uncomfortable-look-at-the-use, 2023. [Accessed 18-02-2026].

[83] McAfee. Are Fake Apps Taking Over Your Phone?, July 2018.

[84] Allison McDonald, Catherine Barwulor, Michelle L. Mazurek, Florian Schaub, and Elissa M. Redmiles. "it's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 375–392. USENIX Association, August 2021.

[85] Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists, Jan 2015.

[86] Susan E. McGregor, Franziska Roesner, and Kelly Caine. Individual versus organizational computer security and privacy concerns in journalism, Jan 2016.

[87] Dhruv Mehrotra. The Ungodly Surveillance of Anti-Porn 'Shameware' Apps — wired.com. https://www.wired.com/story/covenant-eyes-anti-porn-accountability-monitoring-apps/, 2022. [Accessed 18-02-2026].

[88] Flynard Miller. The Criminal Justice System Would Benefit From Prison Education Programs. https://prisonjournalismproject.org/2022/05/13/the-criminal-justice-system-would-benefit-from-prison-education-programs/, 2022. [Accessed 18-02-2026].

[89] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. Dial One for Scam: A Large-Scale Analysis of Technical Support Scams. In *Proceedings 2017 Network and Distributed System Security Symposium*, San Diego, CA, 2017. Internet Society.

[90] Collins W. Munyendo, Kentrell Owens, Faith Strong, Shaoqi Wang, Adam J. Aviv, Tadayoshi Kohno, and Franziska Roesner. "You Have to Ignore the Dangers": User Perceptions of the Security and Privacy Benefits of WhatsApp Mods . In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 4515–4533, Los Alamitos, CA, USA, May 2025. IEEE Computer Society.

[91] Muhammad Muzammil, Abisheka Pitumpe, Xigao Li, Amir Rahmati, and Nick Nikiforakis. The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams. In *Proceedings of the ACM on Web Conference 2025*, WWW '25, pages 1034–1045, New York, NY, USA, April 2025. Association for Computing Machinery.

[92] Martin Nisser, Marisa Gaetz, Andrew Fishberg, Raechel N Soicher, Faraz Faruqi, and Joshua Long. From prisons to programming: Fostering self-efficacy via virtual web design curricula in prisons and jails. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2024.

[93] Martin Nisser, Marisa Gaetz, Andrew Fishberg, Raechel N. Soicher, Faraz Faruqi, and Joshua Long. From Prisons to Programming: Fostering Self-Efficacy via Virtual Web Design Curricula in Prisons and Jails. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, Honolulu HI USA, May 2024. ACM.

[94] Rajvardhan Oak and Zubair Shafiq. "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams.

[95] Rajvardhan Oak and Zubair Shafiq. Victims, Vigilantes, and Advice Givers: An Analysis of Scam-Related Discourse on Reddit.

[96] Colorado Bureau of Investigation Dept of Public Safety. SCAM TARGETING REGISTERED SEX OFFENDERS. https://cms7files.revize.com/northglennco/Departments/Police/Sex%20Offender/Registered%20Sex%20Offender%20Scam%20Advisement.pdf. [Accessed 18-02-2026].

[97] Federal Bureau of Prisons. Freedom Of Information — bop.gov. https://www.bop.gov/foia/#tabs-0, 2026. [Accessed 19-02-2026].

[98] WA Association of Sheriffs and Police Chiefs. Sex Offender Information — waspc.org. https://www.waspc.org/sex-offender-information, 2026. [Accessed 19-02-2026].

[99] Ihudiya Finda Ogbonnaya-Ogburu and Aarti Israni. Supporting the digital aspects of reentry for formerly incarcerated individuals. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '24, New York, NY, USA, 2024. Association for Computing Machinery.

[100] Ihudiya Finda Ogbonnaya-Ogburu and Aarti Israni. Supporting the Digital Aspects of Reentry for Formerly Incarcerated Individuals. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–5, Honolulu HI USA, May 2024. ACM.

[101] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna Dillahunt. Returning citizens' job search and technology use: Preliminary findings. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 365–368, New York, NY, USA, 2018. Association for Computing Machinery.

[102] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R. Dillahunt. Towards an effective digital literacy intervention to assist returning citizens with job search. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[103] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R. Dillahunt. Towards an Effective Digital Literacy Intervention to Assist Returning Citizens with Job Search. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, Glasgow Scotland Uk, May 2019. ACM.

[104] Aisling Ann O'Kane, Yvonne Rogers, and Ann E. Blandford. Gaining empathy for non-routine mobile device use through autoethnography. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 987–990, New York, NY, USA, 2014. Association for Computing Machinery.

[105] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 6412–6424, New York, NY, USA, May 2017. Association for Computing Machinery.

[106] Kentrell Owens, Anita Alem, Franziska Roesner, and Tadayoshi Kohno. Electronic monitoring smartphone apps: An analysis of risks from technical, Human-Centered, and legal perspectives. In *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association.

[107] Kentrell Owens, Camille Cobb, and Lorrie Cranor. "you gotta watch what you say": Surveillance of communication with incarcerated people. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[108] Kentrell Owens, Yael Eiger, Basia Radka, Tadayoshi Kohno, and Franziska Roesner. Understanding experiences with compulsory immigration surveillance in the u.s. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '25, page 887–899, New York, NY, USA, 2025. Association for Computing Machinery.

[109] Justin Petelka, Yixin Zou, and Florian Schaub. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–15, New York, NY, USA, May 2019. Association for Computing Machinery.

[110] Veronica Pimenova, Yotam Sechayk, Fabricio Murai, Andrew Hundt, and Shiri Dori-Hacohen. A Longitudinal Autoethnography of Email Access for a Professional with Chronic Illness and ADHD: Preliminary Insights. In *Proceedings of the 27th International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '25, pages 1–4, New York, NY, USA, October 2025. Association for Computing Machinery.

[111] Georgetown's Prisons and Justice Initiative. Incarceration can put education out of reach for life, report says - THE FEED — feed.georgetown.edu. https://feed.georgetown.edu/access-affordability/incarceration-can-put-education-out-of-reach-for-life-report-says/, 2018. [Accessed 19-02-2026].

[112] Stephen Raher. The Company Store and the Literally Captive Market: Consumer Law in Prisons and Jails — repository.uclawsf.edu. https://repository.uclawsf.edu/hastings_race_poverty_law_journal/vol17/iss1/3/, 2020. [Accessed 19-02-2026].

[113] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, and Mattia Mossano. An investigation of phishing awareness and education over time: When and how to best remind users.

[114] Bianca C Reisdorf, Julia DeCook, Megan Foster, Jennifer Cobbina, and Ashleigh LaCourse. Digital reentry: uses of and barriers to icts in the prisoner reentry process. *Information, Communication & Society*, 25(14):2028–2045, 2022.

[115] Bianca C Reisdorf and RV Rikard. Digital rehabilitation: A model of reentry into the digital age. *American Behavioral Scientist*, 62(9):1273–1290, 2018.

[116] Michelle Natividad Rodriguez and Maurice Emsellem. 65 MILLION "NEED NOT APPLY" The Case for Reforming Criminal Background Checks for Employment. https://static.prisonpolicy.org/scans/65_Million_Need_Not_Apply-2stats.pdf, 2011. [Accessed 18-02-2026].

[117] Reece Rogers. No, the Freecash App Won't Pay You to Scroll TikTok — wired.com. https://www.wired.com/story/no-the-freecash-app-wont-pay-you-to-scroll-tiktok/, 2026. [Accessed 19-02-2026].

[118] Haley Glover Sarah Bray, Megan Quattlebaum. A new study illuminates why the barriers to higher education that incarcerated people confront should be removed (opinion) — insidehighered.com. https://www.insidehighered.com/vie

ws/2020/03/18/new-study-illuminates-why-barriers-higher-education-incarcerated-people-confront, 2020. [Accessed 19-02-2026].

[119] Lorin Schöni, Neele Roch, Hannah Sievers, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. It's a Match - Enhancing the Fit between Users and Phishing Training through Personalisation. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–25, New York, NY, USA, April 2025. Association for Computing Machinery.

[120] Inmate Search Mugshots Arrests Background Check People Search. Inmate Search Mugshots Arrests - Apps on Google Play — play.google.com. https://play.google.com/store/apps/details?id=com.inmate.search.background.check&hl=en_{U}{S}, 2025. [Accessed 19-02-2026].

[121] Hyunjin Seo, Hannah Britton, Megha Ramaswamy, Darcey Altschwager, Mathew Blomberg, Shola Aromona, Bernard Schuster, Ellie Booton, Marilyn Ault, and Joi Wickliffe. Returning to the digital world: Digital technology use and privacy management of women transitioning from incarceration. *new media & society*, 24(3):641–666, 2022.

[122] Hyunjin Seo, Joseph Erba, Darcey Altschwager, and Mugur Geana. Evidence-based digital literacy class for older, low-income african-american adults, 2019.

[123] Wafa Shafqat, Seunghun Lee, Sehrish Malik, and Hyun-chul Kim. The Language of Deceivers: Linguistic Features of Crowdfunding Scams. In *Proceedings of the 25th International Conference Companion on World Wide Web*, WWW '16 Companion, pages 99–100, Republic and Canton of Geneva, CHE, April 2016. International World Wide Web Conferences Steering Committee.

[124] Zitong Shen, Sineng Yan, Youqian Zhang, Xiapu Luo, Grace Ngai, and Eugene Yujun Fu. "It Warned Me Just at the Right Moment": Exploring LLM-based Real-time Detection of Phone Scams. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, CHI EA '25, pages 1–7, New York, NY, USA, April 2025. Association for Computing Machinery.

[125] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 373–382, New York, NY, USA, April 2010. Association for Computing Machinery.

[126] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and privacy for refugees in the united states. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423, 2018.

[127] Eric Spero, Isa Seow, Lucas Betts, Eddie Fuatimau, Robert Biddle, Danielle Lottridge, and Giovanni Russello. Language as Lure: A Naturalistic Study on Pasifika Phishing Susceptibility.

[128] Joey Sprague. Feminist methodologies for critical researchers : bridging differences, 2016.

[129] CSG Justice Center Staff. How States Block Access to Continued Education for People in the Criminal Justice System - CSG Justice Center — csgjusticecenter.org. https://csgjusticecenter.org/2020/02/11/report-states-prevent-access-to-continued-education-for-people-in-the-criminal-justice-system/, 2020. [Accessed 19-02-2026].

[130] Kate Stephens, Matthew Butler, Leona M Holloway, Cagatay Goncu, and Kim Marriott. Smooth Sailing? Autoethnography of Recreational Travel by a Blind Person. In *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '20, pages 1–12, New York, NY, USA, October 2020. Association for Computing Machinery.

[131] Lukas Strobel, Kathrin Maria Gerling, and Jan Ole Rixen. "Is This Seat Accessible for Me?": An Autoethnography of a Person With a Mobility Disability Using Interactive Seat Plans for Public Events. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–15, New York, NY, USA, April 2025. Association for Computing Machinery.

[132] Dennis Tan Jia Jun, Ahmad Sahban Rafsanjani, Saad Aslam, and Mehran Behjati. Human factors in information security: A quantitative study with technical solutions to prevent social engineering attacks. *Digital Threats*, 6(4), December 2025.

[133] David R Thomas. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2):237–246, 2006.

[134] Mindy Tran, Collins W. Munyendo, Harshini Sri Ramulu, Rachel Gonzalez Rodriguez, Luisa Ball Schnell, Cora Sula, Lucy Simko, and Yasemin Acar. Security, Privacy, and Data-sharing Trade-offs When Moving to the United States: Insights from a Qualitative Study . In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 617–634, Los Alamitos, CA, USA, May 2024. IEEE Computer Society.

[135] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1893–1909. USENIX Association, August 2020.

[136] Huahong Tu. Users Really Do Answer Telephone Scams.

[137] usa.gov. How to look up prisoners and prison records | USAGov — usa.gov. https://www.usa.gov/prisoner-records, 2025. [Accessed 19-02-2026].

[138] VineLink. VINELink — vinelink.vineapps.com. https://vinelink.vineapps.com, 2026. [Accessed 19-02-2026].

[139] Wendy Sawyer Wagner and Peter. Mass incarceration: The whole pie 2024, Mar 2024.

[140] Leah Wang and Wanda Bertram. New data on formerly incarcerated people's employment reveal labor market injustices — prisonpolicy.org. https://www.prisonpolicy.org/blog/2022/02/08/employment/, 2022. [Accessed 19-02-2026].

[141] Rick Wash, Norbert Nthala, and Emilee Rader. Knowledge and Capabilities that Non-Expert Users Bring to Phishing Detection.

[142] WebCatalog. JailBase - Desktop App for Mac, Windows (PC) - WebCatalog — webcatalog.io. https://webcatalog.io/en/apps/jailbase, 2026. [Accessed 19-02-2026].

[143] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. Understanding Help-Seeking and Help-Giving on social media for Image-Based sexual abuse. In *33rd USENIX Security Symposium (USENIX Security 24)*, Philadelphia, PA, 2024. USENIX Association.

[144] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, pages 1–12, New York, NY, USA, May 2019. Association for Computing Machinery.

[145] Charlotte West. Many states don't educate people sentenced to life. Now some are coming home. — jjie.org. https://jjie.org/2024/04/12/many-states-dont-educate-people-sentenced-to-life-now-some-are-coming-home/, 2024. [Accessed 19-02-2026].

[146] Holly Wetzel. Research Finds Prison Education Programs Reduce Recidivism — mackinac.org. https://www.mackinac.org/pressroom/2023/research-finds-prison-education-programs-reduce-recidivism, 2023. [Accessed 19-02-2026].

[147] Ryan T. Wright and Kent Marett. The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27(1):273–303, 2010.

[148] Shaomei Wu, Jingjin Li, and Gilly Leshed. Finding My Voice over Zoom: An Autoethnography of Videoconferencing Experience for a Person Who Stutters. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, pages 1–16, New York, NY, USA, May 2024. Association for Computing Machinery.

[149] Guoyi Ye, Geng Hong, Yuan Zhang, and Min Yang. Interface Illusions: Uncovering the Rise of Visual Scams in Cryptocurrency Wallets. In *Proceedings of the ACM Web Conference 2024*, WWW '24, pages 1585–1595, New York, NY, USA, May 2024. Association for Computing Machinery.

[150] Meg Young, Alice E. Marwick, Anuli Akanegbu, Rigoberto Lara Guzmán, Ania Calderon, and Janet Haven. Building Civic Strength for an AI Era — datasociety.net. https://datasociety.net/points/building-civic-strength-for-an-ai-era, 2026. [Accessed 19-02-2026].

[151] Yuxiang Zhai, Xiao Xue, Zekai Guo, Tongtong Jin, Yuting Diao, and Jihong Jeung. Hear Us, then Protect Us: Navigating Deepfake Scams and Safeguard Interventions with Older Adults through Participatory Design. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–19, New York, NY, USA, April 2025. Association for Computing Machinery.

[152] Sarah Zheng and Ingolf Becker. Presenting Suspicious Details in User-Facing E-mail Headers Does Not Improve Phishing Detection.

[153] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. Sok: Human-centered phishing susceptibility. *ACM Trans. Priv. Secur.*, 26(3), April 2023.

A Personal Narratives

A.1 Personal Narrative 1: Relationship Scam While Incarcerated

When I was incarcerated, I was lonely. Extremely lonely. I had friends of course, but no matter how close I became with friends and family, nothing could make up for the lack of a romantic connection. I would go to visitation every weekend because I had an amazing family that supported me, and I was blessed that they could make the drive every week. But after hugging them, getting our food, and sitting down, I would unconsciously scan the room and see other men sharing passionate kisses with their wives or girlfriends and wish that I was them. 8 years is a really long time to go cut off from romance and intimacy, but the desire for connection started long before that.

It's not uncommon for the men inside the walls to share these feelings, the longing for companionship, because everyone feels it. One of the ways men try to combat the loneliness is to make profiles on write a prisoner websites, and people were often successful. I myself met one long-term, long-distance girlfriend whom I dated for about 2 full years.

I remember that, after starting my profile, I would see names pop up on my JPay (now Securus) account, and I would get excited, especially if it was a girl's name. I would think to myself, "is she reaching out because she saw my profile? Does she think I'm attractive? I wonder what she's like, who she is." Even though I always had the purest of intentions, knowing that most connections I built were professional or platonic, I couldn't help it. I was desperate for connection, and hopeful that every single time I saw a new name, that it would lead to one. This is the emotional state that most men in prison are constantly in: lonely and longing for connection.

About 6 years into my prison sentence, I started getting new names popping up, Sage, Alexis, Sarah, Melinda, and with each name, came a letter in the mail that the service would send me. I remember one from Melinda Unruh, talking about how she's a lonely woman, whose husband passed away. How she doesn't talk to many men because of pain from the loss she went through. How she spends her time with her dog in the forest. And how she thought I looked sweet and that she thought that maybe she'd be open to talking to me. I couldn't help but connect with everything she said. I knew what it was like to lose people, to feel alone, to be cut off from community, and to find a meaningful partnership with a dog. After all, I was in the dog program and used a picture of me

and a dog for my profile picture. I tried writing back, sending JPay messages, and even calling the number she gave me, all to no avail.

After about 3 weeks of trying with no luck, I finally gave up trying to get in contact with her. I didn't think too much about it afterwards. After all, there were a lot of people who got on my JPay that never actually reached out. I went on thinking that for about another few months as new names cropped up on my JPay without them reaching out until I received a new letter; one from a California police department.

In this letter, I was told that the department was investigating illegal fraudulent activity, and I was terrified at first because I didn't know why I would be involved in their investigation. As I continued to read, I realized they weren't investigating me, they were investigating a list of names. Familiar names: Sage, Alexis, Sarah, Melinda Unruh, and others I recognized too. They told me that these were the names someone was using to scam prisoners and that if I respond to any messages these people send me, I could possibly be charged with fraud as well.

Prisoners, much like myself at the time, are emotionally vulnerable, facing long sentences, and often do their entire sentence completely alone. Some have friends and family, but few actually have romantic partners or other intimate connections. I, like so many others, was susceptible to that kind of manipulation and tactic because not only was it easy to believe, but I wanted to believe that someone reached out to me, was interested in me. It made the scam that much more powerful. Thankfully I never got in contact with the scammer and never lost anything to them, but I know others were not so lucky.

A.2 Personal Narrative 2: Business License Scam Post-Incarceration

When I got out of prison, every step I took felt scary. I was trying so hard to rebuild my life, and starting my own business was one of the things I was most proud of. It gave me hope. It made me feel like maybe I really could create a new future. So when a letter came in the mail saying I had to pay money to "reinstate" my business, my heart dropped. The letter looked real. It had logos, warnings, deadlines. I remember thinking, "Oh no… what if I lose the one good thing I built for myself?"

After incarceration, you carry this heavy fear and mistrust, of systems, people, and even yourself. I always say, "Prison teaches you to question everything, but reentry expects you to trust things you don't understand." That makes people like me easy targets.

At first, I was ready to send the money right away. Panic took over. But something inside me said, "Call someone." So I reached out to a friend. We sat and processed the letter together, reading every line, talking it through. Without their support, I would have sent in the money immediately, and I would have paid $70 more than it actually costs to renew a business license. That thought still makes me shaky because I know how easy it would've been to lose that money.

When I later learned the whole thing was a scam, my heart sank. I felt embarrassed, mad at myself, and just tired. Tired of feeling like the world waits for people like me to slip. But the truth is, this happens to so many people coming home. We don't always know what's real, what's required, or who to ask. And scammers know that fear is loud.

Now, I tell this story so others won't fall for things like this. I'm learning to slow down, ask questions, check things out, and trust that reaching out is strength, not shame. This was a painful lesson, but it made me more aware, more cautious, and more connected to the people who truly have my back.

A.3 Personal Narrative 3: Toll Scam Post-Incarceration

For me, when I first got out of prison, I think one of the biggest things that I had to deal with was the fact that everything was a potential landmine. It didn't stop then, and it still continues today, that I know it takes absolutely nothing to rock the foundation of my parole and really send me back. Part of the fear comes directly from the idea that authority will have a different or jaded view of something I'm doing while free, because it's just that bit of rapport and relationship building that has kept me otherwise safe. Not that I've done anything wrong, but anything can be misconstrued, and that's where the danger of the scams really does come in. I know for me, part of the idea of scams in and of itself is the fact that they use authority in which to execute the scam. So, most things like a toll pass or a speeding ticket all come fraught with disaster. All it's going to take is the one scam that says, "Hey, a camera caught you going through an intersection after the light turned red," and I, like most people in my circumstance, would just simply panic long enough to think, "I don't want to go back to prison. Whatever this is, I'll do whatever it takes to make it go away, to include payment." Even though I am firm in my driving ability, it still only takes a subtle suggestion to invoke the fear. That's the stark-raving reality of what we have to deal with, especially when under the directives of community corrections. It's imperative that we become better educated about what these scams are, how they develop, and how they're implemented, because it's incredible, the amount of fear that is already consuming a person who has been recently released. The last thing they need is somebody faking the thing they hate the most or fear the most, and that's the punishment and the idea of going back to prison. I know for me, every rogue parking charge or Good-to-Go pass charge all comes with some level of danger. What happens if I don't pay? In reality though, I never needed to, but because I have been reaffirmed that the Department of Corrections and their Community Custody Division doesn't view wrongdoing with the same measure of evidence that the courts do, my fears become a scammer's best target.

B Surveys

B.1 Workshop Participant Survey

(all free text besides Q11 which had a yes/no checkbox + 'other' free text option)

1. Which years were you incarcerated?
2. How long has it been since you were released?
3. Did you have access to any computers or computer skills while incarcerated (including educational/business classes)? If so, what were they?
4. How comfortable were you with technology before being incarcerated?
5. What technology did you use regularly before you were incarcerated (e.g. landline telephone, cell phone, computer, iPod, iPhone, etc)?
6. What technology do you use regularly now?
7. How has technology changed since you were incarcerated? What was new to you when you were released?
8. Considering technology, what have been the most difficult changes to adapt to?
9. Do you have any worries when using technology? If so, what are they?
10. Where do you normally go to for information/help regarding technology challenges?
11. Are you ever worried about your information (e.g. messages, internet browsing history, social media posts) being viewed by others?
12. If you answered yes: Who are you worried about seeing that info?
13. If you answered above: Do they view this information? Who and how regularly?
14. Do you ever get unsolicited phone calls, texts, or emails, from sources you don't know or trust?
15. Do they ever ask for money or personal information?
16. What do the calls/texts/emails try to convince you of?
17. How do you respond initially to these calls/texts/emails?
18. How did this encounter progress or end up? Was it a scam?
19. If so, what did you do about it?
20. What information did the scammer have about you (e.g. name, DOC number, phone number, email, incarceration history, employment history)?
21. Do you ever use apps to make money, win points, earn rewards? If so, what are those apps?
22. Is there anything else you'd like to share regarding digital literacy, adapting to the digital world post-release, scams, data privacy, surveillance, electronic monitoring, community custody internet restrictions, etc?
23. Was this workshop useful?
24. What worked well?
25. Is there anything you wish was different about the workshop?
26. What should we change for the next one?
27. What topics do you want to learn more about?
28. What topics do you think we should cover in future workshops?
29. Is there anything else you'd like us to know about your experience today?

B.2 Workshop Volunteer Survey

(all free text)

1. What questions did this participant have for you?
2. What were some challenges in answering the question?
3. Did anything surprise you in your conversation?
4. Did they have any different conceptions of technology compared to you?
5. Anything else you want to share about this conversation?

B.3 Scam Follow-Up Survey

1. Did you attend our Computer Basics for Reentry Workshop (in September 2025)? (yes/no checkbox + other freetext)
2. Have you ever fallen for or experienced a scam? (yes/no checkbox + other freetext)
3. Have you received or engaged with a scam claiming that they were the government, authorities, law enforcement, a judge, the DMV, etc? (yes/no checkbox + other freetext)
4. Did they threaten arrest, fines, warrants, or other legal punishment, if you did not comply? (yes/no checkbox + other freetext)
5. Why do you think you engaged with the scam? Options (checkbox):
    - They were threatening legal punishment (like rearrest)
    - They were threatening financial punishment (like fines)
    - I didn't know or expect it to be a scam
    - I didn't mean to engage - it happened too fast/without my knowledge
    - I haven't engaged with a legal/fine related scam
    - other (free text)
6. Have you ever experienced or engaged with a scam claiming to want a sexual or romantic relationship/message from you? (yes/no checkbox + other freetext)

7. Why do you think you engaged with the sexual/relationship scam? Options (checkbox):
    - I engaged because I was kind of lonely after getting out of prison
    - I engaged because I didn't know/expect it to be a scam
    - I engaged because I was scared
    - I didn't engage because I was scared
    - I didn't engage but they still claimed to have something on me
    - Haven't engaged with a relationship-related scam
    - other (free text)
8. Have you ever experienced or engaged with a scam that claims they have a job or financial opportunity for you? (yes/no checkbox + other freetext)
9. Why do you think you engaged with a job related scam? Options (checkbox):
    - Really needed money
    - Was curious
    - Was trusting of them
    - Haven't engaged with a job-related scam
    - other (free text)
10. Have you reported any of these scams? (yes/no checkbox + other freetext)
11. If you answered No, why didn't you report the scam(s)? Options (checkbox):
    - Didn't want to interact with law enforcement
    - Didn't know who to report to
    - Didn't want to get anyone in trouble
    - Felt ashamed or embarassed
    - other (free text)
12. How often do you see or receive potential scams? (free text)
13. Do you think you are better or worse at identifying scams than people who have not been incarcerated? (free text)
14. What about you or your experience makes you better or worse at identifying scams than people who have not been incarcerated? (free text)
15. Is there anything else you want to share about scams, incarceration, digital literacy, technology, reentry, etc? (free text)

C Qualitative Codebooks

The **workshop participant survey codes** included:

- Participants are worried about DOC/CCOs getting their information
- Experiencing identity theft or scam immediately after release
- Digital skills gap due to long isolation
- Dependency on shared or monitored networks
- Internet restrictions, electronic monitoring, or "no-social-media" clauses
- Trauma-related digital distrust
- Even when help is available, participants rely on friends or family for support rather than verified sources
- Workshop improvement takeaways

The **workshop volunteer survey codes** included:

- Highly practical help desired and tied to daily living, education, and employment
- Digital divide (no devices, confusing software, limited experience)
- Tech support sessions turned into personal storytelling
- Monitoring
- Participants wanted to learn but often carried shame, frustration
- Workshop improvements takeaways

The subsequent **combined codebook**:

- Scam experiences
- Digital monitoring
- Digital skills gap
- Digital education gap
- Asking technology questions in interpersonal / community / friend / family conversations
- Practical and educational help desired (for future workshops)

The **scam follow-up survey codes** included:

- Government scams + susceptibility
- Relationship scams + susceptibility
- Job scams + susceptibility
- Digital literacy
- Trauma-related distrust for reporting
- Better at identifying scams (e.g., due to life experience)
- Worse at identifying scams (e.g., due to digital divide)