

USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Nice to Know You're Not Alone: Co-designing Community-centered Online Safety and Privacy Education with Librarians

Tanisha Afnan, Sheza Naveed, Griffin Christie, and Jackie Hu, *University of Michigan;* Byron M. Lowens, *Indiana University Indianapolis;* Allison McDonald, *Boston University;* Florian Schaub, *University of Michigan*

https://www.usenix.org/conference/soups2026/presentation/afnan

This paper is included in the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security
is sponsored by USENIX.

Nice to Know You're Not Alone: Co-designing Community-centered Online Safety and Privacy Education with Librarians

Tanisha Afnan,[1] Sheza Naveed,[1] Griffin Christie,[1] Jackie Hu,[1]
Byron M. Lowens,[2] Allison McDonald,[3] Florian Schaub[1]
[1]*University of Michigan* [2]*Indiana University Indianapolis* [3]*Boston University*

Abstract

Online safety and privacy literacy education is often offered in community settings and spaces, such as libraries, which allow for educational offerings tailored to community needs. However, such efforts are often resource constrained and place substantial burdens and responsibility on individual educators. We present findings from a co-design study with librarians offering online safety and privacy education in public and academic libraries to address their challenges in bringing these trainings to their communities. Fourteen participants across four co-design workshops engaged in guided prompts, discussions, and activities to develop innovative and sustainable ideas for enhancing community-centered online safety and privacy education efforts. Educators also ideated promising directions for independent learning resources that could deepen patrons' understanding of relevant topics on their own time after a training workshop. We discuss the implications of our findings for strengthening community-centered online safety and privacy education and resources.

1 Introduction

Despite growing online safety and privacy risks, privacy and security literacy remains critically underdeveloped [12, 63], leaving many individuals without the necessary skills to protect themselves online. Prior work suggests that individuals turn to informal channels, such as friends or family members, for security and privacy advice rather than consulting educational resources [11, 44, 47]. This reliance on informal sources highlights the importance of *community-engaged educators*, such as public librarians, who serve as trusted peers and sources of knowledge within communities. They can provide privacy and safety education that is contextually relevant and accessible in the form of workshop series, training sessions, or drop-in hours for community members [1, 53]. In prior work with community-engaged educators, Afnan et al. [1] found that, in contrast to academic distinctions between privacy and security, community-engaged educators' literacy efforts often integrate privacy, security, and online safety (e.g., information vetting) competencies as a reflection of the increasingly integrated threat landscape online. Educators face multiple challenges in leading this vital work, such as time, resource, and organizational constraints, that limit the impact and reach of their educational offerings [1]. In addition, infrequent and comparatively short workshops and trainings make it difficult for community-engaged educators to go beyond basic topics, highlighting a need for trainings with complementary independent learning resources that could allow interested students to deepen their knowledge regarding more advanced privacy or online safety topics [1].

Building on Afnan et al.'s findings [1], our study focused on supporting community-engaged privacy and online safety education with librarians by generatively identifying individual and collective opportunities for addressing their needs and challenges in context. Specifically, we conducted a participatory design study with librarians across the U.S. who offered online safety education to diverse populations in public and academic libraries. Libraries offer an ideal context for this research due to their established role as trusted community hubs in the U.S. that historically have provided patrons access to information, resources, and educational programs across various subjects [26]. Our primary research questions were:

RQ1: How do library educators conceptualize privacy and online safety literacy and approach community-engaged educational offerings for their communities?

RQ2: What are the barriers and challenges library educators face in delivering privacy and online safety education that is responsive to different communities' needs?

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

RQ3: What resources do library educators envision to help overcome these barriers?

Across four participatory design workshops with 14 participants in total, we jointly identified promising research, policy, and design directions that could help mitigate challenges in community-engaged privacy and online safety education. Our findings (1) reaffirm the critical need for tailoring support to the diverse needs of library patrons in different contexts, (2) further illustrate challenges with limited resources and identify issues with the utility of existing educational materials, and (3) demonstrate a need for more interactive and accessible learning resources that can deepen learners' understanding of relevant topics beyond offered classes and workshops. Our participants also discussed (4) the need for professional development opportunities, including more interchange among librarians and connection with other community-engaged educators offering privacy, security, and online safety trainings and professionals in related fields.

2 Related Work

We discuss related work on privacy/security education in the library context, on libraries as hubs of community education, and on participatory design in privacy and security research.

2.1 Privacy and Security Education Efforts

The volume of privacy and security advice available online can overwhelm users seeking information [48, 49], while simultaneously leaving them uncertain about which steps are most important for them to prioritize for their individual privacy needs. Redmiles et al. found that age, socioeconomic status, and education level deeply influence an individual's likelihood of engaging in safer online practices [46]. Individuals are also more apt to accept guidance from peers, such as family and friends, than from formal resources [44]. Building on this insight, some research has explored training community members to serve as peer educators [21, 22, 39].

More formal cybersecurity education efforts in K-12 settings [52] and within higher-education institutions, such as Egelman et al.'s Teaching Privacy Program (TPP) [13], often take a one-size-fits-all approach, which may exclude material relevant to marginalized users with identity-specific concerns [1]. We find this concern voiced by educators in some of the limited research that has examined community-engaged privacy/security education initiatives. McLeod et al. found that while school teachers preferred adaptable, easy-to-use, low-tech security resources that emphasized critical thinking, resource creators were more inclined to focus their designs on emerging cybersecurity trends, interactivity, and gamification, leading to a misalignment among the two groups as teachers desired resources that were more directly relevant to student concerns, rather than more universally prescriptive [35]. McLeod et al. recommended that content creators and security experts should make an effort to involve teachers in resource development to better meet students' needs [35]. Similarly, Afnan et al. [1] found that community-engaged educators teaching privacy and security topics were often aware of available educational resources (e.g., EFF) but often did not use them, opting to create their own, due to difficulties in adapting existing resources to their communities' needs.

Community-engaged educators, specifically librarians, have also produced a growing body of privacy and security resources in recent years [57–60]. Projects such as Towson University's "Cybersecurity Labs and Resource Knowledgebase" (CLARK) demonstrate how digital libraries can centralize peer-reviewed teaching modules that make security and privacy instruction more modular, shareable, and adaptable across institutions and contexts [58]. Users can customize lesson selections based on personal interests or the needs of their patrons. CLARK and other digital libraries [20, 41, 54] ensure patrons can pursue privacy/security learning with continuous and open access to materials they can use independently or in conjunction with a community-engaged educator. National library organizations have created privacy and security curricula, field guides, toolkits, and workshop materials for use in public libraries [43, 67]. Local initiatives, such as the "NYC Digital Safety: Privacy and Security" program, illustrate how library systems have developed privacy and security programming, offering patron workshops, training resources, and community partnerships [37].

Privacy and security education has become increasingly recognized as an evolving responsibility within librarianship rather than a peripheral concern. For example, in 2014 the American Library Association expanded its privacy 'mandate' to account for teaching patrons about how behavioral tracking practices conducted by government agencies and commercial entities can target their metadata [15, 61]. However, how libraries and librarians build capacity for privacy education and how this education is delivered remains understudied. Hartman-Caverly identified multiple approaches for privacy literacy initiatives, including knowledge-sharing networks and privacy communities of practice, to help librarians respond confidently to evolving privacy and safety risks and patrons' technical challenges [19].

This body of work demonstrates the range of privacy, security, and online safety educational efforts, and the promising role of librarians in designing and delivering privacy education that is responsive to their communities' privacy needs.

2.2 Libraries as Community Education Hubs

In the U.S., libraries have a long history of serving as hubs for community education, often offering free access to continued learning opportunities. In the digital age, they have adapted to provide access to computers, the internet, and digital liter-

acy training, including topics related to privacy, security, and online safety [8]. Librarians often act as privacy and security educators [1], and serve diverse audiences, with library patrons varying dramatically in age, ethnicity, and income-level, among other characteristics [8].

Libraries have been noted as promising spaces for participatory action and design research for public education efforts, as they are able to work across sectors in various contexts to address community needs [33, 65, 66]. Collaborative research conducted in partnership with librarians and community members can yield resources, training, and support for community-led initiatives that can help improve local conditions and later be replicated to create greater social change [26].

Kozubaev & DiSalvo outline how researchers can develop technologies and design solutions that consider the challenges and opportunities faced by librarians [26]. They point out the need to design for everyday heterogeneity and contingency, i.e., the complex set of tasks involved in a librarian's daily work that range from managing circulation desks, shelving books, and assisting patrons to providing tech literacy training or children's programming. Librarians' educator role is also often complex and contested. School librarians must balance instruction with collections and technology management [36]. Instruction librarians in academic settings characterize themselves as "librarians who teach" rather than as just teachers or librarians, pointing to a unique role that is often underrecognized by their institutions [4, 25]. Librarians interested in further instructional training are instead expected to prioritize training relevant for core responsibilities [30].

At the same time, public librarians are asked to introduce patrons to a "staggering number" of privacy and security tools and practices while facing knowledge gaps, time limits, and budget constraints [31]. In practice, many librarians use only a small subset of available privacy/security tools and remained uncertain about how those tools actually work [29]. Hartman-Caverly and Chisholm, therefore, recommend developing resources that prioritize privacy/security literacy and critical thinking skills over tool-specific trainings that may quickly become outdated [18].

2.3 Participatory Design in Privacy & Security

We used participatory design (PD) research methods [24] to involve librarians as collaborators to co-develop ideas for more nuanced and responsive privacy and security learning resources. PD emphasizes collaboration, shared understanding, and participant empowerment, to ensure that the outcomes reflect the collective knowledge and realities of stakeholders [9, 24, 50, 55]. In a review of participatory design applications, Robertson and Simonsen highlight the need for broader participation in co-design processes, emphasizing the importance of including individuals beyond traditional user groups within shifting digital landscapes [50]. They also discuss the importance of genuine partnerships with users, arguing for more community-engaged and embedded collaboration. This sentiment is reflected in Costanza-Chock's design justice framework, which emphasizes a shift in design practice away from 'expert' designers and developers towards participatory design processes that empower marginalized communities to shape the technologies and systems that impact their lives [9].

Some prior privacy and security research has utilized PD techniques [7, 17, 23, 27, 56, 64]. For example, Kumar et al. explored how games and storytelling can be used to teach children about online privacy [27]. Yao et al. employed co-design to better understand desired privacy controls for smart home devices [64]. Such prior PD studies often focused on potential end users, who may not be fully aware of relevant privacy risks and issues that affect their larger communities. In contrast, to advance community-engaged privacy/security education, we worked with community-engaged educators as co-creators. Our participants held valuable technical and pedagogical expertise as teachers, while also possessing intimate knowledge of the needs of their patrons as individuals embedded within the broader communities they serve.

3 Methods

We employed a participatory design approach, grounded in community-centered collaboration [3, 45], to elicit librarian educators' challenges in offering privacy and online safety eduction, how to support library educators in this work, and how to support library patrons' learning about online safety, privacy, and security within and beyond trainings. In contrast to prior work that focused primarily on identifying challenges of community-engaged privacy/security educators and librarians (e.g., Afnan et al. [1]), our study engages librarians generatively to identify individual and collective opportunities for addressing participants' needs and challenges in context. All study materials are available in an OSF repository.[1]

Ethics statement. Our study was reviewed and approved (exempt) by the University of Michigan's IRB. Participants were informed about the study purpose and consented to workshops being recorded. Transcripts were anonymized after analysis to protect participant privacy.

3.1 Recruitment and Demographics

We recruited librarians based in the U.S. who had experience leading classes or training sessions on online safety, particularly topics related to privacy and security, as prior work has found that these topics are often intermixed or integrated in community education efforts [1]. We reached out to libraries across the U.S. that advertised digital literacy trainings on their websites, which we identified through online searches. We also utilized large mailing lists dedicated to librarians to

[1] All study materials are provided here: https://osf.io/2qwjr/overview?view_only=479977c650a7434faddb738f9a0647f1.

Table 1: Participants overview

Workshop	ID	Library Type	Library location and context
1	P01	Public	Rhode Island, suburban
1	P02	Public	New Jersey, urban
1	P03	Public	Michigan, rural
1	P04	Academic	Massachusetts, suburban
2	P05	Academic	Pennsylvania, suburban
2	P06	Academic	New York, urban
2	P07	Academic	Massachusetts, suburban
3	P08	Public	Michigan, suburban
3	P09	Public	Maine, suburban
3	P10	K-8 School	Rhode Island, rural
3	P11	Public	Michigan, urban
3	P12	Public	Rhode Island, suburban
4	P13	Public	Rhode Island, rural
4	P14	Academic	Oregon, suburban

circulate our recruitment messages. Lastly, we reached out to existing contacts at libraries offering such trainings.

Interested individuals completed a screening survey to determine eligibility. We then contacted them individually via email to gauge their availability before assigning them to one of our workshops. Given the specificity of our eligibility criteria and the significant time commitment, all participants received a $120 virtual gift card for participating. Due to these factors, we also encountered some minor recruitment challenges, including no-shows, scheduling conflicts, and persistent interest from individuals who were not eligible.

Our sample included 14 librarians (5 men and 9 women) serving a variety of communities. They worked in various states, as well as in a mix of urban, suburban, and rural environments. The sample included 8 public librarians, 5 academic librarians (including one from an online university), and 1 school librarian. These librarians served diverse populations, including college students, older adults, children and adolescents, low-income, job-seeking, and homeless adults, as well as members of various minority ethnic and racial groups. Though participants had little to no formal cybersecurity training, all held master's degrees from ALA-accredited institutions, with 5–20+ years of tech teaching experience. Participants primarily offered in-person trainings and workshops.

3.2 Study Design

We conducted four participatory design sessions with groups of 2–5 participants in March and April 2025. We aimed for 4–8 participants per workshop, but due to no-shows and last-minute cancellations our group sizes varied. While most workshop activities were designed for small groups, we found that they still worked well for even our smallest session (2 participants) with minimal adaptations, allowing for longer individual reflection and sharing by participants. The duration of workshops ranged from 2 hours and 18 minutes to 2 hours and 50 minutes (excluding breaks), largely due to the varying group sizes. Workshops 1 and 3 included primarily public librarians, Workshop 2 only academic librarians, and Workshop 4 was mixed (see Table 1). Despite participants' diversity in library and community contexts, we observed similar patterns, ideas, and themes emerge from all four workshops.

All workshop were conducted online on Zoom to enable participation independent of location and accommodate librarians across time zones. Participants were asked to keep their video turned on to facilitate a more natural conversation and encourage active participation in the workshop activities. Workshops were audio- and video-recorded, allowing us to reference participants' expressions during analysis and identify speakers which can otherwise be challenging in a group setting. Recordings were transcribed with Zoom. In all workshops, two researchers were present; the first author led the workshop and facilitated activities, another team member took field notes and documented artifacts for later analysis.

To translate hands-on activities to an online environment, we utilized Mural, an online whiteboard application with built-in Zoom integration. Co-design workshops and activities were structured following best practices for virtual participation, including the Community-Led Co-design Kit [3], which adapts tenets of inclusive co-design and design justice [9]. We provide an overview of our core workshop activities below; our full Facilitation Guide is available in our OSF repository.

Prompts, discussions, and activities, were designed in alignment with our research questions, and were pilot-tested with all co-facilitators prior to deployment. We initially considered three one-hour-long sessions, but decided to adopt a single-session format to better accommodate participant schedules (i.e., it's easier to dedicate one morning, afternoon, or evening for a workshop than to block time over multiple days or weeks). Our workshops were loosely based on the three-phase design process from the Community Led Co-design Kit [3] and consisted of the following activities (see Figure 1):

Introductions. Facilitators and participants introduced themselves to the group, including what library they work for and where it is located.

Warm-up. The warm-up phase focused on getting participants comfortable with the online workshop setting. We introduced Mural as a tool. Participants then completed a *Four Quadrants Activity*, in which they filled out four prompts: what they bring to the workshop, challenges they face, communities they serve, and hopes for the group. Participants then shared responses to build shared understanding of group strengths and needs.

Discovery. Next, we focused on collaboratively defining and understanding privacy and online safety education as taught by our participants. Guided discussions and exercises elicited participants' goals, challenges, and desired outcomes within their library settings, as well as current teaching workflows.

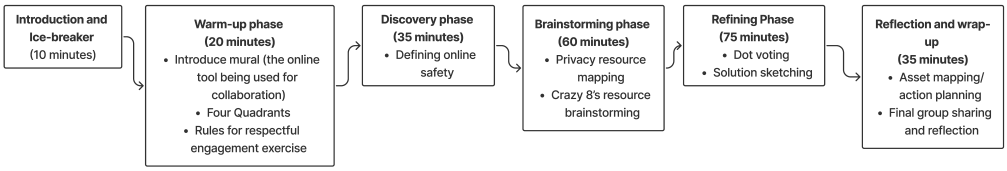


Figure 1: Overview of the workshop structure and activities.

A core activity focused on *defining online safety.* Participants individually brainstormed what "online safety" means to them, discussed their definitions in pairs, and then shared with the whole group. This activity helped ground each session around the concepts and terms participants used.

Brainstorming/ideation. This phase centered on generating solution ideas for the gaps and challenges in participants' efforts. Participants engaged in various brainstorming techniques to encourage ideation, without being limited by practical considerations. In a *privacy resource mapping* activity on Mural, participants identified and categorized existing resources they were familiar with and may reference for creating their programming. Participants further did *Crazy-8s brainstorming* on Mural, sketching eight different ideas within eight minutes. Participants could focus on any of the previously discussed challenges in their solution ideation.

Refinement. This phase focused on collaboratively critiquing, refining, and expanding upon promising solution directions. Participants presented their individual solution ideas and engaged in clarifying discussions. They then collectively voted on the most compelling solutions in a *Dot Voting* activity, in which everyone reviewed the ideas brainstormed in the Crazy-8s activity and voted on the four most promising ones. Next, participants collaboratively or independently refined one of the highest-voted solutions for future implementation in a *solution sketching activity*, in which they used three frames to illustrate how the idea would work in practice.

Reflection & wrap-up. The workshops concluded by gathering any final thoughts from participants. In an *action planning activity* participants created concrete plans for bringing solution ideas to their home libraries. This included identifying key partners, key actions, and a concrete timeline for eventual implementation. We also included time for open questions and interest in continued collaboration at the end.

3.3 Data Analysis

We used thematic analysis following Braun & Clarke's process [5] to identify themes in educators' experiences, challenges, and suggested design solutions for improved online safety and privacy education. Analysis began with affinity diagramming of design artifacts and field notes, followed by inductive coding of the transcripts to develop a comprehensive set of themes. Initial findings were regularly discussed with the research team, who offered feedback and advice during codebook development. Finally, we engaged in iterative rounds of deductive coding with the final set of themes established in the codebook. All analysis was conducted with ATLAS.ti, a qualitative data analysis software with image analysis functionality. The first author engaged in a solo coding process due to being the primary facilitator for all workshops, following guidance by McDonald et al. [34].

In reporting our findings, we prioritize participants' verbal explanations and quotes, using visual artifacts to exemplify points where useful, because participants discussed their ideas extensively and often with more detail and nuance than their digital sketches conveyed on their own.

3.4 Limitations

Our study has some limitations. Our study is situated in the U.S. library context. Libraries hold a distinct role in communities in the U.S., being publicly-funded and widely accessible. Libraries are regarded as trusted community institutions that provide digital literacy support and social services. As is typical with qualitative and participatory design research, our work is not meant to generalize or represent all perspectives or the needs of all librarians who teach privacy or online safety topics, or the challenges and needs experienced by community-engaged privacy and security educators in other roles, countries, or cultures. At the same time, our findings provide new insights and participants' identified promising solution ideas and directions.

4 Findings

In this section, we unpack our participants' experiences and challenges in teaching their communities about privacy and security topics, and identify promising new directions for designing learning resources.

4.1 Conceptualizations of Privacy and Security

At the beginning of each workshop, we led participants through a series of small group discussions so both facilitators and other participants could learn about their experience with teaching privacy and security topics.

Privacy, security, and online safety part of digital literacy. While we recruited library-based educators teaching privacy, security, and online safety, most participants identified their work more broadly as digital literacy education. This framing was especially prevalent with public librarians, particularly in workshop 1. While academic librarians across sessions were less likely to be teaching basic digital skills (e.g., creating an email account), these participants largely agreed that their work focused on teaching other essential skills, such as how to navigate online learning management systems or use scholarly databases. This underscores an important finding, that, within current library instructional contexts, *digital privacy and its related issues are rarely taught in isolation*. Privacy, security, and online safety were often treated as interchangeable terms, confirming findings by Afnan et al. [1], and taught couched within a broader set of essential digital skills.

> "I've been in libraries for 8 years. [...] I do monthly digital literacy trainings here at the library, and then I also do like a walk-in session once a month, where people can just come in with whatever. Mostly it has been older adults from a digital literacy standpoint, and the response is good, but I know there are dozens and dozens, if not hundreds, out there that need more help with staying safe online." (P3)

Building a shared definition for online safety. When prompted to define what online safety and privacy meant to our participants, and what topics or skills they taught in relation to that understanding, most participants tried to balance a conceptual understanding of different privacy and security topics with teaching practical skills. While the specific topics varied based on each audience's contextual needs (e.g., participants serving more non-English speaking patrons focused more on password hygiene than privacy on TikTok—a topic brought up by teen or child services librarians), participants worked on a collective definition of online safety within each workshop. These definitions were similar, focusing on *online autonomy, anonymity, asset protection, consent, and skepticism,* with slight variations among workshops. For example, in workshop 2 which included only academic librarians, there was a stronger focus on maintaining online anonymity, particularly for international students facing increasing concerns about their immigration and visa statuses.

> "A thing that came up in our group between a few of us was, the idea that like you can't really have [online] safety without a deeper understanding of the concept. And especially... like I brought up the concept of autonomy, which is one that I talk about with patrons a lot, and like understanding where your information is going, how it might be used, how it might be misused and kind of what you're trading off whenever you're using these online tools." (P9)

This reflects a general understanding among participants that privacy, online safety, and cybersecurity are not isolated concepts and skills but rather deeply integrated [1].

How privacy and online safety is operationalized. While topics varied, how participants taught these topics, as well as the challenges they encountered, were highly similar. For many, their position as community educators allowed them to align their materials and programming closely with their community's needs. For example, scholarly reference librarians working with college students often incorporated guidance on navigating social media safely, especially with tips related to online activism, into their instruction. However, many public librarians, serving primarily older adults who are less likely to use these platforms, tended to exclude social media advice. However, some topics were covered by nearly all participants, including password hygiene, information vetting, scams, and online harassment.

> "We work with different demographics, and we both immediately recognize that. And for me, [I always teach] about passwords and social media. But for [other participant who works with school children], her students are actually mostly not on social media because of their age, but the big thing for her is online video games and passwords. [...] We're both worried about weak passwords and how that could lead to things like someone hacking into a bank account." (P10)

Even though the instructional context and primary audiences varied among them, our participants shared substantial similarities and agreement in their sentiments, motivations, and underlying conceptualizations of online safety.

4.2 Challenges in Librarian-led Education

We uncovered several shared frustrations and challenges among participants across the different contexts in which they worked. Our findings affirm those from prior work with librarians and community educators but add nuanced insights on how participants cope with specific challenges.

Limited resources. The biggest obstacles to participants' privacy and security teaching efforts were a lack of time and the overwhelming needs of their learners. The current model, often limited to a monthly, hour-long lecture-style class, was found to be insufficient for covering the breadth of online safety topics relevant to their communities.

> "The main challenge that I find is just demand on my time. Like there's only one of me in the department. [...] Sometimes I feel like I shortchange the patrons because I just don't have time to meet with them as frequently or as long as they really need." (P9)

Additionally, participants expressed concern that this model not only hinders effective learning, but also increases demands on educators to find supplementary support mechanisms.

> "What I try to impress upon people is that you know, digital literacy is like learning to read and write. It takes lots of practice, and that a one hour class or a 90 min class isn't necessarily going to stick with you unless you practice it, and kind of reinforce that information through the week. I try to find websites or exercises or things that people can do once they leave the classroom." (P8)

Existing educational resources are diffuse and perceived as inaccessible. To explore further, we asked participants to consider the existing educational resources they relied on. Each workshop group engaged in a resource mapping activity, in which participants shared and categorized educational resources related to privacy, security, and online safety, including those they use for preparation or share directly with learners. Across workshops, participants quickly recalled numerous resources. Most shared a mix of organizational resources that they, or someone at their library, had developed, and public websites or articles. Popular resources included guides and advice from the Electronic Frontier Foundation [16], the Library Freedom Project [32], the Federal Trade Commission [14], and the American Library Association [2].

Through mapping these resources, participants identified several issues with them. While each identified multiple resources, participants felt there was no *one* source they could comfortably turn to when preparing their classes. Participants in each workshop described the tedious process of searching for and aggregating information from multiple sources, which they then would translate into more digestible lessons.

> "[When I'm] making a class, definitely one of the constraints is that it's a time competition with my desk duty as just being like a librarian during the day when I'm not doing the service specific to a class or tech help. I would love it if there were classes already done, like if I didn't have to create it from scratch. Because I don't have like one place [I can go to], it's always like scattered. And then it's hard to then tell a patron, 'Hey, just go to this website to keep learning about it' because I had to gather the pieces to make the classes [from multiple places] myself." (P13)

Through our resource mapping activity, which encouraged participants to categorize resources based on intended audience, complexity, medium, and topic, participants began to recognize trends across existing resources. In particular, they identified what kinds of resources were missing that would most benefit their work and their patrons' learning. For example, in workshop 3, the group observed that most mapped resources lacked a clear target audience and were primarily geared towards beginners, which was seen as limiting their usefulness for diverse learners and contexts. Some participants also found current resources to be inaccessible. For example, a public librarian in workshop 1, serving a diverse urban area, struggled to find shareable non-English resources. Educators were also reluctant to recommend resources that involved a sign-up process, such as Northstar's self-guided educational programs [40], or that were not adapted for mobile devices.

> "I mean, I listed some websites that I highly rely on, that I recommend to people. But most of my [learners], the senior citizens, are not going to go to Tom's Hardware. They're not gonna figure it out, even though it's a wealth of knowledge. [...] It just has to be as simplistic as possible. And you know the fewer clicks, no accounts needed, just get into a video and watch it. Or pull up a document, whatever it is." (P3)

For resources that participants did not feel were aimed at beginners, they instead found them to be laden with technical jargon. These resources were geared towards individuals already confident in their online safety skills, and similarly failed to meet the needs of the diverse learners they served.

> "Most of these are written for relatively well resourced people who have at least a basic understanding of how to use their devices already. I feel like a lot of it is targeted at sort of like a savvy person who probably owns their own device, probably multiple devices, and is experienced enough with them to know how they work and to know enough of the vocab to interpret the information that's on these websites." (P9)

This sentiment, that even resources targeted at end-users tended to still be too difficult to use, surfaced across workshops.

> "What's hard is the [resources] that I think that help people also require a more sophisticated understanding of even how to use a computer. So like, I think [for example] the data detox kit resource. I know that one tends to be module based. So you have to go through steps and think through it. And that can be really hard for people who are like at the beginning stages of computers, but they're also the ones who are most vulnerable." (P4)

Participants felt such resources were beneficial for developing teaching materials, but they could not share them directly with their patrons. Many participants also expressed a need and appreciation for printable materials that could be handed out on paper.

> "I think that the most valuable resources on this list for me in terms of direct patron-facing resources tends to be ones that have things I can print. I think, for a certain type of learner, maybe videos and interactive things and websites work well. But the vast majority of the patrons that I work with don't want to be told to go to a website to go learn more about this topic. They want a book, they want a handout. They want a human being who's going to help them with it." (P9)

These findings contrast with efforts by organizations such as the EFF [16] and the Library Freedom Project [42] to produce resources in easily digestible and printable formats. This points to a disconnect between educational efforts by non-profit organizations and community-engaged educators, although they share the same goals of fostering privacy, security, and online safety education. This is perhaps partly the result of limited time and a plethora of online resources—even when our participants are putting in the time to find and curate resources, it can be overwhelming to evaluate all of the offerings that existing organizations provide. Our findings further point to a common need by educators to adapt materials to their communities' needs and context, which made re-use of existing resources challenging.

Must advocate for educational offerings to both supervisors and patrons. Beyond time constraints, participants also struggled to convince potential learners and higher-ups of the value of online safety and privacy education. Several public librarians reported low attendance in their classes, noting that these topics often take a backseat to patrons' more immediate concerns, such as navigating homelessness.

> "Not that many people come to learn about things. And then also convincing people that this is something they should be concerned about is difficult. And often I feel like I'm shouting into the wind that this is a big problem you should care about. It's hard, because there are a lot of things to care about, particularly at the moment." (P14)

Academic librarians, similarly, found that student participation heavily depended on the attitudes of administrators and faculty. The academic librarians in workshop 2 agreed on the need for generating *faculty buy-in*, i.e., the persuasive effort they felt was necessary to gain faculty support for their library initiatives.

> "It's hard to find time with students, and, like the easiest way to find time with students is if there's faculty buy-in. But most faculty don't see this as necessarily important. [...] And so we've done things like had faculty workshops on different topics that have sort of helped to have the people see how helpful, whatever information is presented, could be for their class, but that also requires, like the faculty to be interested. They're not required to attend any of that stuff." (P12)

These findings suggest that the effort our participants put into creating and offering privacy, security, and online safety trainings and resources is often experienced as insufficient, requiring them to expend considerable additional effort on advertising and advocating for these offerings to make sure they are being utilized by patrons, which frustrated participants.

Educators feel isolated in their efforts. The undervaluing of this critical work left several participants feeling isolated in their mission to improve their community's privacy and security literacy, with many describing a sense of loneliness that occasionally hindered their creativity and motivation. This sentiment was often coupled with participants' frustrations and struggles with staying up-to-date with new technologies and their associated privacy risks and security threats.

> "Technology is evolving so fast that I often either don't have the time, or even the access to [keep up]. Some people would walk in with, you know their smartwatches, and I knew about smartwatches, but I didn't have one in my library, and I didn't purchase one for myself, so I would just be sitting and learning alongside the patron." (P1)

4.3 Better Supporting Learners and Educators

Participants brainstormed and collectively refined solution ideas to address the challenges they experienced. Solution ideas primarily focused either on (1) supporting learner needs or (2) addressing educator constraints to better meet learners' needs. Table 2 provides an overview of the most popular directions identified by participants.

4.3.1 Learner-focused solution ideas

Participants generated various ideas for educational resources that could deepen learning beyond the trainings they offered at their libraries. Several similar solutions emerged across workshops, suggesting a consensus on effective strategies for privacy and security literacy education among participants.

Interactive educational resources and processes. One theme focused on making educational resources and processes more interactive to keep learners engaged for longer and beyond single workshops. Educators, particularly those who worked with adolescents and college students, were especially interested in gamifying learning opportunities. P13 & P14 in workshop 4, for example, despite coming from different library contexts (public and academic), found affinity in thinking about their similarly younger primary audience. They worked together to refine ideas to reinforce privacy decision-making with an online role-playing game (see Figure 2).

Table 2: Most popular and recurring solution ideas across our participatory design workshops.

Solution Type	Audience	Description	Examples and Quotes
Interactive Educational Approaches	Learners	Solutions that promote active learning by incorporating interactive elements or collaborative activities	Take-home worksheets that include guided exercises for practicing specific skills: *"An idea I have is for take-home child & parent worksheets after discussing online safety in class. The reason why I love this one is because it is very simple and very easy to do, and I think it helps with that home to school connection. And then [...] it opens the opportunity for parents to have those conversations with their children at home."* (P10)
Accessibility-focused Approaches	Learners	Solutions that "meet students where they are" by not requiring a personal device or travel	Providing tactile resources instead of only digital resources: *"I get really frustrated by people who try to solve problems of digital literacy with digital tools. I feel like there's a lot of entities out there who are like, we'll just make an app, or we'll just make a website [...] For the vast majority of the patrons that I work with, they don't want to be told to go to a website to go learn more about [something]. They want a book, they want a handout. They want a human being who's going to help them with it."* (P6)
Non-Class Based Library Offerings	Educators & Learners	Ideation directions that focus on expanding library educational services beyond structured class sessions	Cybersecurity community challenge for adults to learn about new topic and then teach their children: *"Maybe some type of monthly community challenge for adults to teach their children, or just children in the community about what they learned in these library trainings. We do a lot of that in the library I work at. For lack of a better word, challenges, to motivate people, inspire people to do something, learn about something, act on something."* (P7)
Professional Development	Educators	Ideation directions that focus on helping educators to stay up-to-date with information and enhance teaching abilities	Open access textbook that is regularly updated with new topics and trainings for educators: *"I thought something like an open access textbook would be a good idea, just because they are so easy to adapt and also to update. It could be under a creative commons license, of course, so it will be kind of open for everyone, but maybe it could focus on the university context, among librarians or among faculty, or it could be regarding a wider professional development association."* (P11)
Social Support	Educators	Ideation directions that focus on addressing issues of educator loneliness, isolation, or creative burnout	Opportunities for collaboration with professionals in different fields that share similar goals: *"I think we could be integrating more into community programs. [...] A lot of cities and towns are creating these villages for helping older adults who want to stay at home and having volunteers go to their house [to help] with various things. We could also help with technology, and this village concept might work because it is partnering with an existing program of volunteers and the people that help are already vetted and part of the village."* (P1)

> "There's games out there for everything, and so some kind of privacy simulation game that they can interact with others on might be fun. [...] You can use it to teach students about information online and using social media." (P14)

Across workshops, participants generated ideas applicable to themselves and others. For example, P10, the sole school librarian in our study, felt their K-8-focused ideas could also benefit other participants. They suggested a kid-friendly sticker chart for tracking privacy/security literacy mastery could be transformed into a LinkedIn badge or certification for job-seeking patrons at P8's public library, showcasing the adaptability of generated ideas. Workshop 3 participants identified parallels between the children and older adults they catered to, and pursued solution ideas that integrated caretakers into the learning process, e.g., involving parents of children, or the adult children of older adults who are already often seen as "data custodians" of their family members.

Improving learners' access to resources. Participants across all sessions also consistently focused on improving learners' access to resources, addressing issues identified earlier in the workshops. Low-tech solutions, such as printed or tactile resources, were popular among our participants, to account for limited computer or Internet access and to reduce access barriers by removing reliance on technology. Ideas included zines focused on complex or niche topics that could not be covered in regular class sessions, scam recovery plans, and guides for managing privacy settings on popular smartphones and social media platforms. Physical password journals appeared frequently as well, with participants suggesting they could include password protection advice and dedicated space for practicing strong password creation strategies.

Participants who wanted to attract more young adults to their classes brainstormed social media marketing tactics such as creating educational short-form videos on TikTok. Low turn-out at their library classes led participants, especially public librarians, to think about place-based solutions and ways to expand library support services. This included partnering with local businesses and community hotspots, such as popular cafes, to offer pop-up lessons and programming. At-home support ideas were also popular among participants, such as an on-demand phone hotline for emergency advice, or a messaging platform so patrons and librarians could communicate outside of class time.

> "We need to take it somewhere outside of the tech

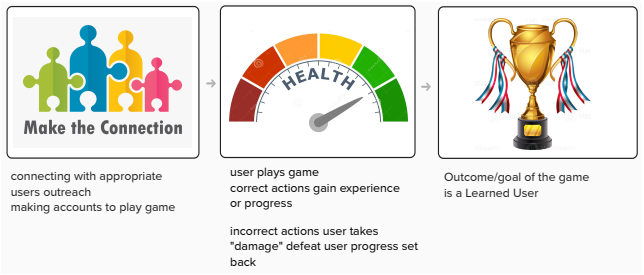


Figure 2: Storyboard sketch of a potential educational game.

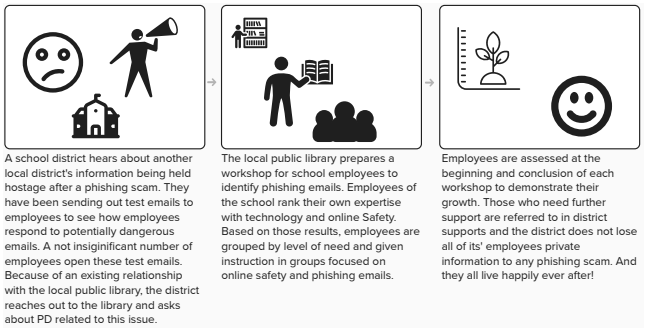


Figure 3: Storyboard for collaborative development programs.

> lab. [...] Maybe outreach to actual local businesses to inform them about digital literacy. Many places have staff development days, so maybe we can make it a service of the library to be a part of company staff development days to educate [other businesses] about digital and privacy literacy." (P5)

Collaboration beyond libraries. Relatedly, multiple participants were interested in more inter-organizational collaboration opportunities. Ideas included partnering with other educators and community service organizations to find common ground and amplify shared messaging (see Figure 3). For example, P10 suggested co-creating a lesson plan with their school's health teacher about cyberbullying and revenge porn, while a public librarian in the same session considered collaborating with local financial institutions (e.g., banks, small business administration agency) for teaching about scams and identity theft. While learner-focused, participants also appreciated these ideas for their potential to alleviate some of the isolation experienced by participants.

4.3.2 Educator-focused solution ideas

Discussions with participants revealed a significant need for resources and support for educators as well. Ideas mainly centered on professional development and on fostering community, collaboration, and creativity among educators.

Professional development. Participants highlighted a need for easier ways to stay current with new privacy, security, and online safety issues. For example, three participants in

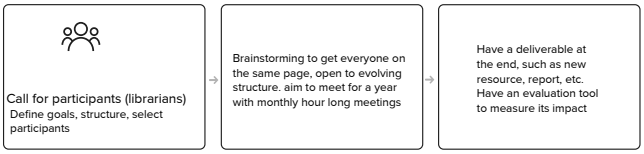


Figure 4: Participant sketch of an action plan for a virtual community of practice.

different sessions mentioned that their patrons were increasingly interested in AI safety, but that they felt unprepared to address those concerns. To fill such knowledge gaps, participants envisioned ideas such as open-access textbooks and online courses specifically tailored for library educators.

One popular idea that emerged independently in workshops 2 and 4 was an online platform where educators could share their teaching materials with other librarians, creating a central place for education resources and addressing the issue of an overwhelming number of available resources and sources. Workshop 4 participants ideated that this platform could include the ability to rate and review each other's materials to mitigate the information overload participants reported experiencing. Other ideas, which were ultimately not refined further, included a podcast for librarians to discuss emerging technologies, curated resource lists, and virtual educator toolkits. Many of these solutions aimed to streamline the often time-consuming information gathering process involved in creating new classes and programs.

> "My thought would be something like once someone similar to me has put together something, something about passwords for example... it would be useful if we could have like a repository. So then if I've made a class, and you know we've made it in a library, then another librarian could use it, and vice versa. [...] I like the idea that it'd be a place where I could submit what I've done and then look at what other people have done, and then hopefully be able to pull from that, hoping that we all do it in good faith." (P14)

Addressing educator isolation. Ideas to mitigate the sense of loneliness participants experienced in their teaching efforts included reinforcing the value of online safety and privacy education and fostering social connections and networking among library educators. The most desired solution, which emerged independently in multiple workshops, was a virtual *community of practice* for privacy and security library educators that could be open to various types of librarians, bridging library specialties, while the virtual nature would allow educators to participate from across the country (see Figure 4).

> "I think it's just nice to know you're not alone. We're all kind of struggling with this work. And just to brainstorm together, you know different concepts,

how to improve things. I like the idea of expanding and thinking more about academic librarians [as a public librarian] and the research that they do and how we can partner, because sometimes it does seem like two different worlds. But there's definitely collaboration that can happen." (P1)

Participants reported that isolation and limited resources had dampened their drive to innovate in their work, but that our workshops illustrated to them the value of being in community. At the end of our workshops, many expressed a reinvigorated interest and passion for improving their educational efforts. For example P8 shared:

> "I really enjoyed the conversation and getting kind of the encouragement to understand that many other libraries are, or librarians are, facing the same struggles that I am. You know, in terms of trying to instruct classes and helping people with technology. Sometimes it seems like we get the same questions day after day, week after week, and sometimes you wonder if you're making a difference. But you know I think we are, and I think we've got some really good ideas here, and I hope some of this stuff actually comes to fruition." (P8)

5 Discussion

Our study highlights the critical role of community-engaged educators, specifically librarians, in promoting security, privacy, and online safety literacy, and the importance of incorporating their perspective into the resource development process. Our findings underline the necessity of tailoring educational resources to communities' needs, and unveil insights into the challenges experienced by librarians in their educational work. Based on our findings, we discuss opportunities for addressing educators' challenges and promising directions for designing engaging privacy and security resources.

5.1 Ecosystems of Support for Librarians

Regarding RQ1, our findings affirm that community-engaged librarians are well positioned to understand and anticipate the privacy, security, and online safety needs of their community, allowing them to tailor their educational approaches accordingly. For example, in a community with many older adults, an educator might focus on recognizing and avoiding family impostor scams [68], while in a community with mainly young adults, the emphasis might be on social media privacy and safe online activism [10, 51]. This targeted approach ensures that education is relevant, timely, and directly applicable to learners, leading to increased engagement and a greater likelihood of behavioral change. At the same time, regarding RQ2, participants shared considerable challenges and constraints in doing this educational work, which motivated the co-creation of potential learning and support ideas for privacy, security, and online safety education (RQ3). While our workshops yielded various specific solution ideas, we highlight here overarching takeaways.

Co-creating adaptable privacy and security resources. Our participants described relying on a range of public resources when preparing privacy and security programming, including news articles, organizational toolkits, and online guides. However, participants rarely incorporated these resources directly into their patron-facing lessons. This reflects a tension observed throughout our findings and related work [1, 35]. Although expert organizations and government agencies produce accurate and regularly updated materials, these resources often assume a high degree of technical fluency. As a result, participants explained that such materials required significant translation, simplification, or contextualization before they could meaningfully support patrons with varied levels of digital literacy and limited time for instruction. These observations highlight an opportunity to strengthen the connection between community-centered privacy and security education and the broader ecosystem of public institutions responsible for digital safety. Participants' experiences point to a need for resources that are not only vetted and timely, but also flexible, digestible, and designed with diverse learners in mind. Building on the co-design orientation of our work, future efforts should explore how guidance produced by public institutions or non-profits might be adapted or co-designed with librarians to better align with the realities of library-based instruction. Such collaboration could reduce the duplication of effort in creating educational materials, promote greater consistency in public messaging about digital safety, and support coordinated partnerships between libraries and public institutions that collectively sustain privacy education at scale.

Collaborative opportunities for technical exchange. Participants expressed difficulties in keeping up with evolving technologies and associated privacy and security risks, a sentiment echoed in prior studies [28, 62]. Our participants were interested in collaborating with partners beyond the library, including academics, cybersecurity experts, and other local institutions. These findings suggest opportunities for professional development programs, initiatives, and experiences that would allow librarian educators to learn from expert practitioners (e.g., monthly brown bag meeting with computer science faculty at a nearby university), while also building collaborative relationships that can boost the visibility of their programming. Such initiatives could also work to bridge the researcher–practitioner gap identified in prior work [35], and alleviate the burdens experienced by librarians during the tedious information gathering process when preparing educational programming, which some library-based projects have sought to address in the past [20, 41, 54, 58].

Platforms for communal knowledge sharing. A common idea that emerged from our workshops is the development of

an online platform or digital repository that compiles a collection of high-quality, ready-to-use resources (including ones created by current educators themselves) that librarians can easily access and integrate into their programs. Uploaded materials could be reviewed and vetted by educators for their efficacy, address niche or complex topics to meet diverse needs, and be available as lesson plans, presentation templates, and interactive activities. The CLARK digital library system for cybersecurity [58], for which material are regularly updated and reviewed, could serve as an inspiration for such broader literacy efforts.

Virtual communities of practice. Many participants felt isolated and lonely in their solitary education efforts. Our workshops highlighted how participants valued connecting with other librarians leading similar educational programming. Our findings emphasize a need to facilitate a network that allows librarians to connect, share best practices, and collaborate on privacy and online safety education. Such gatherings have already been recognized as productive in prior work, e.g., developing resources and a national roadmap for privacy strategy in libraries [67]. Our participants suggested several forms similar collaborations could take, including a dedicated online forum, a series of regional meetings, or a virtual mentorship program. To expand the reach of such a network, participants seemed most inclined towards virtual options. Our participants' ideas are in line with prior recommendations for developing continuing privacy education for librarians [19], e.g., through reading clubs, knowledge-sharing networks, or informal privacy-oriented gatherings. Academic researchers, technical practitioners, and librarians should consider these aspects to create a sustainable system of support for community-engaged educators. Such support systems could empower librarians, address their current challenges, and help to expand their privacy and online safety education efforts to reach and impact a broader audience.

5.2 Designing Engaging Resources

Our participants also generated several ideas and opportunities for creating effective and engaging educational resources.

Balancing practical and conceptual advice. Participants felt that current resources tended to overly focus on prescriptive advice, which was also found in analyses of advice sources [38]. Our participants emphasized the need for learners to develop a more conceptual understanding of online safety, including the relevant systems that govern data flows, to foster effective and protective decision making. This is consistent with Wissinger's conception of privacy literacy as an extension of critical thinking and digital literacy skill [63], which highlights the need for resources that integrate theoretical and actionable components. Resources should further ground practical advice in real-world scenarios that reflect experiences of different groups (e.g., a guide for how to protect your personal information after you've lost your wallet). Future work should investigate how to do so effectively.

Incorporate interactive elements. Participants found current resources to be too abstract to capture the attention of their patrons. Librarians that served children and teens stressed advantages of gamifying lessons; others observed positive learning effects of visual aids, such as infographics or flowcharts, over text alone. Future resources and research could explore embedding interactive elements, such as quizzes, threat simulations, and group discussions, to further enhance engagement and retention, building on research findings that found applied and proactive learning formats to better support comprehension than abstract guidance [6, 18].

Tailoring content for diverse use cases. To foster use, our findings suggest that educational materials need to be designed to reflect needs of various communities, be usable across different modalities (e.g., printable, different languages, mobile-device friendly, etc.), and be easily adaptable for different educational and community contexts. Creating such resources requires significant effort, but also provides opportunities for researching and developing new educational knowledge production processes, such as using automated translation services, developing open-source materials that can be collaboratively adapted and updated, and designing modular resources with components that can be customized to different contexts (e.g., templates, reusable content blocks, and adaptable activities).

Fostering participation. Our findings further highlight a challenge in conveying the value and relevance of privacy and security educational offerings, as demonstrated by participants reporting often low attendance in offered trainings. Participants discussed ideas for promoting trainings on social media and non-class-based educational offerings, such as competitions. Future work should investigate opportunities for raising awareness of privacy, security and safety issues that are connected with different training opportunities.

6 Conclusion

Our participatory design study reveals actionable opportunities for improving community-based privacy and online safety education, and for addressing the challenges faced by educators. Though our study focused on librarians, our findings have broader implications for other informal education settings. By adopting a community-centered approach and involving educators in the design process, we uncovered ways to create more effective and inclusive learning experiences with regards to privacy, security, and online safety that can find applications in other contexts as well.

Acknowledgments

This work was partially supported by a University of Michigan Rackham Graduate Student Research Grant. The authors thank Kristin Fontichiaro for input on the study and workshop design, the participants for sharing their insights, and the reviewers for their constructive feedback on the manuscript.

References

[1] Tanisha Afnan, Sheza Naveed, Griffin Christie, Jackie Hu, Byron M. Lowens, Allison McDonald, and Florian Schaub. How we define privacy literacy: Teaching experiences & challenges of community-engaged privacy educators. *Proceedings on Privacy-Enhancing Technologies (PoPETs)*, 2026(1):552–566, 2026.

[2] American Library Association. Privacy field guides. https://www.ala.org/advocacy/privacy/fieldguides, accessed 2024-10-20.

[3] Dana Ayotte, Cheryl Li, Sepideh Shahi, Titania Veda, Colin Clark, and Gloria Bernal. Community-Led Co-design Kit. https://co-design.inclusivedesign.ca/. accessed 2024-11-22.

[4] Lisa Becksford. Teacher, librarian, or both? a quantitative investigation of instruction librarians' teacher identity. *College & Research Libraries*, 83(3):372, 2022.

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

[6] Olivia Castello and Alex Pfundt. Engaging learners through self-guided tutorials: Implementing and assessing a flipped classroom model for information literacy instruction. *The Journal of Creative Library Practice*, 2017.

[7] Chhaya Chouhan, Christy M LaPerriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J Wisniewski. Co-designing for community oversight: Helping people make privacy and security decisions together. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–31, 2019.

[8] Gobinda Chowdhury, Alan Poulter, and David McMenemy. Public library 2.0: Towards a new mission for public libraries as a "network of community knowledge". *Online Information Review*, 30(4):454–460, 2006.

[9] Sasha Costanza-Chock. *Design justice: Community-led practices to build the worlds we need*. The MIT Press, 2020.

[10] Alaa Daffalla, Lucy Simko, Tadayoshi Kohno, and Alexandru G Bardas. Defensive technology use by political activists during the sudanese revolution. In *2021 IEEE symposium on security and privacy (SP)*, pages 372–390. IEEE, 2021.

[11] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. Breaking! a typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2018.

[12] Laurien Desimpelaere, Liselot Hudders, and Dieneke Van de Sompel. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in human behavior*, 110:106382, 2020.

[13] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. The teaching privacy curriculum. In *Proceedings of the 47th ACM technical symposium on computing science education*, pages 591–596, 2016.

[14] Federal Trade Commission. Identity theft and online security. https://consumer.ftc.gov/identity-theft-online-security. accessed 2025-9-9.

[15] Alexandre Fortier and Jacquelyn Burkell. Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information technology and libraries*, 34(3):59–72, 2015.

[16] Electronic Frontier Foundation. Electronic frontier foundation. https://www.eff.org/, accessed 2025-9-9.

[17] Foad Hamidi, Kellie Poneres, Aaron Massey, and Amy Hurst. Using a participatory activities toolkit to elicit privacy expectations of adaptive assistive technologies. In *Proceedings of the 17th International Web for All Conference*, pages 1–12, 2020.

[18] Sarah Hartman-Caverly and Alexandria Chisholm. Privacy literacy instruction practices in academic libraries: Past, present, and possibilities. *IFLA Journal*, 46(4):305–327, 2020.

[19] Sarah Hartman-Caverly and Alexandria Chisholm. *Practicing Privacy Literacy in Academic Libraries: Theories, Methods, and Cases*. Chicago, IL: Association of College & Research Libraries, 1st edition, 2023.

[20] Gregory W. Hislop, Lillian Cassel, Lois Delcambre, Edward Fox, Rick Furuta, and Peter Brusilovsky. Ensemble: creating a national digital library for computing education. In *Proceedings of the 10th ACM Conference on SIG-Information Technology Education*, SIGITE '09, page 200, New York, NY, USA, 2009. Association for Computing Machinery.

[21] Jack Holt and James Nicholson. Scaffolding online safety in older communities: Exploring the relationship between digital literacy and cybersecurity. *ACM Trans. Comput.-Hum. Interact.*, February 2026.

[22] Julie Hui, Kristin Seefeldt, Christie Baer, Lutalo Sanifu, Aaron Jackson, and Tawanna R. Dillahunt. Community tech workers: Scaffolding digital engagement among underserved minority businesses. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW2), October 2023.

[23] Casey Lee Hunt, Kaiwen Sun, Zahra Dhuliawala, Fumi Tsukiyama, Iva Matkovic, Zachary Schwemler, Anastasia Wolf, Zihao Zhang, Allison Druin, Amanda Huynh, et al. Designing together, miles apart: A longitudinal tabletop telepresence adventure in online co-design with children. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*, pages 52–67, 2023.

[24] Finn Kensing and Jeanette Blomberg. Participatory design: Issues and concerns. *Computer supported cooperative work (CSCW)*, 7:167–185, 1998.

[25] Maoria J Kirker. "am i a teacher because i teach?": A qualitative study of librarians' perceptions of their role as teachers. *portal: Libraries and the Academy*, 22(2):335–354, 2022.

[26] Sandjar Kozubaev and Carl DiSalvo. Cracking public space open: design for public librarians. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2021.

[27] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children*, pages 67–79, 2018.

[28] Alan F. Luo, Noel Warford, Samuel Dooley, Rachel Greenstadt, Michelle L. Mazurek, and Nora McDonald. How library it staff navigate privacy and security challenges and responsibilities. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association.

[29] Monica Maceli. Librarians' mental models and use of privacy-protection technologies. *Journal of Intellectual Freedom & Privacy*, 4(1):18–32, 2019.

[30] Monica Maceli and John J Burke. Technology skills in the workplace: Information professionals' current use and future aspirations. *Information Technology and Libraries*, 35(4):35–62, Dec. 2016.

[31] Monica G. Maceli. Encouraging patron adoption of privacy-protection technologies: Challenges for public libraries. *IFLA Journal*, 44(3):195–202, 2018.

[32] Alison Macrina. Library freedom project. https://libraryfreedom.org/, accessed 2024-10-20.

[33] Marjorie Mayo. Spaces and places for popular education and participatory action research. In *Community-based Learning and Social Movements*, pages 41–56. Policy Press, 2020.

[34] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):72:1–72:23, 2019.

[35] Joy McLeod, Leah Zhang-Kennedy, and Elizabeth Stobert. Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 587–603, 2024.

[36] Margaret K. Merga. School librarians as literacy educators within a complex role. *Journal of Library Administration*, 60(8):889–908, 2020.

[37] Metropolitan New York Library Council. NYC Digital Safety. https://nycdigitalsafety.org/, 2022. accessed 2024-11-22.

[38] Mattia Mossano, Kami Vaniea, Lukas Aldag, Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 130–139. IEEE, 2020.

[39] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. Training and embedding cybersecurity guardians in older communities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[40] Northstar. Northstar digital literacy. https://www.digitalliteracyassessment.org, accessed 2025-11-17.

[41] OER Commons. National science digital library. https://oercommons.org/hubs/NSDL, accessed 2025-11-20.

[42] Library Freedom Project. Library freedom project. https://libraryfreedom.org, accessed 2025-9-9.

[43] Denise Fitzgerald Quintel and Amy York. *Privacy and Safety in Online Learning*. MT Open Press, Middle Tennessee State University, Tennessee, 2023.

[44] Emilee Rader and Rick Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[45] Yolanda A Rankin, Jakita O Thomas, and Nicole M Joseph. Intersectionality in HCI: Lost in translation. *Interactions*, 27(5):68–71, 2020.

[46] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 666–677, 2016.

[47] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[48] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108, 2020.

[49] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[50] Toni Robertson and Jesper Simonsen. Challenges and opportunities in contemporary participatory design. *Design Issues*, 28(3):3–9, 2012.

[51] Dana Rotman, Sarah Vieweg, Sarita Yardi, Ed Chi, Jenny Preece, Ben Shneiderman, Peter Pirolli, and Tom Glaisyer. From slacktivism to activism: participatory culture in the age of social media. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*, pages 819–822, 2011.

[52] Rahime Belen Sağlam, Vincent Miller, and Virginia NL Franqueira. A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, 66(3):274–286, 2023.

[53] Erica Shusas, Patrick Skeba, Eric PS Baumer, and Andrea Forte. Accounting for privacy pluralism: Lessons and strategies from community-based privacy groups. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2023.

[54] Skills Commons. https://partner.skillscommons.org, accessed 2025-11-20.

[55] Clay Spinuzzi. The methodology of participatory design. *Technical communication*, 52(2):163–174, 2005.

[56] Kaiwen Sun, Ritesh Kanchi, Frances Marie Tabio Ello, Li-Neishin Co, Mandy Wu, Susan A. Gelman, Jenny Radesky, Florian Schaub, and Jason Yip. "why is everything in the cloud?": Co-designing visual cues representing data processes with children. In *Proceedings of the 23rd Annual ACM Interaction Design and Children Conference*, IDC '24, page 517–532, New York, NY, USA, 2024. Association for Computing Machinery.

[57] Syracuse University. Center for digital literacy. https://ischool.syracuse.edu/research/center-for-digital-literacy/, accessed 2025-11-20.

[58] Blair Taylor, Sidd Kaza, and Melissa Dark. Designing a cybersecurity curriculum library: Best practices from digital library research. In Kim-Kwang Raymond Choo, Tommy Morris, Gilbert Peterson, and Eric Imsand, editors, *National Cyber Summit (NCS) Research Track 2021*, pages 47–59, Cham, 2022. Springer International Publishing.

[59] University of British Columbia. Digital tattoo project. https://digitaltattoo.ubc.ca/, accessed 2025-11-20.

[60] University of Pennsylvania Libraries. Hoesley digital literacy fellows program. https://curf.upenn.edu/content/hoesley-digital-literacy-fellows-program, accessed 2025-11-20.

[61] Kenneth Varnum, editor. *New top technologies every librarian needs to know*. LITA guide. ALA Neal-Schuman, Chicago, 2019.

[62] Jessica Vitak, Yuting Liao, Priya Kumar, and Mega Subramaniam. Librarians as information intermediaries: Navigating tensions between being helpful and being liable. In *Proc. iConference 2018*, page 693–702. Springer, Cham, 2018.

[63] Christina L Wissinger. Privacy literacy: From theory to practice. *Communications in Information Literacy*, 11(2):378–389, 2017.

[64] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12, 2019.

[65] Jason Yip and Kung Jin Lee. The design of digital learning activities for libraries through participatory design. In *Reconceptualizing libraries*, pages 203–216. Routledge, 2018.

[66] Jason C Yip, Kung Jin Lee, and Jin Ha Lee. Design partnerships for participatory librarianship: A conceptual model for understanding librarians co designing with digital youth. *Journal of the Association for Information Science and Technology*, 71(10):1242–1256, 2020.

[67] Michael Zimmer and Bonnie Tijerina. Library values & privacy in our national digital strategies: Field guides, convenings, and conversations. https://cipr.uwm.edu/2018/08/02/project-report-library-values-privacy/, 2018.

[68] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. Cross-contextual examination of older adults' privacy concerns, behaviors, and vulnerabilities. *Privacy-Enhancing Technologies (PoPETs)*, 2024.