"I'm Literally Just Hoping This Will Work:" Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities

Daniela Napoli, Khadija Baig, Sana Maqsood, Sonia Chiasson
Carleton University
{daniela.napoli, khadija.baig, sana.maqsood}@carleton.ca, chiasson@scs.carleton.ca

Abstract

To successfully manage security and privacy threats, users must be able to perceive the relevant information. However, a number of accessibility obstacles impede the access of such information for users with visual disabilities, and could mislead them into incorrectly assessing their security and privacy. We explore how these users protect their online security and privacy. We observed their behaviours when navigating Gmail, Amazon, and a phishing site imitating CNIB, a well-known organization for our participants. We further investigate their real world concerns through semi-structured interviews. Our analysis uncovered severe usability issues which led users to engage in risky behaviours or to compromise between accessibility or security. Our work confirms the findings from related literature and provides novel insights, such as how software for security (e.g., antivirus) and accessibility (e.g., JAWS) can hinder users' abilities to identify risks. We organize our main findings around four states of security and privacy experienced by users while completing sensitive tasks, and provide design recommendations for communicating security and privacy information to users with visual disabilities.

1 Introduction

More than 2 billion people worldwide live with some form of visual disability [36]. In this paper, we work with individuals with limited visual function such as those who are blind, have low vision, or have other visual disabilities. These individuals' visual capabilities are not situational nor can be changed with corrective lenses. Accessible technologies allow people with visual disabilities to autonomously achieve tasks, which improves their overall quality of life [15].

In practice, they often encounter usability issues, even when services meet common accessibility guidelines [6, 37, 44]. Examples include: confusing or misleading feedback, insufficient information, and compatibility issues between operating systems and assistive software [9, 29, 47]. As such, accessibility and usability are interdependent, emphasizing that approaching web accessibility in isolation is ineffective.

Practical guidelines and frameworks for user-centered security have been proposed [17, 18, 27, 35, 50], but most of the proposed solutions for managing web-based threats are visual which makes them inaccessible to users with visual disabilities, thereby compromising their security and privacy.

Prior work on the security and privacy concerns of users with visual disabilities [3, 24, 25, 48], highlights the unique challenges of designing accessible security and privacy systems. Specifically, that it requires designers to carefully consider and implement both accessibility and usable security design guidelines. Our work adds to this growing body of literature by focusing on users with visual disabilities' security and privacy experiences while web browsing in situations where they are working with potentially sensitive information.

To this end, we conducted a task-based user study and semi-structured interviews with 14 users to identify their security and privacy concerns while web browsing and the effectiveness of their protection strategies. Our work was guided by the following research questions:

RQ1: What types of online security/privacy concerns and barriers exist for those with visual disabilities when visiting websites?

RQ2: Are web security cues accessible and can they be easily interpreted?

RQ3: How do users with visual disabilities perceive and manage web-based risks and threats?

Based on both the study tasks and interviews about real-life practices, we found that users with visual disabilities experienced a number of severe security and privacy-related issues

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

including: inaccessible antivirus software, misleading screen reader outputs, and ill-fitting security advice. These issues can lead to increased security and privacy risks for users. For example, none of our participants were able to correctly identify our phishing website as potentially malicious.

From our findings, we identify four security and privacy awareness "states" which consider accessibility challenges and their influence on security and privacy strategies over time. We propose design recommendations which better suit the capabilities of people with visual disabilities.

2 Background

Many users with visual disabilities routinely complete transactions (e.g., banking and shopping) online, but face severe accessibility issues and have privacy or security concerns [25, 42]. Their major concerns include viruses, encountering CAPTCHAs, spam emails, unauthorized access to search history, and location-based data tracking. Some of these concerns could be addressed through specialized security software.

However, existing security software is often inaccessible and incompatible with screen reader keyboard short-cuts [42]. Similarly, Dosono et al. [19] observed 12 users with visual disabilities use email, banking, and eCommerce websites via screen readers. Poorly labelled login elements confused users with visual disabilities. Additionally, other accessibility issues with audible password masking, insufficient error messages, and password recovery methods negatively impacted users' control of their accounts containing sensitive information.

Ahmed et al. [3] interviewed 14 users with visual disabilities and found that privacy issues forced them to rely on inconvenient workarounds like disabling the screen (even if they require visual cues), wearing headphones (minimising their awareness of physical surroundings), and relying on sighted assistants to complete transactions on their behalf. Hayes et al. [24] shadowed 8 users with visual disabilities for two days, and found similar concerns and workarounds. Some users were also concerned that their sensitive information being stored in an insecure manner which could leave them vulnerable to security breaches.

Assistive technologies affect users' experiences. For example, screen reader outputs are serial in nature; since information is delivered line-by-line, users with visual disabilities must sequentially listen to options to identify the desired item or must skip through headings and sample paragraphs until they have found relevant data to achieve their goals [45, 47].

When it comes to security, users with visual disabilities may not rely on HTTPS or SSL/TLS dialogues to assess whether a website is legitimate or fraudulent in Abdolrahmani et al.'s [1] study with 11 participants. Several expert evaluations have found that the security mechanisms involved in completing common web-based security tasks (like logging into a website or purchasing an item online) were inaccessible, impeded the opportunities for users with visual disabilities to behave securely, and could instill a false sense of security [14, 19, 33].

As a result, the security techniques of users with visual disabilities are different from sighted users' behaviours [45]. Most recent work in this realm has focused on novel security technology for users with visual disabilities. Voice-controlled assistants like Amazon Echo have become inadvertent accessible solutions for people with visual disabilities in independently managing smart devices in their homes and pose as aids for therapy and caregivers [30, 38]. Branham et al. [10] propose a number of design guidelines to adapt home assistants so that they are more efficient and controllable for users with visual disabilities. However, as Akter et al. [4] argue, smart home devices do not yet properly consider the contexts of assisting individuals with visual disabilities and should better consider the privacy and security of the users with visual disabilities and those in their environments.

Other recent security and privacy solutions have been more deliberately designed to aid people with visual disabilities, including: improved audio CAPTCHA implementations [20], observation-resistant password schemes [13, 31], and accessible password managers [7]. These technologies are successful because they leverage the unique capabilities of users with visual disabilities within the system design [43].

As noted in previous work [22, 48], this research area requires further investigation. Most studies in the area are conducted with small samples, which suggest that further validation is required. Additionally, many mainstream security and privacy mechanisms are still not designed to properly integrate the competencies of users with visual disabilities [43].

Our contributions to the literature: In this paper, we confirm and extend previous findings relating to the security concerns of users with visual disabilities. We further explore how they manage and interact with various security indicators on the web, and whether these actions offer the desired level of protection. We identify obstacles not yet discussed in the literature, including: assistive technology misleading users while they assess phishing indicators and an evident distrust by users in security advice. We discuss the complex nature of users' security management techniques and various factors contributing to risky behaviours sometimes forced by inaccessible indicators. Finally, we suggest recommendations for improving security mechanisms based on our research.

3 Methodology

Our study took place in 2018 and was cleared by our university's Research Ethics Board and the Canadian National Institute for the Blind (CNIB). Sessions took place in three quiet locations, with participants choosing the location most convenient: our research lab, conference room at the Canadian Council of the Blind (CCB), or an office at the CNIB. All sessions were audio-recorded and transcribed.

Phase 1: Pre-test Participants verbally completed a demographics questionnaire with the researcher.

Phase 2: Website Tasks Participants were asked to complete three security tasks on their assigned website (Table 1). If time permitted, participants were asked to repeat the process on a second website. Participants were pseudo-randomly assigned to websites ensuring even allocation across the three sites. Our protocol was that if a participant deemed a website illegitimate at any point, we told them to stop interacting with it and we assigned a new site. Participants worked on a task until they decided it was complete. Between each task, participants answered 5-point Likert scale questions about the usability of the task. The researcher noted any observations relating to participants' interactions with the websites.

Websites: The websites elicited opportunities for exposure to security risks pertaining to eCommerce and email. While the spoofed CNIB website is primarily an informational resource, the Shop and Donation pages collect personal information (e.g., address, credit card) which can put users' privacy at risk. The spoofed website used a domain we purchased, *ccnib.ca* and did not use SSL/TLS. Other than these differences, the spoofed website was identical to the legitimate one, in terms of the content and user interface design.

Technological setup: The technology used during the study varied according to participants' needs/preferences. We offered them two setups: a desktop with JAWS, ZoomText, keyboard, mouse, and speakers or, an iPad with built-in accessibility features. They could use these, plus any other tools (e.g., physical magnifying glass), or their own devices. One participant chose to complete the study on their own iPad, 12 used the desktop setup running Windows 10, and two used the iPad (iOS 11).

Collection of personal information: Personal information used in the tasks (e.g., (usernames, passwords, credit card information) was provided by the researcher. Participants were encouraged to complete the tasks as they normally would with their own information outside of the study. We avoided emphasizing security or privacy during the study, to mitigate bias on users' typical behaviours while interacting with the websites.

Phase 3: Questionnaires and semi-structured interviews Through two verbal questionnaires and a semi-structured interview, participants elaborated on their online security and privacy concerns, the security advice they have received, and the protective security actions they take in their everyday life outside of the study.

Questionnaires: The first questionnaire asked participants to rate (on a scale 1 to 5) their level of concern for each item in a list of cybersecurity threats mentioned in a previous study by other web users with visual disabilities [25], presented in random order. The second questionnaire asked participants to rate the effectiveness of common security advice [26, 40], and likelihood they would adhere to these protective actions in real life.

Interview: Next, we conducted a semi-structured interview to further investigate participants' most pressing concerns, methods for protecting themselves online, obstacles they face while maintaining their security and privacy. After the interview, we debriefed the participants who used the spoofed website.

3.1 Participants

Fourteen participants with visual disabilities (7 blind, 7 partially sighted), completed three phases of the 90-minute study. Participants were recruited via social media posts, mailing lists, and through the CNIB. Once recruited, participants were provided a digital copy of the consent form ahead of their session. At the beginning of the session, the researcher reviewed materials with participants, and obtained verbal consent.

Our participants (6 women, 8 men) were over 18 years old, from Ottawa or Toronto, and had a visual disability. Their median age was 52.5 years, similar to the age distributions of prior accessibility user studies [19, 42, 46]. Nine had a college diploma or university degree. We categorized eight as unemployed: they were full-time volunteers, on long-term disability, or active job seekers; six were employed.

Participants rated their limitations in three visual capability dimensions (see Table 3 in the Appendix): visual acuity, visual field, and light perception. Aligning with common usage of the terms, we categorized participants with "very limited" capabilities affecting both eyes as "blind" and others as "partially sighted." Participants were given $50 for their time and were compensated for study-related travel expenses.

All participants were familiar with using the Internet. In daily life, most blind participants relied on screen reading software such as JAWS, NVDA, and iOS VoiceOver. Those with partial vision used custom settings on their device/browser or used screen reading/magnifying software like ZoomText. Table 3 (Appendix) provides participant's demographics, and the technological setup they used during the study. Five with low vision used the ZoomText 11 screen magnifier; participants with low vision used no specialized assistive software and instead used custom browser settings or device features like pinch-to-zoom when needed. All blind participants used screen readers, like JAWS 18 or VoiceOver.

4 Results

We were able to holistically consider participants' experiences by gathering information from task-based observation,

Website	URL	Task A	Task B	Task C
Amazon	https://www.amazon.ca	Verify whether site is legitimate	Login (if safe)	Complete purchase
Gmail	https://mail.google.com	Verify whether site is legitimate	Login (if safe)	Download attachment
Spoofed CNIB	http://www.ccnib.ca	Verify whether site is legitimate	Find donation page	Donate money

Table 1: The websites used and associated tasks completed during the sessions. Note the extra C in the spoofed CNIB URL

questionnaires, and semi-structured interviews about their real life practices. We identified several usability and accessibility issues which impact users' capabilities to identify security threats and to employ protective actions.

We report on our findings from Phase 2 and 3 below, then we summarize the relationships identified between the various data into four states of online security and privacy awareness. These states depict general behavioural trends in our participants' experiences and touch upon the security and privacy threat scenarios related to these trends.

4.1 Phase 2: Website Tasks

Table 2 summarizes participants' accuracy in identifying the legitimacy of the websites and their self-reported responses for all website tasks during the study. These responses include: the perceived accessibility of the website, task ease, and confidence ratings. Confidence ratings related to participants' certainty in having completed the task in its intended entirety (i.e., correctly). We note that these represent participants' perspectives and do not necessarily reflect whether the task was actually completed successfully or securely.

Due to our sample size, we did not run statistical tests on website task data. However, generally, participants rated websites as accessible ($M = 4.0$, $SD = 1.3$), were confident they had completed the tasks correctly ($M = 4.5$, $SD = 0.8$), and thought that the tasks were neutral-to-easy to complete ($M = 3.9$, $SD = 1.1$). We focus on the obstacles observed.

Task A: The participants' first task was to verify the site's legitimacy. The Gmail and Amazon sites were legitimate, and the CCNIB site was a spoof. All but one participant considered the provided websites to be legitimate[1]; all reported a high degree of confidence in their assessments. As a result, participants were mostly correct about the legitimacy of Amazon and Google websites. However, *none* of the participants recognized our spoof website, CCNIB, as illegitimate. Overall, 11/18 assessments were correct despite participants' confidence in their ability to complete the task. In particular, all participants assessing CCNIB rated their confidence as 5 (on a 5-point Likert scale) despite their incorrect assessments.

We observed participants' legitimacy assessments to be impacted by several factors. First, many leveraged untrustworthy security indicators such as professional looking, or familiar sounding alternate text for, logos and page content. Secondly, some participants mentioned that the site seemed to be associated with a reputable organization so it must be legitimate and trustworthy. Thirdly, some participants were unsure how to assess website legitimacy because it was not something they often considered:

> *"I don't think about a site's security often. I would if it seemed like a hacky site. If it wasn't professional, or if things were out of order, or if the buttons were in weird places." (U03)*

Our observations suggest that many participants did not rely on trustworthy indicators when assessing website legitimacy.

Some participants did attempt to take security precautions that were aligned with security best practices. Specifically, we observed some participants double check URL addresses for spelling inconsistencies. Unfortunately and importantly, for blind participants, this effort was futile for the spoofed site since JAWS announced the spoofed CCNIB site's address in the same way it would read the legitimate CNIB URL: `H-T-T-P-colon-slash-slash-W-W-W-dot-cuh-nib-dot-cah`. Thus, blind participants could not detect this phishing clue unless they used the screen reader to read the URL letter by letter. Since it is unlikely for any user to do this unless they are already suspicious of a website, relying on JAWS feedback to detect domain inconsistencies is ineffective.

One partially sighted participant, U12, detected our phishing site's extra "c" by looking at the URL. However, they dismissed this concern and completed a monetary transaction because the page content met their expectations:

> *"There's a lot of detail here... I'm very confident that it is legitimate because I'm looking at a product [in their online store] that I'm familiar with, and that is really only sold by the CNIB." (U12)*

We were careful in our instructions to avoid priming participants to be unrealistically security-conscious, however, being part of the study may have encouraged some participants to let their guard down or otherwise behave in ways they would not outside of the laboratory setting in Phase 2. When asked to reflect on their behaviour related to the tasks, nearly all participants said it was similar to their real-life behaviour. Only one participant mentioned that that they trusted that the researchers would not "lead them astray" and were inclined to assume all provided websites were legitimate. While we took efforts to increase ecological validity and we have no

[1] The participant decided that the Gmail site was likely illegitimate only after completing all tasks.

indication that this was a widespread problem, this effect is a known challenge for security and privacy studies [23]. To accommodate for these limitations, we dive deeper into users' real life practices and attitudes during Phase 3.

Task B: All attempts (18/18) to complete Task B: logging in to Amazon and Gmail or finding the donation page on the CCNIB website were ultimately successful with some issues.

Participants experienced no issues with finding the donation page on CCNIB. The Gmail login page has minimal content and users are automatically placed in the login form fields. On the Amazon homepage, users must skim through page content to find the login link and then skim through the page to find the form fields for entering login credentials.

Despite their eventual success, blind participants experienced accessibility issues during the login processes with Gmail and Amazon. With JAWS' password masking techniques, each password character is announced as "star." This provided blind participants with no feedback to confirm which characters they had input. The websites also provided no audible feedback about successful login. Instead, participants relied on the lack of warning to confirm successful login. Some were initially unsure if they had successfully logged in the websites, or if they just could not find a warning about login failure when skimming elements from the entire page.

Additionally, participants were unsure how much sensitive information was being displayed on the screen after logging into the sites. This limited blind participants' control over account information and their personally identifiable information (PII) because they must audibly skim through the page to confirm successful login and may unintentionally instruct the screen reader to announce private account information aloud.

Task C: All participants were able to complete Task C on the Gmail and CCNIB websites but only four out of six participants were able to finalize a purchase through Amazon, giving an overall completion rate of 16/18.

The two participants who were unable to complete the task were blind: U04 used VoiceOver and U14 used JAWS. Both faced insurmountable accessibility obstacles on Amazon because of information provided only through colour-based cues. Specifically, the website formatted a corrected shipping address when finalizing a purchase. The nuanced differences between the original and corrected address were highlighted in red but not described with alternate text.

To progress through the purchasing process, users must choose one of the two formatted addresses. Both participants tried unsuccessfully to identify which address to use for several minutes before we guided them to the next portion of the study to ensure the remainder of the session could be completed within the study's allotted time.

This accessibility hurdle is another example of the limited control users with visual disabilities have over websites and, in turn, limited control over their PII while interacting with websites. In this circumstance, participants were unable to access feedback relating to issues with a mailing address. A blind user unable to perceive Amazon's suggested options could be forced to complete a task in a way they cannot be sure aligns with their security and privacy values (e.g., by sharing the task and access to their account with a sighted person for assistance). This can be concerning because users are often expected to understand the implications of their actions and may not be provided secure or private defaults [32].

4.2 Phase 3: Questionnaires

Phase 3 deals with participants' real life experiences, concerns, and attitudes. Figure 1 summarizes participants' reported level of concern for 12 cybersecurity threats common to people with visual disabilities. The number in each cell of the matrix indicates the number of participants who selected the given Likert scale response. The colour intensity of the cells is based on the popularity of the response, with higher numbers having darker colour intensity.

Our participants generally expressed moderately high levels of concern. They were most concerned with protecting their financial information, their identity, their data, and their device from theft or disclosure. They were least concerned with threats relating to surveillance and eavesdropping.

Figure 1 summarizes participants' Likert-scale responses for their perception of the effectiveness of each protective action and the likelihood that they would take these actions.

Participants rated most of the actions as effective or very effective for protecting themselves online. However, they gave low ratings to two fundamental security measures: enabling automatic updates, and using a password manager.

For both of these measures, participants identified accessibility issues that rendered them ineffective from their perspectives. For example, automatic updates can lead to system changes that cause programs to no longer be compatible with assistive software. Also, due to password masking techniques, JAWS announces password characters as a "star" rather than the character. This leaves blind participants unable to confirm the accuracy of their entered passwords before logging in or storing their passwords in software, which undermines the perceived utility of password managers. Allowing users to audibly unmask their typing when entering a password for storage into a password manager (or when logging in from a location safe from eavesdropping) might help with this issue.

We saw some relationships between participants' perceived effectiveness of advice and the likelihood that they would follow this advice: the actions rated as most effective were generally likely to be followed. However, this relationship was not true for all actions. Accessibility concerns had a direct impact on participants' likelihood to follow the protective actions. Participants were less likely to adhere to security advice they considered ill-fitting for people with visual disabilities. For example, while multi-factor authentication was considered

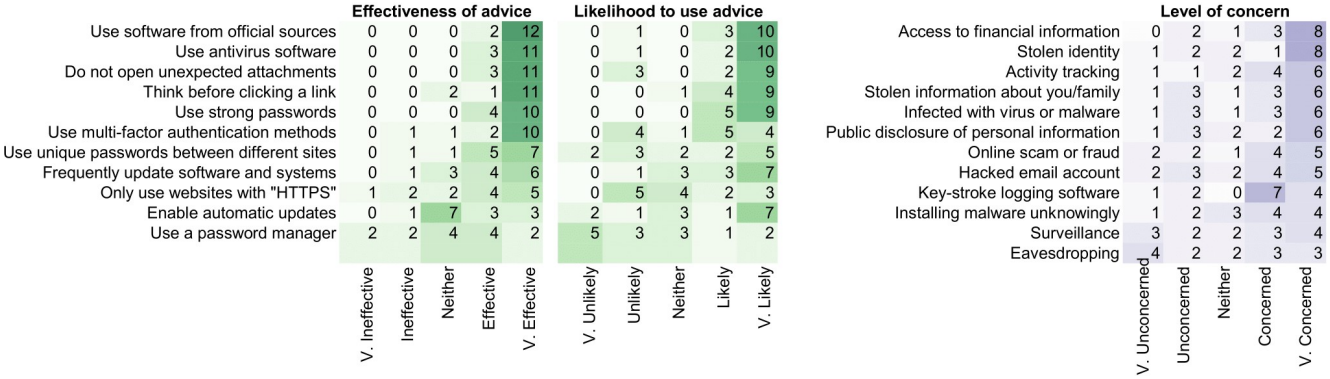

Figure 1: Number of participants selecting each Likert-scale response rating: the perceived effectiveness of security advice (left), likelihood that they will adhere to the advice (center), and their level of concern per threat (right). Darker cells indicate more popular responses.

very effective, many participants were unlikely to activate it on their own accounts because it increased the difficulty of logging in, and this task was already challenging on its own.

Some participants reported a lack of confidence in the security advice they receive. Two participants specifically noted their distrust in sighted individuals who present themselves as technology or web security experts. Participants expressed low confidence in the effectiveness of protective security actions and in the advice intended to help them avoid threats. Evident distrust in security advice was mainly rooted in a disconnect between the security expert's perception of the participant's experiences and participant's actual lived-experience:

> *"People say they know the difference between a threat and a non-threat, but someone who is actually blind knows the risk... People who use just regular everyday technology they take a lot of risks, it's just a reality. I have to be safer and smarter about it." (U01)*

Participants who expressed trust in security advice and tried to comply were greatly hindered by accessibility issues. For example, U14 explained that he used anti-virus software and kept the program updated. Yet, aspects of the interface were inaccessible to his screen reading software so he was unable to read and resolve flagged issues. The participant expressed that when confronted with a warning, he had to chose from the subset of accessible actions within his antivirus and hope that these would resolve the detected issue.

In some cases, adhering to security advice is not an option. When U12, a partially sighted participant, attempted to input information on the CCNIB website, he was unable to easily locate the form fields because the website was incompatible with the Chrome plugins he used to increase page contrast and aid in identifying page sections.[2] U12 explained that this was a common issue that often forced him to move closer to the screen and strain his only sighted eye. In these circumstances, he could not prioritize protecting sensitive data:

> *"I'm literally just hoping this will work. So safety's not really being considered, which is unfortunate, obviously." (U12)*

These findings demonstrate a need for improved mechanisms and security advice which properly consider the circumstances of users with visual disabilities and the assistive software they use. Improvements may increase users with visual disabilities' trust in the system, and enable them to perform the security actions that they wish to undertake.

4.3 Phase 3: Interviews

We further collected contextual data relating to users' real life experiences while browsing online, the strategies they employ to maintain their security online, and their feelings of safety.

4.3.1 Qualitative Analysis Methodology

Interview data, observational notes, and other verbal feedback provided during the session was coded based on Braun and Clarke's [11] six phases of thematic analysis.

Our initial research intent was to explore themes relating to users' attitudes, behaviours, concerns, and desires. For the first iteration, the lead researcher extracted 356 relevant excerpts from notes and recordings from all participants. These were organized according to the four overarching themes with closely related excerpts grouped as trends. We coded trends to formulate an initial codebook containing 35 codes. Three researchers iteratively discussed and refined the codebook, resulting in 17 codes in the second version.

[2] Note that we had duplicated the legitimate site exactly, and that the CNIB site **should** be accessible given that its target users have visual disabilities.

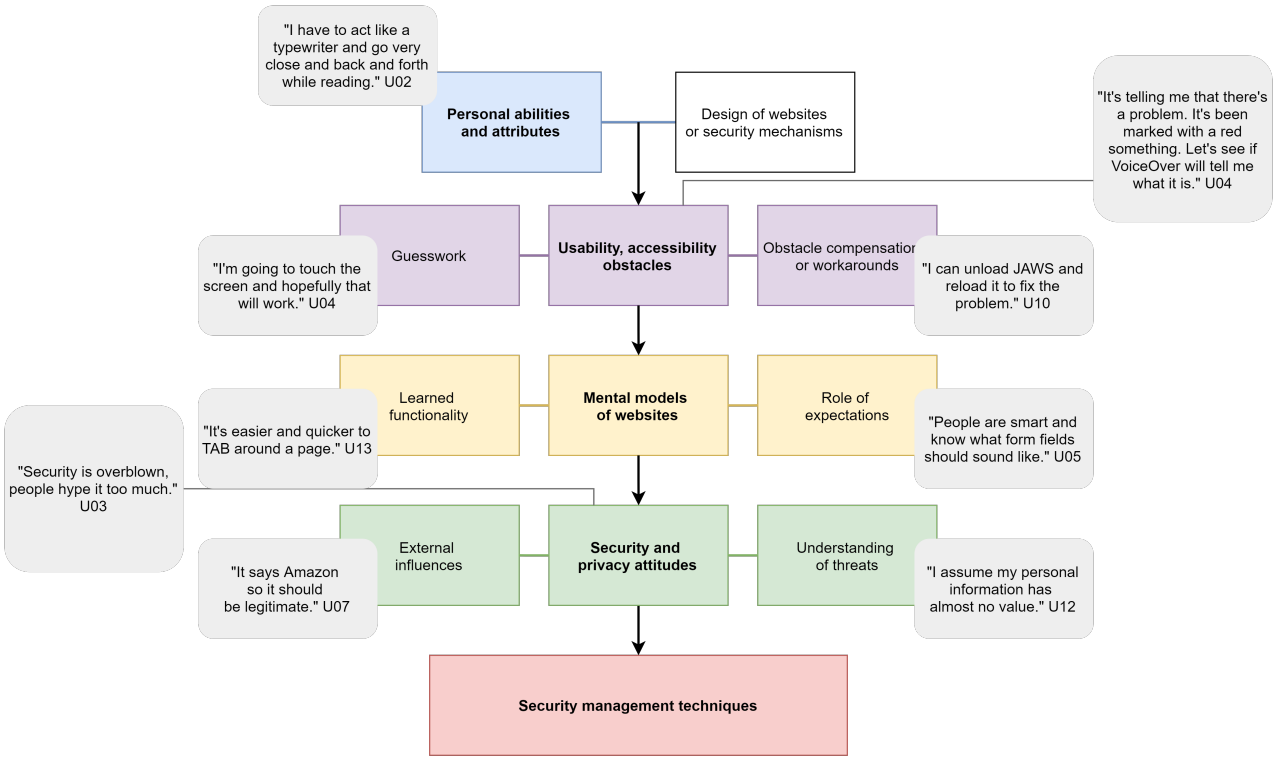

Figure 2: Relationships between the main codes formulated during our thematic analysis of participant interviews and feedback comments. Example excerpts are also included.

During the second round, two of these researchers used the second version of the codebook to independently code the same five randomly selected 90-minute transcripts. The mean Kappa score for inter-coder agreement across all codes was 0.66. This can be interpreted as good agreement. We met to discuss discrepancies in coding, come to agreement, combine redundant codes, and modify others to better fit the data, resulting minor changes. Then, the remaining transcripts were split between the two researchers and coded with the final codebook as shown in Table 4 in the Appendix.

4.3.2 Results

We summarize key takeaways from our qualitative analysis in Figure 2. Our analysis suggests an interdependent nature amongst our codes which linked to participants' security management techniques (further explored in Section 5).

Below, we provide sample excerpts to describe key codes/code groups and their relationships. In examining the relationships, we noted similarities with Cranor's human-in-the-loop security framework [18] which details aspects of effective security communications and can be used to identify how security indicators may fail to deliver information to users. Notably, we identified parallels with the *personal variables, intentions,* and *capabilities* factors which affect how users receive, process, and apply security and privacy information. When framed within this context, our qualitative analysis can provide insight into the nuances of communicating security information to users with visual disabilities.

Personal abilities and attributes: During discussion, participants contextualized the obstacles they faced with details about their visual disabilities, preferences, personalities, or technological skills when handling obstacles:

> *"As a partially sighted person, I try to get rid of the clutter, even in my mind, before I do something like this because it's easy to get distracted and take more time or more unnecessary use of vision." (U12)*

> *"I guess I should be a little more vigilant but, I'm still one of those people that if I go on a website I assume that that's where I should be." (U02)*

> *"I'm used to problem solving text stuff. That's what I do, and that's what I teach other people to do so it doesn't bother me that much. I just wish I could do it faster." (U05)*

Demographics and personal characteristics impact a person's ability to understand security indicators and influence how they take protective actions [18]. Participants' feedback in this code group was critical to understanding the context of users' experiences and fundamental variables impacting other codes relating to users' security/privacy attitudes and

behaviours. Thus, Figure 2 has it as the highest level factor in the chain influencing security management techniques.

Usability, accessibility obstacles: Participants described several challenges they experienced which were influenced by their individual capabilities and characteristics. We recognized these issues as infringements of basic usability or accessibility principles. These issues, when framed as *communication impediments* [18] can cause partial or full security information communication failures.

We gathered further insight relating to these obstacles as participants speculated what went wrong and described the workarounds they used to achieve their goals:

> *"I guess the webpage was programmed such that this was worthy of a restart... I don't think it had to do with something we tapped on. I think it had to do with the way the page was structured." (U04)*

> *"I can unload JAWS and reload it because that will fix the problem. If it doesn't read anything like before, I restart it again." (U10)*

As shown in Figure 2, the obstacles users faced were shaped by their individual characteristics and then influenced how they perceived and operated websites. For example, blind participant with technical backgrounds who faced several accessibility issues described more sophisticated workarounds, such as using advanced search options, compared to partially sighted users who encountered fewer issues. Users with sophisticated workarounds also mentioned using technical security indicators such as HTTPS or checking for SSL/TLS certificates. Interestingly, sophisticated workarounds did not necessarily align with accurate interpretations of how these indicators help their security, suggesting that these users had a superficial grasp of the issue despite their background.

Mental models of websites: The literature suggests that a user's familiarity with security indicators, vocabulary, and structure will impact their comprehension of risks and threats [18]. Thus, participants' feedback relating to how they understand and use systems was essential.

Participants described the shortcuts they use to interact with websites and browsers such as skimming for relevant page content via headings and using tabs to quickly access page features. Our findings reflected the shortcuts noted in related studies [19, 43] exploring the browsing behaviours of users with visual disabilities. These excerpts also reflected the importance of consistency and standard presentation as new interfaces can take a long time to learn:

> *"I assume that the actions are going to be on the right-hand side of the margin. If I was clueless and I didn't know how to use a website at all, then I would be bouncing around there for days." (U01)*

As highlighted in Figure 2 participants' mental models were impacted by the obstacles they faced and their mental models subsequently had downstream implications on how they completed security tasks. At times, participants had developed useful heuristics to inform their mental models and potentially help them with identifying phishing:

> *"You can usually tell if something you're looking at [isn't] actually Google or PayPal because it will say your bank account is compromised, click here. Banks never do that. They won't say click here to go to your account." (U05)*

Other times, participants' mental models and expectations for websites included reliance on unreliable cues that could mislead them. This also occurs with sighted users, but the types of cues occasionally differed because of the lack of visual feedback. For example, a blind participant believed a website was legitimate when they heard form feedback they had previously heard while using another website they trusted. Similarly, two partially-sighted participants trusted the spoofed CNIB website after they found content about assistive technology for people with visual disabilities, and this aligned with their expectations for the website.

Security and privacy attitudes: We coded participants' relevant comments while completing website tasks and questionnaires relating to their security concerns and advice. During the interviews, participants provided further information about what made them feel secure while browsing online. These included external influences like trusting specific companies or trusting friends and family:

> *"I feel safe online when people I've trusted tell me that whatever I'm using is safe. Anti-virus will keep me safe. My passwords will keep me safe. Sticking to what I know will keep me safe." (U01)*

> *"I feel safe on pages [where] I'm offering sensitive information, I believe that a company will have something to lose. If I lose, they lose too." (U04)*

Participants' security and privacy attitudes were also impacted by their understanding of technology and by their understanding of associated security threats:

> *"On my phone I know I'm not going to get viruses. I open attachments on my phone so I can save it to Dropbox or somewhere where I can access it on any platform. That way I'm not getting viruses or anything I don't need to have." (U05)*

Participants rated the threats they found most concerning in Section 4.2, and we found broad agreement for some threats. When we probed this topic further during the interviews, we noted that, despite some agreement on the scales, some participants explained that they found these issues very concerning, whereas others expressed an unconcerned attitude towards security and privacy:

"I always have to have my guard up. I know that people would perceive me as vulnerable." (U10)

"I don't really think about security because if I would always think about the, 'Oh what would happen if...', then I would never go online." (U07)

Attitudes seemed to be influenced by participants' individual characteristics, the obstacles they faced, and their individual security mental models. The different attitudes also contributed to the differences we observed in users' **security management techniques** which we elaborate in Section 5.

5 States of Online Security and Privacy

Security and privacy management techniques can be viewed as an amalgamation of users' lived experiences and understanding of websites/security mechanisms which are limited by accessibility and usability obstacles. Participants' adapt their security and privacy strategies depending on several factors relating to personal experiences and external factors. An individual may transition between strategies depending on the context of the task at hand, or may get stuck in one state due to accessibility obstacles or their security mental models.

The relative importance of each factor in influencing security management techniques varied per participant. Individual participants' management techniques also changed depending on the accessibility issues they faced per website, their current task goals, and the value of the information they exchanged with websites. To address the fluidity and complexity of this process, we identify "states" of security and privacy awareness that participants may go through while browsing online and affect their related behaviours and strategies.

These states are relevant to participants with any degree of vision disability as we did not observe that this influenced their likelihood of being associated with a given state. Furthermore, similar to describing security folk models [49], we focus less on the accuracy of participants' perspectives and more on the potential security and privacy implications related to these states of awareness.

5.1 Unconcerned, overconfident

Participants in the *unconcerned, overconfident* state either believed that they had taken the necessary precautions and that they could now freely navigate online without risk, or they believed that it was easy to spot online risks so additional precautions were unnecessary. In both cases, participants were unknowingly placing themselves at risk.

As previously mentioned, participants' understandings of security was greatly influenced by their understanding of web technology and the security mechanisms enabled on their system. Specifically, U04 shared that after taking precautions to protect himself and his devices, he is not concerned about his security and privacy and thus proceeds to trust that he will be secure while completing tasks online. However, some precautions U04 implemented relate to a common misconception that Apple products are impervious to security breaches.

Other participants made similar comments relating to Apple products or websites affiliated with Amazon or Google. Additionally, those who expressed lower levels of concern tended to rely on gut reactions about which websites seemed "hacky" and unprofessional when detecting threats. These assessments rely solely on website content they can read with assistive technology and cannot include available information that may be helpful but is inaccessible. This suggests that individuals relating to this state of security and privacy awareness may be more likely to fall victim to social engineering techniques relying on high-fidelity copies of the legitimate site, or spoofed organizational affiliations while completing tasks online. Therefore, an unconcerned, overconfident approach to security can lead to increased risk-taking habits or, in the worst case scenario, security apathy such as the following:
"Security is overblown. People hype it too much." (U03)

5.2 Concerned, overwhelmed

Participants in the *concerned, overwhelmed* state were worried about their online security and privacy but were unsure which protective techniques could address their concerns and were not confident in their ability to protect themselves online.

These participants expressed deep concern regarding their online security and privacy. Individuals relating to this state were more likely to mention security and privacy considerations while completing tasks. Additionally, these individuals mentioned several repressive habits they have in real life, including not banking or shopping online, only visiting websites which were recommended by trusted family or friends, and deleting all emails received from unknown recipients because they did not trust their own abilities in detecting threats. Often, individuals who relate to this state were anxious because of personal or secondhand experiences with security breaches.

Individuals who demonstrated great concern regarding their security and privacy also often expressed uncertainty in their ability to identify potential threats and to implement effective protections due to conflicting advice or accessibility issues that hindered them from taking desired precautions. Once in this state, an individual may feel overwhelmed or blame themselves for this uncertainty:

"Because I don't have any kind of background in programming or anything other than just being an end-user, I feel like a lamb to the slaughter. I just go in there without knowing that I shouldn't be." (U02)

5.3 Jaded, resigned

Participants in the *jaded, resigned* state may have been concerned about their online security and privacy, but severe us-

ability issues forced them to abandon protective actions and rely on others to protect their online security and privacy.

These participants approached their online security and privacy with fatigue due to usability and accessibility issues which limited their ability to employ protective strategies. These participants expressed a sense of powerlessness and were ultimately forced to rely on other, sighted, individuals to manage their security and privacy. Particularly, U14 regularly faced accessibility obstacles in managing his antivirus software, updating his systems, and navigating websites. Ultimately, he relied on his daughter to verify his security when completing tasks. Similarly, when U09 faces major challenges, she must relinquish autonomy and rely on trusted family members and friends to complete online purchases on her behalf to assure the security of her financial information.

Those in a jaded state initially approach their online activities with concern and try to be proactive against threats, but may become resigned:

> *"If someone wants to hack your computer, they will do it because there are always loopholes in any software that you're using. It doesn't matter whether you have the best antivirus or security software, it can still be hacked." (U13)*

When individuals are concerned for their security and privacy but must forfeit their independence to complete tasks, their ability to engage with technology is greatly limited.

5.4 Comfortable, unimpeded

Some participants were confident in the actions they took to protect themselves online while others were less inhibited by accessibility obstacles. Yet, no participants were both completely unimpeded, comfortable, and used effective security management techniques. Therefore, this fourth security state relates to an ideal state wherein users with visual disabilities are technologically empowered and can confidently manage their online security and privacy.

Users relating to this security state would have readily available access to all pertinent information they need to form informed security and privacy decisions. Additionally, users with visual disabilities in this state would have access to advice about protecting their security and privacy which adequately considers their nuanced concerns and lived realities relating to non-visual browsing experiences and the interaction between websites/software and assistive technologies. Furthermore, individuals in this state would be familiar with protective best practices and be able to implement these tactics in a manner that better reflects their browsing strategies.

To reach this state, we need to better consider the unique strengths and capabilities of different user groups, including those with visual disabilities in the design of security and privacy interfaces. Aligning with Reyez-Cruz et al. [43], we suggest that more sophisticated designs should include modes of interaction ideally suited to the capabilities of different groups of users rather than simply considering accessibility as an add-on to the "standard" interface.

5.5 Comparing to Sighted Users

We briefly highlight the main commonalities between our findings and related literature on sighted users. For example, *optimism bias and overconfidence* [2] refers to users underestimating the chances of becoming a victim to cybercrime and thus becoming less alert online. Like users with visual disabilities in the *Unconcerned, overconfident* state, sighted users who are familiar with a website may feel safe, trust that they are secure, and then bypass warnings [41]. This bias puts both groups of users at risk especially when they use unreliable cues like website content [5] to decide whether a website is legitimate. However, we note that sighted users may have more opportunity to recognize and recover from their error since most security cues are visual.

Furthermore, users may not have not enough mental resources to evaluate all options and potential consequences while attempting to achieve their goals [2] and must sift through overwhelming amounts of advice to make security and privacy decisions [39]. While these studies were done with sighted users, we note some parallels with participants from our study falling into the *Concerned, overwhelmed* state. Again, the differentiating factor is the additional burden faced by users with visual disabilities who must also deal with accessibility challenges and security advice that makes assumptions about users' ability to view security cues.

6 Discussion

Through task-based scenarios, questionnaires, and semi-structured interviews, we uncovered several major usability issues for users with visual disabilities. Users were hindered from completing security activities during the study and in real life, including accurately verifying the legitimacy of a website, securely logging into a website, and maintaining control of PII while completing online transactions. These obstacles impeded users' mental models of websites and negatively impacted their security and privacy attitudes.

Our study focused on strengthening the empirical knowledge base of accessibility issues pertinent to online security tasks. Particularly, we confirm findings relating to the security and privacy concerns of users with visual disabilities [3], their website credibility assessments [1], and the role of sighted allies when managing online security and privacy [24]. Our work increases confidence in the generalization of research findings within the realm of usable security and accessibility. This triangulation and confirmation work is particularly important given that studies in this area often have small sample sizes due to the difficulties of recruiting for this population.

Our study also extends existing work by highlighting several instances where security information is not effectively

communicated to users via assistive technology. Furthermore, participants identified ill-fitting security advice they perceived as ineffective and were unlikely to employ. Participants also shared their experiences with inaccessible indicators and anti-virus software. Further, we observed that interfaces provided participants with little to no guidance for protecting themselves online and, at times, they were prevented from completing their task entirely or were misled by assistive cues (e.g., reading the CCNIB URL in an identical manner as the legitimate CNIB URL). To our knowledge, the observation that assistive technology can actually mislead users or obfuscate important security cues has not previously been reported.

Some of the issues raised in our study could be avoided by adhering to website accessibility guidelines, but we note that the issue is more complex than this. These guidelines do not address the unique issues that arise in supporting users while maintaining their online security and privacy. One significant factor is that online security relies on more than the design of a website itself, which is the sole focus of most guidelines. For example, accessible web security also involves the browser chrome and other software or mechanisms (e.g., antivirus software, password manager), as well as the interaction between these technologies and the assistive software.

We outline recommendations for designing security interactions which can better serve users with visual disabilities in transitioning towards more beneficial states of privacy and security awareness. These recommendations align with existing general guidelines in usable security, and focus on the nuances of applying these principles when considering users with visual disability. We also emphasize the importance of closely collaborating with people with visual disabilities, ideally who are knowledgeable about security, to ensure that any changes resulting from these recommendations properly reflect the perspective and needs of users with visual disabilities.

Prioritize security information: Security interfaces should describe the current state of security and related available functions in simple and clear language [50]. Much of this information is available in browsers but cannot not be accessed by users with visual disabilities due to a mismatch between the competencies of these users and the design of most security interfaces. Sometimes this information is overlooked by users while trying to compensate for other accessibility issues. Therefore, security information should be more readily available via different modalities in a prominent, predictable, and easy-to-access location.

Assistive software output could prioritize security information over page content. For blind users, this would mean that reliable indicators are read aloud before less reliable indicators like page titles or content. For partially sighted users, this information could be pushed into, and emphasized within, their default field of view such as automatically zooming in on an address bar or other visual security cues rather than the page's header or navigation menu. Designers could also take advantage of the sequential nature of the web page experiences of users with visual disabilities. If properly implemented, users would automatically scan through security indicators before accessing the web content. This will inform users of potential security measures (or risks) before they interact with page content and decide to trust a website. However, designs will have to carefully balance the priorities of users to avoid potential frustration caused by presenting security warnings before relevant task information. Ultimately, users should retain control over whether security information is prioritized or simply easily available on-demand.

The use of other sensory channels can be used to minimize competition between website content and security cues. Salient non-visual warnings, like temperature feedback [34,51] can aid users with and without visual disabilities.

Provide proactive assistance: Security systems should be designed in a way that users can diagnose and recover from security errors [16]. Our work shows that screen reader users were not provided sufficient audible information to properly diagnose errors that were visibly shown on the tested websites. Some mentioned being unable to access and comprehend the problems being flagged by their anti-virus software. All of our participants demonstrated a willingness to resolve issues, but were uncertain of how to properly recover from the errors they faced. We emphasize that cues which help users in fixing security issues should be both accessible and directive.

Directive systems should proactively suggest solutions to users while providing enough context that they can understand the current state of their system and, if needed, how to improve it, without negatively impeding their cognitive load. This suggestion is based on: (i) the evident mental models of our participants with visual disabilities, (ii) their expressed need for more helpful guidance, and (iii) Felt et al.'s "suggestive design" approach to SSL/TLS dialogues [21]. In the context of sighted users, Felt et al. argue that users are more likely to adhere to security warnings if the dialogues highlight the advised steps. Directive security and privacy mechanisms can help users with visual disabilities who are concerned but unsure how to protect themselves online. Improved guidance can prevent these individuals from transitioning to a state of feeling helpless and resigned.

Similar to prioritizing security information, proactive assistance has the potential to cause frustration if delivered at an inopportune time. Users who are already at capacity with their current task may be overwhelmed by additional information, no matter how well intended. Making the assistance available in a side channel accessible on-demand may be preferable to interrupting the user's primary task. Future work should explore how to best assist users with visual disabilities who desire further support.

Make security advice relevant: Many of our participants with visual disabilities completed online transactions with an

inherent trust in their devices and/or the organizations that supposedly owned the websites. Sighted users also trust that external entities (E.g., firewalls, IT staff, or website owners) will maintain proper security [12,49]. Due to the severe accessibility obstacles, users with visual disabilities currently have limited means to personally maintain their security. Thus, interfaces which provide accessible contextual security and privacy guidance could be helpful for these users.

Security advice for users with visual disabilities must appropriately fit their lived experiences. Users who did not perceive sources of advice to empathize with their experiences and circumstances were unlikely to employ suggested security best practices. Future work could develop better security advice tailored for people with visual disabilities and the realities of their online experiences and assistive software. Participatory techniques are necessary wherein individuals with visual disabilities collaborate with sighted counterparts to devise appropriate tools and materials [43].

6.1 Recommended Practices

Reflecting on our practices, we identify some aspects of our study that facilitated participation for our target user group. In particular: recruiting through a trusted advocacy group, having the option to meet participants at a familiar place, covering the cost of transportation for the participant and an aid if necessary, providing the option to use their own devices, allowing individuals to self-identify whether they met the study's participation criteria, and avoiding unnecessary stress and risk from using their personal credentials (which could be visible to the researchers).

For this study, we worked closely with CNIB while designing, recruiting, and facilitating our study. We emphasize that the perspective of individuals within the target community should heavily influence all aspects of the research. Ideally, these individuals should be members of the research team. When not feasible, working closely with an advocacy organization like the CNIB, or community groups (e.g., Hayes et al. [24]), offers a viable alternative. We recommend that interested readers reference some of the excellent literature on conducting respectful and cooperative research involving people with have visual disabilities (e.g., [3,8,24,43]).

6.2 Limitations

Our findings provide insight to the behaviours and attitudes of users with visual disabilities. We collected data from a sample of local individuals whose views may not fully reflect the experiences of all people with visual disabilities. Additionally, our sample size is similar to those in related literature but is small compared to other usability studies due to recruitment difficulties despite our collaboration with CNIB. Furthermore, lab studies can introduce biases relating to users' behaviours or self-reported responses. Particularly, participants were provided credentials to complete tasks. This may have led participants to be less cautious; however, all participants said that they behaved in study as they normally would in real life. To further counter this potential bias, we focused a large part of our analysis on questionnaire and interview data exploring their real-life practices, in addition to observations from the the study tasks.

Future studies could explore alternative methodologies (e.g., using throw-away accounts or linking study compensation to performance) but these have their own trade-offs and limitations. Alternatively, studies could leverage other data collection methods, such as indirect observation [28] over a longer time period to further monitor how users behave outside of the lab. Additionally, accessibility and security research should go beyond considering visual disabilities to consider other disabilities and their intersections.

7 Conclusion

Through task-based scenarios, questionnaires, and a semi-structured interview with users who have visual disabilities, we identified a number of significant barriers they face while managing their online security and privacy, including: inaccessible antivirus software, misleading screen reader outputs, insufficient feedback relating to login processes, and unsuitable security advice. Participants' real life online security and privacy strategies varied depending on their current state of security and privacy awareness. Some people were prone to risk-taking habits and security apathy due to their trust in particular devices or associated organizations. Others were more concerned but felt unsure and overwhelmed while trying to protect themselves. Often, these individuals did not trust that they had the abilities to identify potential threats nor trust security advice that did not reflect their lived experiences. Obstacles led to security fatigue in some cases, where some users with visual disabilities felt resigned to rely on trusted sighted family and friends to manage their online interactions. Future work should continue to explore how to improve currently implemented security mechanisms with better consideration of a wider range of users' needs and capabilities.

Acknowledgments

The authors acknowledge funding from Natural Sciences and Engineering Research Council of Canada (NSERC) through the Canada Graduate Scholarships Doctoral program (Napoli), Discovery Grant program (Chiasson), and Canada Research Chair program (Chiasson). This research was also supported by an eCampusOntario Digital Inclusion Research Grant for 2017-18.

References

[1] A. Abdolrahmani and R. Kuber. Should I trust it when I cannot see it?: Credibility assessment for blind web users. In *ASSETS*, pages 191–199. ACM, 2016.

[2] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, Y. Wang, and S. Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), August 2017.

[3] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 3523–3532. ACM, 2015.

[4] T. Akter, B. Dosono, T. Ahmed, A. Kapadia, and B. Semaan. "I am uncomfortable sharing what I can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1929–1948. USENIX Association, August 2020.

[5] M. Alsharnouby, F. Alaca, and S. Chiasson. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82:69–82, 2015.

[6] R. Babu, R. Singh, and J. Ganesh. Understanding blind users' web accessibility and usability problems. *AIS Transactions on Human-Computer Interaction*, 2(3):73–94, 2010.

[7] N. Barbosa, J. Hayes, and Y. Wang. Unipass: design and evaluation of a smart device-based password manager for visually impaired users. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 49–60. ACM, 2016.

[8] N. Barbosa and Y. Wang. Lessons learned from designing and evaluating smart device-based authentication for visually impaired users. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO, June 2016. USENIX Association.

[9] Y. Borodin, J. Bigham, G. Dausch, and I. Ramakrishnan. More than meets the eye: A survey of screen-reader browsing strategies. In *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A)*, page 13. ACM, 2010.

[10] S. M. Branham and A. Rishin M. Roy. Reading between the guidelines: How commercial voice assistant guidelines hinder accessibility for blind users. In *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '19, page 446–458, New York, NY, USA, 2019. Association for Computing Machinery.

[11] V. Braun and V. Clarke. Thematic analysis. In H. Cooper, P. Camic, D. Long, A. Panter, D. Rindskopf, and K. Sher, editors, *APA handbook of research methods in psychology*, volume 2, chapter 4. American Psychological Association, Washington, DC., 2012.

[12] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[13] D. Briotto Faustino and A. Girouard. Bend passwords on bendypass: A user authentication method for people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '18, page 435–437, New York, NY, USA, 2018. Association for Computing Machinery.

[14] M. Buzzi, M. Buzzi, B. Leporini, and F. Akhter. User trust in ecommerce services: perception via screen reader. In *New Trends in Information and Service Science, 2009. NISS'09. International Conference on*, pages 1166–1171. IEEE, 2009.

[15] Statistics Canada. Partcipation and activity limitation survey 2006 facts on seeing limitations. Technical report, Canada, 2006.

[16] S. Chiasson, P. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, pages 1–16, 2006.

[17] S. Chiasson, P. van Oorschot, and R. Biddle. Even experts deserve usable security: Design guidelines for security management systems. In *SOUPS Workshop on Usable IT Security Management (USM)*, pages 1–4. USENIX, 2007.

[18] L. F. Cranor. A framework for reasoning about the human in the loop. *UPSEC*, 8(2008):1–15, 2008.

[19] B. Dosono, J. Hayes, and Y. Wang. "I'm stuck!:" a contextual inquiry of people with visual impairments in authentication. In *Proceedings of The Symposium on Usable Privacy and Security*, pages 151–168. USENIX, 2015.

[20] V. Fanelle, S. Karimi, A. Shah, B. Subramanian, and S. Das. Blind and human: Exploring more usable audio CAPTCHA designs. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 111–125. USENIX Association, August 2020.

[21] A. Felt, A. Ainslie, R. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving ssl warnings: Comprehension and adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2893–2902. ACM, 2015.

[22] O. Gaggi, G. Quadrio, and A. Bujari. Accessibility for the visually impaired: State of the art and open issues. In *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–6, 2019.

[23] S. Garfinkel and H. Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[24] J. Hayes, S. Kaushik, C. E. Price, and Y. Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Symposium on Usable Privacy and Security ({SOUPS})*. USENIX, 2019.

[25] F. Inan, A. Namin, R. Pogrund, and K. Jones. Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1):28, 2016.

[26] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Symposium On Usable Privacy and Security*, volume 15, pages 1–20. USENIX, 2015.

[27] P. Jaferian, D. Botta, F. Raja, K. Hawkey, and K. Beznosov. Guidelines for designing it security management tools. In *Proceedings of the 2nd ACM Symposium on Computer Human interaction For Management of information Technology*, page 7. ACM, 2008.

[28] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.

[29] J. Lazar, A. Allen, J. Kleinman, and C. Malarkey. What frustrates screen reader users on the web: A study of 100 blind users. *International Journal of Human-Computer Interaction*, 22(3):247–269, 2007.

[30] B. Leporini and M. Buzzi. Home automation for an independent living: Investigating the needs of visually impaired people. In *Proceedings of the Internet of Accessible Things*, W4A '18, New York, NY, USA, 2018. Association for Computing Machinery.

[31] D. Marques, T. Guerreiro, L. Duarte, and L. Carriço. Under the table: tap authentication for smartphones. In *Proceedings of the 27th International BCS Human Computer Interaction Conference*, page 33. British Computer Society, 2013.

[32] A. H. Mhaidli, Y. Zou, and F. Schaub. "We can't live without them!" app developers' adoption of ad networks and their considerations of consumer risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[33] D. Napoli. Developing accessible and usable security (ACCUS) heuristics. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI EA '18, pages SRC16:1–SRC16:6, New York, NY, USA, 2018. ACM.

[34] D. Napoli, S. Navas Chaparro, S. Chiasson, and E. Stobert. Something doesn't feel right: Using thermal warnings to improve user security awareness. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[35] J. Nurse, S. Creese, M. Goldsmith, and K. Lamberts. Guidelines for usable cybersecurity: Past and present. In *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on*, pages 21–26. IEEE, 2011.

[36] World Health Organization. World report on vision, 2019.

[37] C. Power, A. Freire, H. Petrie, and D. Swallow. Guidelines are only half of the story: accessibility problems encountered by blind users on the web. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 433–442. ACM, 2012.

[38] A. Pradhan, K. Mehta, and L. Findlater. "Accessibility came by accident": Use of voice-controlled intelligent personal assistants by people with disabilities. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[39] E. M. Redmiles, S. Kross, and M. 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*, CCS '16, page 666–677, New York, NY, USA, 2016. Association for Computing Machinery.

[40] R. Reeder, I. Ion, and S. Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15:55–64, 2017.

[41] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page

1–13, New York, NY, USA, 2018. Association for Computing Machinery.

[42] G. Regal, E. Mattheiss, M. Busch, and M. Tscheligi. Insights into internet privacy for visually impaired and blind people. In *International Conference on Computers Helping People with Special Needs*, pages 231–238. Springer, 2016.

[43] G. Reyes-Cruz, J. E. Fischer, and S. Reeves. Reframing disability as competency: Unpacking everyday technology practices of people with visual impairments. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–13, New York, NY, USA, 2020. Association for Computing Machinery.

[44] D. Rømen and D. Svanæs. Validating WCAG versions 1.0 and 2.0 through usability testing with disabled users. *Universal Access in the Information Society*, 11(4):375–385, 2012.

[45] N. Sahib, A. Tombros, and T. Stockman. A comparative analysis of the information-seeking behavior of visually impaired and sighted searchers. *Journal of the Association for Information Science and Technology*, 63(2):377–391, 2012.

[46] S. Szpiro, S. Hashash, Y. Zhao, and S. Azenkot. How people with low vision access computing devices: Understanding challenges and opportunities. In *Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 171–180. ACM, 2016.

[47] M. Vigo and S. Harper. Challenging information foraging theory: Screen reader users are not always driven by information scent. In *Conference on Hypertext and Social Media*, pages 60–68. ACM, 2013.

[48] Y. Wang. The third wave? Inclusive privacy and security. In *Proceedings of the 2017 New Security Paradigms Workshop*, NSPW 2017, page 122–130, New York, NY, USA, 2017. Association for Computing Machinery.

[49] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, New York, NY, USA, 2010. Association for Computing Machinery.

[50] A. Whitten and J. Tygar. Why Johnny can't encrypt: A usability evaluation of pgp 5.0. In *Security Symposium*, volume 348, pages 169–184. USENIX, 1999.

[51] G. Wilson, H. Maxwell, and M. Just. Everything's cool: Extending security warnings with thermal feedback. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 2232–2239. ACM, 2017.

Website	Correct Assessments	Accessibility	Perceived					
			Task A		Task B		Task C	
			Ease	Conf.	Ease	Conf.	Ease	Conf.
Gmail	5/6	4.2	3.50	4.17	4.00	4.33	3.67	4.67
Amazon	6/6	3.5	4.17	4.50	3.83	5.00	2.83	3.67
CCNIB	**0/6**	4.3	4.33	5.00	4.33	4.83	4.17	4.00

Table 2: Phase 2 results. Number of correct assessments for whether the site was legitimate or fraudulent; mean Likert scale ratings (out of 5) for the site's perceived accessibility, self-reported ease of completing the task and level of confidence in completing task in its entirety.

A Post-Task Questionnaire

Questions 1, 2, and 3 were asked after completing each task. Questions 4, 5, and 6 were asked after completing all tasks for a website.

Q1: Is this website...Legitimate or Fake?

Q2: How easy or difficult was it to complete the task? (1. Extremely difficult, 2. Difficult, 3. Neither easy nor difficult, 4. Easy, 5. Extremely easy)

Q3: How confident are you that you completed the task? (1. Extremely unsure, 2. Unsure, 3. Neither sure nor unsure, 4. Sure, 5. Extremely sure)

Q4: How would you rate the website's accessibility? (1. Extremely inaccessible, 2. Inaccessible, 3. Neither accessible nor inaccessible, 4. Accessible, 5. Extremely accessible)

Q5: How does this activity compare to your experiences with similar tasks outside of this study?

Q6: What other steps might you take if you were faced with a similar situation in real life?

B Post-Test Questionnaire

Q1: Rate your level of concern with the following digital threats on a scale of 1 (very unconcerned) to 5 (very concerned). *Ordering of options randomized per participant.*

- Someone stealing your identity
- Someone gaining access to your financial information
- Someone stealing private information about you/your family
- Your personal information being made public
- Falling victim to an online scam or fraud
- Someone hacking in to your email
- Unintentionally installing malicious software
- Your device becoming infected with a virus or malware
- Your device becoming infected with key-stroke logging software
- Someone eavesdropping on you
- Someone watching your interactions without you knowing

Q2a: Rate the effectiveness of the following protective actions on a scale of 1 (not effective at all) to 5 (extremely effective). *Ordering of options randomized per participant.*

- Frequently update software and systems
- Enable automatic updates
- Use software from official, trusted sources
- Use antivirus software
- Use strong passwords
- Use unique passwords between different sites
- Use multi-factor authentication methods
- Use a password manager
- Only use websites that include "HTTPS" in the URL address
- Think before clicking a link
- Do not open unexpected attachments

Q2b: On a scale of 1 (extremely unlikely) to 5 (extremely likely), how likely are you to take the protective actions? *Refer to listed options above. Ordering of options randomized per participant.*

C Post-Test Interview

Q1: Tell me more about what happens when you face... *an obstacle we observed or the user mentioned.*

- **Q1a:** What do you think caused this issue?
- **Q1b:** How did this problem affect your mood?
- **Q1c:** How do you think this problem affected your security or privacy?

Q2: How often do you consider your personal security and privacy when surfing the web? (1. Never, 2. Very rarely, 3. Rarely, 4. Occasionally, 5. Very frequently, 6. Always)

Q3: How safe do you usually feel when offering sensitive information online? (1. Extremely unsafe, 2. Unsafe, 3. Neither safe nor unsafe, 4. Safe, 5. Extremely safe)

Q4: If any, what are your most pressing concerns when browsing online?

Q5: What makes you feel safe online?

ID	Sex	Age	Visual acuity	Visual field	Light perception	Occupation	OS	Accessories	Assistive	Settings	Browser	Website
U01	F	20	Very limited	Very limited	Very limited	Student	W	K	JAWS	Default	IE	Gmail
U02	F	55	Somewhat	Somewhat	Somewhat	Unemployed	W	K, M, D, glasses	ZoomText	Voice reader	IE	Amazon
U03	M	26	Very limited	Somewhat	Not at all	Student	W	K, M, D	JAWS	Default	IE	Gmail
U04	M	6 3	Very limited	Very limited	Very limited	Retired	iOS	None	VoiceOver	Default	Safari	Amazon
U05	F	51	Very limited	Very limited	Somewhat	Technologist	W	K	JAWS	Default	IE	Gmail
U06	F	54	Somewhat	Very limited	Somewhat	Unemployed	W	K, M, D	ZoomText	High-contrast, voice reader	IE	CCNIB
U07	M	51	Very much	Very limited	Somewhat	Contractor	W	K	JAWS	Default	IE	Amazon
U08	M	41	Somewhat	Somewhat	Somewhat	Unemployed	W	K, M, D, magnifying glass	ZoomText	Default	IE	Gmail, CCNIB
U09	F	68	Somewhat	Not at all	Somewhat	Small business owner	iOS	Book stand	None	Default	Safari	Amazon
U10	M	68	Very limited	Very limited	Not at all	Retired	W	K	JAWS	Default	IE	CCNIB
U11	F	70	Somewhat	Somewhat	Somewhat	Retired	W	K, M, D	ZoomText	Default	IE	Gmail, CCNIB
U12	M	51	Very limited	Very limited	Somewhat	Unemployed	W	K, M, D, glasses	None	High-contrast, cursor enlarge	Chrome	Amazon, CCNIB
U13	M	40	Somewhat	Not at all	Somewhat	Unemployed	W	K, M, D	ZoomText	Default	IE	Gmail, CCNIB
U14	M	55	Very limited	Very limited	Very limited	Customer Service	W	K	JAWS	Default	IE	Amazon

Table 3: Participant demographics and the devices/software used during user study sessions. OS column represents the operating system used where: “W” represents Windows 10. Accessories column represents the technology used during the session where: “K” is keyboard with tactile markers, “M” is standard computer mouse, and “D” is display monitor.

Code	Description	Code Group
Personal abilities or attributes	Participant expresses confidence or apprehension in their abilities/attributes which play a role in completing tasks	**Personal abilities and attributes**
Preferences	Participant expresses preference (or aversion) for certain techniques to completing tasks.	
Usability or accessibility obstacles	Instances mentioned during discussion or experienced while completing tasks in which participants face challenges that infringe usability/accessibility	**Usability, accessibility obstacles**
Guesswork	Participant hypotheses in how the system works, what it is doing, or how to strategize interactions to achieve desired ends.	Guesswork
Obstacle compensations or workarounds	Participant techniques in overcoming issues while trying to complete tasks.	Obstacle compensations or workarounds
Mental models of websites	Participant understandings of how websites work based on experiences and expectations.	**Mental models of websites**
Learned functionality language	Terms and phrases indicating participants' unique interaction with and navigation of websites, using assistive technology or software.	Learned functionality
Roles of website expectations	Participant expectations of a site/system and their implications on task processes.	Role of expectations
Legitimate and/or secure websites	Cues which participant uses to validate website legitimacy or security.	
Apathy towards privacy/security	Instances in which participant is unconcerned for their online privacy/security.	**Security and privacy attitudes**
Security is secondary	Participant gives higher priority to other aspects of the interaction than their personal privacy/security.	
Security uncertainty	Participant expresses uncertainty in maintaining their personal privacy/security.	
Security concerns	Participant describes their privacy/security concern(s).	
External influences	Evidence of brand, institution, software, etc. influence on participants' understanding of privacy/security.	External influences
Tolls of infringed security	Participant describes negative consequences (experienced or presumed) of privacy/security infringements.	
Incomplete/inaccurate security mental models	Participant techniques in protecting themselves which are based in incomplete/inaccurate understandings of threats.	Understanding of threats
Security management	Participant describes their methods in managing their personal privacy/security.	**Security management techniques**

Table 4: Final version of the codebook which describes participants' interview data and other feedback.