ACCESSIBLE AND USABLE SECURITY: EXPLORING VISUALLY IMPAIRED USERS' ONLINE SECURITY AND PRIVACY STRATEGIES

by
Daniela Napoli

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF ARTS

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2018

Abstract

Visually impaired individuals are increasingly reliant on the Internet in their daily lives. Yet, existing security mechanisms may not sufficiently help these users protect their online security and privacy. We explore this issue through two complementary studies. First, we conduct an expert evaluation to assess web-based security cues through JAWS. We propose a set of 9 heuristics combining usable security and web accessibility principles to guide our expert evaluation. We uncover several severe issues that are not identified by automated accessibility checkers. Second, we conduct a task-based user study with 14 visually impaired users to observe their security habits and concerns when navigating the web. Again, our findings suggest that severe usability issues lead users to take risks or force them to choose between accessibility or security. Based on our findings, we provide practical recommendations to remedy these issues by tailoring security information to effectively communicate with visually impaired users.

Acknowledgements

To the memory of Dr. Anthony Whitehead.
The catalyst for my endeavours at Carleton University.

This research was funded in part by eCampusOntario through the Digtial Inclusion Research Grant for 2017-18. Several other people and organizations have graciously contributed to this research in a variety of ways. I would like to acknowledge a few:

Thank you to Mahadeo Sukhai, Sue Marsh-Woods, CNIB Toronto, Kim Kilpatrick, and CCB Ottawa for your integral role in recruitment and providing study space to conduct our user studies. With your support, our research progressed seamlessly. Thank you to every person who participated in our user study. I appreciate your time, interest, and invaluable feedback. I hope your comments continue to inspire all those who aim to develop a safer, more accessible, web for all.

Thank you to all the members of CHORUS laboratory. Heng Sun and Sana, thank you for helping prepare the test websites. Becky, Yomna, Michael, Jessica, and Dani thank you for helping prepare the user studies. Your assistance made this work that much more manageable.

Thank you to Professor Audrey Girouard and Professor Robert Biddle for sitting on my defence committee. Thank you to Professor Alex Ramirez for chairing my defence. Your thoughtful feedback in strengthening this thesis is deeply appreciated.

Thank you to my phenomenal research supervisor, Professor Sonia Chiasson. I owe the success of this research, and all relating work, to your unwavering guidance and dedication. Through out this entire process, I have been grateful to be under your supervision. I am delighted to be given the opportunity to continue to work together in the future.

Finally, to my loving family and Tyler: You have kept me grounded and focused so that I could bring this research to life. Thank you so much.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Hundreds of millions of people around the world live with visual impairments [81] and many rely on advancing technology to improve the quality of their life. Despite advances in web accessibility, these individuals still struggle to complete simple tasks on the Web, and they often feel limited and reliant on sighted individuals when working with these interfaces [39]. These usability concerns can be particularly detrimental for the online privacy and security of visually-impaired users.

There is minimal literature that explores both web accessibility and usable security. Therefore, the usability issues pertaining to the methods in which visually impaired individuals maintain their online security and privacy are not well documented. We aim to address this issue through the following Masters thesis.

1.2 Research Questions

Our research aims to advance the knowledge of the issues surrounding online accessibility and usable security for visually impaired users as they use assistive technology on the web. Our research is guided by three main research questions:

Q1 What types of online security/privacy concerns and barriers exist for those with visual impairments when visiting websites?

Q2 Are web security cues easily accessible and interpretable?

Q3 How do these users perceive and manage web-based risks and threats?

Our research aims to identify issues that hinder secure and private web browsing for those who are visually impaired. Furthermore, we aim to uncover more information about visually impaired users' attitudes, behaviours, concerns, and desires in online security and privacy to better understand their experiences. This information will allow us to identify limitations in using assistive technology for security and privacy tasks. Our results should help guide intervention techniques for users of this demographic.

1.3 Contribution

This research contributes to the foundation of universal cybersecurity. Our studies identify the current security and privacy concerns and barriers that exist for those with visual impairments when accessing websites. We aim to understand how these users perceive and manage web problems that impact their security or privacy.

We make four main contributions to the field of human-computer interaction:

1. We propose an amalgamated set of accessible and usable security heuristics rooted in related best practices and observed user behaviours.

2. We conduct a security and privacy focused expert evaluation of popular websites including government, eCommerce, and social media pages accessed via JAWS screen reading software.

3. We present empirical data regarding visually impaired individuals' security and privacy attitudes, behaviours, concerns, and general experiences.

4. We make user-centered recommendations for designing accessible interfaces that foster secure and private experiences when using screen reading and magnifying technology.

Other potential benefits of this research project include practical recommendations for industry professionals and government decisions makers. The outcomes of our project can provide a basis of security best practices tailored to visually impaired users. These best practices can be extended to those in web development who aim to create usable and accessible technology. Ultimately, the research project can continue to raise awareness of the challenges experienced by this traditionally marginalized group within the broader technology and cybersecurity community.

1.4 Thesis Outline

Our research begins in Chapter 2 where we discuss important web accessibility and usable security literature, and identify the gaps we aim to address.

Then we will use two distinct and complementary study approaches to answer the research questions we have posed. In Chapter 3, we will conduct an expert evaluation of websites, including WCAG-compliant sites, to assess whether it is possible to recognize and manage possible threats while using a screen-reader. In Chapter 4, we will conduct a user-study with visually impaired users to further explore areas of concern and to allow us to articulate users' habits in protecting their privacy and security on the web.

Lastly, in Chapter 5, we bridge the results of our two studies to identify commonalities in the results of our various research methods, address the research questions we have posed, share our insight in conducting security studies with visually impaired users, and make recommendations for future related research.

1.5 Publications and Presentations

Early results relating to our proposed heuristics have been accepted for publication in the 2018 ACM CHI Student Research Competition.

> D. Napoli, "Developing Accessible and Usable Security (ACCUS) Heuristics." In *Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems (CHI), Student Research Competition*, 2018.

A 45-minute workshop in applying our main findings while designing accessible interfaces has been accepted and will be presented at the 2018 Annual Accessibility Conference hosted by the University of Guelph. It will be recorded and made publicly available online and shared with our community collaborators and other relevant stakeholders.

> D. Napoli, "Design Tips to Help Non-Visual Visitors Stay Secure Online." presented at The 10th Annual Accessibility Conference: Designing for Diverse Abilities, University of Guelph, Canada, 2018.

Chapter 2

Background

For this thesis, we explore the intersect of two fields within the realm of human-computer interaction: accessibility and usable security. In this chapter we discuss key issues within each domain and identify areas of improvement for each field separately. Then, we discuss how the domains have overlapped, and we identify the gaps within accessible and usable security literature that our research will address.

2.1 Visual Impairments and Technology

Our research focuses on the technological experiences of users with sight loss. Sight loss refers to the degree of visual disability that cannot be accommodated through corrective lenses. Approximately 253 million people around the world live with some degree of sight loss [81]. Like most people, individuals with sight loss have become increasingly immersed in technology at work and at home. Canadians with sight loss, specifically, use the Internet to achieve tasks they would not normally be able to do and, in general, increase the quality of their daily life [23].

As with any disability, degrees of sight loss – here on referred to as "visual impairments" – vary immensely from person to person. For example, of the total 253 million population, 36 million people live with no sight [81], or are "blind," and 217 million people live with a low or medium amount of sight [81], or are "partially sighted."

A range of technology exist to assist people with any degree of visual impairment in participating in popular technology. This includes Braille displays, which translates on-screen text to a more tactile output, or keyboards with enlarged keys and print to improve the legibility of this common computer accessory.

Visually impaired individuals also rely on assistive software to enhance their access to computers or other personal devices. One form of assistive software, known as screen readers, interacts with a device's operating system to describe relevant information through audible outputs. Through keyboard shortcuts or other gestures, screen readers enable visually impaired users to traverse through a system's interface based on information they can hear. Popular screen readers include, Job Access With Speech (JAWS) [94], NonVisual Desktop Access (NVDA) [72], and VoiceOver on Apple Devices [57].

Other assistive software, screen magnifiers, enlarges on-screen interactions to make visual cues easier to see. Some screen magnifiers have screen reader functionality, and this allows partially sighted individuals to use both their vision and hearing to interact with technology. Some popular screen magnifier/readers are ZoomText [51] and SuperNova [74].

2.2 Web Accessibility

Web accessibility has been defined as, "all people, particularly disabled and older people, can use websites in a range of contexts of use, including mainstream and assistive technologies; to achieve this, websites need to be designed and developed to support usability across these contexts" [83]. Essentially, web accessibility researchers and designers aim to minimize the barriers found by people with various disabilities when using technology.

Accessibility research has also explored ways of improving technology to accommodate people various cognitive abilities (e.g. [47]), motor abilities (e.g. [62]), and autism (e.g. [89]). For this thesis, we solely address accessibility research pertaining to visual disabilities.

2.2.1 Visually Impaired Users' Experiences

Visually impaired users' browsing behaviours are evidently vastly different from sighted users' behaviours [91]. Thus, much research effort has focused on exploring visually impaired users' experiences. This research has identified a number of major issues impeding the usability of websites and other technological interfaces for these users.

User studies assessing visually impaired users' online experiences suggest that websites are about three times less usable then they are for their sighted counterparts [82]. Babu et al. [13] suggest a number of visually impaired users' problems violate Nielsen's [78] basic usability principles. For example, blind screen reader users often inadvertently exit out of form fields when trying to delete characters in input fields through the backspace button. This issue, the authors suggest, violates error avoidance and system satisfaction heuristics.

A number of issues pertaining to visually impaired users' online experiences have been associated with poor usability, including: confusing or misleading feedback, insufficient information, and compatibility issues between operating systems and assistive software [17, 68]. Furthermore, Vigo and Harper suggest that the inherent serial nature of screen reader outputs is one of the most impeding aspects of visually impaired web experiences [103]. They suggest that since information is delivered line-by-line, visually impaired users must resort to exhausting every possible option to overcome issues or gamble on different tactics to achieve their goals.

Lazar et al.'s survey [68] of visually impaired users' frustrations suggest that these individuals are more determined to spend time to fix issues than other sighted users, yet they still feel helpless and angry at the computer when sites are inaccessible. To compensate for these frustrations, Borodin et al.'s [17] observational study suggested that visually impaired users often develop personalized workarounds to overcome accessibility issues. Their results also highlight key characteristics of visually impaired users' browsing methods that have since been commonly noted in related literature, including: accelerated speech outputs [99,106]; navigation through headings and other page landmarks [110]; and skipping extraneous, irrelevant, or seemingly inaccessible content [20].

2.2.2 Professional Perception of Accessibility

Progress towards addressing the problems in visually impaired users' experiences heavily relies on developers, designers, and other stakeholders. Thus, professionals' perceptions of web accessibility has often been a topic discussion in related research.

Early surveys [46, 69] of webmasters, engineers, programmers, and other administrative staff suggest that the individuals involved in development processes are supportive of the "ethical" aspects of accessibility but cite limitations in organizational resources including time, money, or managerial support. Also, respondents often find web accessibility efforts hard to justify since visually impaired users make up a small portion of their total targeted demographic.

To coax stakeholders to invest in web accessibility, researchers [76,88] have emphasized the economic benefits of engaging the visually impaired population in eCommerce and other online businesses, and the consequential technological benefits of search engine optimization resulting from accessible websites.

Yesilada et al.'s [114] survey suggests that the understanding of web accessibility varies and conflicts among stakeholder groups. However, their results suggest that key driving motivations for web accessibility emphasize social implications of web accessibility, such as "being inclusive" or "being ethical," rather than the economic or technical advantages that are argued as important benefits of web accessibility. Additionally, Yesilada et al.'s [115] more recent survey suggests that the dissemination of specialized guidelines and other standards improve the validity of web accessibility and thus improve professionals' perceptions and investment in web accessibility.

2.2.3 Best Practices and Standards

In the early 2000s, Pernice and Nielsen [82] and Theofanos and Redish [100] proposed web accessibility design guidelines based on the results of task-based usability studies including visually impaired users. Each set of guidelines emphasized accommodating the observed user needs including: short, clear, straightforward audible cues to represent visual aspects of the design; longer automatic refresh times to accommodate lengthier browsing processes; and, the logical ordering of content to improve comprehension of audible assistive software outputs.

Though these guidelines are sound, they have not gained as much traction in the web development community as the World Wide Web Consortium's Web Content

Accessibility Guidelines (W3C WCAG). Both versions 1.0 and 2.0, with its corresponding Web Accessibility Initiative Accessible Rich Internet Applications (WAI-ARIA) techniques [30], are among the most commonly referred to web accessibility standards.

The initial version of the WCAG (1.0) [28] was published in 1999 as a reference for developing websites that can be used easily and quickly by a variety of audiences including people with disabilities. The document contains 14 "checkpoints" that developers can use to aid the accessibility of their systems. These checkpoints were prioritized into three levels that increased in programming complexity and level of accessibility. For example, in the WCAG 1.0, Priority 1 checkpoints includes elements, such a text equivalent for images or sounds, that developers "must" satisfy to ensure accessibility. Priority 2 checkpoints, such as properly identifying lists and list items, are considered aspects that developers "should" satisfy. Priority 3 checkpoints, including providing options for users to receive information in their preferred language or content type, are optional suggestions that address the broadest range of disabilities

The WCAG 2.0 [29] was released in 2008. It elaborated upon previous checkpoints and established four overarching themes in achieving web accessibility: Perceivable, Operable, Understandable, and Robust (POUR). Essentially, a website abiding to the POUR principles would be easy to comprehend and use by a number of users with a variety of abilities who may use assistive tools.

The WCAG 2.0 also categorizes POUR principles into three levels (A, AA, and AAA) ranging from lowest to highest degrees of conformance. Level A conformance includes providing basic accommodations such as alternative text. Level AA requirements build upon the previous level and include providing heading labels which describe the content's purpose. Level AAA conformance includes more complex solutions which accommodate wider sorts of disabilities including providing synchronized pre-recorded sign language interpretation for all digital media. This level of conformity is not often achievable nor enforced therefore, Level AA is often a more realistic level of WCAG 2.0 conformity.

The WCAG 2.0 guidelines have been adopted by stakeholders around the world, and are noted in number of national laws including Section 508 [50] of the United States of America and the Disability Discrimination Act [11] of the United Kingdom. In Canada, the Accessibility for Ontarians with Disabilities Act (AODA) [22] requires all public and private (with more than 50 employees) organizations' to ensure their web content meet WCAG Level AA criteria by January 2021. This means that the majority of websites which are owned by Ontarian organizations must abide by more than the basic WCAG requirements or face administrative penalties or other court enforcements [80].

2.2.4 WCAG Implications

From a user perspective, web accessibility is not defined by technical checkpoints but rather, it is rooted in positive experiences. As Aizpurua et al.'s [4] results suggest, visually impaired participants consider websites as "accessible" if the page contains content and functionalities that matched their expectations and worked in a manner that allow them to complete their desired tasks. Evidently, websites that do not adhere to the WCAG can still be considered accessible if they meet users' usability needs.

Therefore, accessibility and usability seem to be complementary aspects of an interface. Aizpurua et al.'s [5] follow-up study found strong significant correlations between the hedonistic qualities associated with perceived accessibility and common usability attributes including: manageable, practical, clear, and exciting. Commonalities between accessibilty and usability principles have been highlighted elsewhere. In fact, HCI experts [13, 84, 90] have uncovered several usability issues on web pages that abide to the WCAG and therefore emphasize that approaching web accessibility through technical requirements alone is ineffective.

The WCAG's shortcomings have been attributed to the impracticality of applying the guidelines during development processes [65]. Others [71] suggest that the WCAG oversimplifies disability and therefore denies designers the ability to be deeply understand and improve interfaces. Web developers [67,119] have argued against the W3C's general approach to developing the WCAG. Most notably, in the controversial, "To Hell with WCAG 2" [27], former W3C volunteer Joe Clark notes that people with disabilities are essentially excluded from shaping and contributing to the guidelines.

Thus, the WCAG may be an influential resource to designing systems for people with disabilities, but it still requires improvement. One way to improve the WCAG, and the general state of web accessibility, is through user-centered approaches based in richer and real world contexts. Accessibility researchers [31, 32] also urge future work to focus on better defining, documenting, and meeting users needs.

2.3 Usable Security

The field of usable security emphasizes the value of assessing and integrating user behaviours within the design of security mechanisms. Over the past two decades, researchers have emphasized that tailoring to the human aspects of security and privacy systems can help curb the severity of security and privacy threats (e.g. [97, 120]).

Some of the main security and privacy threats that users face when browsing the web include: password hacking [64], phishing [41,96], man-in-the-middle attacks [111] and, malicious software [40, 44]. Usable security research has explored how to assist users in behaving in a security- and privacy-aware manner to avoid online threats; yet, as we will discuss later, most usable security research has focused on users with average sight abilities.

2.3.1 Design Guidelines and Frameworks

In 2014, Garfinkel and Lipford [48] summarized the progress in the usable security domain. Per their summary, the main lessons learned from usable security research suggest that security systems should: reduce security responsibility on system users, enable more secure defaults, provide clear and concise instructions, describe security contexts, and generally train users to adopt best practices.

Several usable security researchers have proposed practical guidelines to user-centered security systems (e.g. [26,59,79]). We highlight one set of key usable security design guidelines and a commonly adopted security framework below.

In “Why Johnny Can’t Encrypt...” [108], Whitten and Tygar proposed pivotal usable security principles encompassing four main priorities: 1) ensure users can know what security tasks are required, 2) explain how to successfully complete related tasks, 3) design to prevent dangerous errors pertaining to security, and 4) make them comfortable enough to use the system again. These principles were intended to guide the design of the user-facing dimensions of security systems.

Cranor [34] proposed the "human-in-the-loop" security framework to properly integrate humans in security processes that cannot be solved through automation. This framework emphasizes the need for effective communication pertaining to warnings, notices, status indicators, training, and policies with *human receivers*, or users, to ensure security information can be appropriately processed and executed. Designers adopting this framework can identify and mitigate human-related failures within their security system.

2.3.2 Applying Usable Security Principles

These influential works do not suggest that usable security can be solely achieved through visual means; yet, much of the key solutions to assist users in managing web-based threats have been primarily vision based.

Work has gone into honing the visual representation of security indicators embedded in the browser chrome including "HTTPS" and corresponding lock icons [107]. Li et al. [73] suggested that highlighting a site's domain within the URL address bar can also allow users to quickly examine and identify phishing. Additionally, Abbasi et al. [1] suggested that some tool bars can significantly increase users' ability to detect and avoid phishing.

Users who engage with browser indicators are usually provided supplemental information regarding their state of security. For example, clicking on the lock icon in Internet Explorer will bring up a dialogue which details the site's SSL or TLS certificate information. Biddle et al. [16] proposed a SSL dialogue redesign that presents web site ownership and other corresponding security information more comprehensibly. Felt et al. [43] further proposed methods of tailoring textual information to improve users' comprehension of the security threat to increase the likelihood that users will remember and obey related warnings.

Outside of the browser chrome[1], Dhamija and Tygar [37] proposed "dynamic security skins," or hashed background images specifically assigned to windows that are authentic and secure, to assist users' in identifying spoofed sites. Schechter et al.'s [93] study shows that users will share sensitive information on pages with or without the presence of HTTPS and lock icons; but, users may be deterred by the absence of "authentication images" that are associated with credible pages. Additionally, since users do not consistently adhere to static, chrome-based security indicators, Egleman et al. [41] suggested that users are more likely to adhere to active warnings which fill up the entire page and interrupt users' processes.

"Habituation" is the term that refers to users ignoring or dismissing warning messages and is cited to be one of the leading causes of users' failure to comply with security indicators [19]. Anderson et al. [9] propose that polymorphic variations of visual warnings, such as windows that jiggle or change in size and colour, are more resistant to habituation effects.

In sum, usable security literature prioritizes users' evident behaviours and mental models. However, usable security literature has particularly focused on vision-based methods of guiding users in secure online behaviours. Garfinkel and Lipford [48] suggest that usable security research should expand to include different computing environments and user populations like those with disabilities. Exploring non-visual security mechanisms, tailored to those who are visually impaired, can begin to address the evident void in usable security literature.

2.4 Accessible and Usable Security

Considering the difficulties in developing suitable security systems and truly accessible interfaces, visually impaired users' vulnerability to cybersecurity threats is concerning. Yet, research at the crux of accessibility and usable security is uncommon; there is a lack of understanding which security issues pose usability challenges for visually impaired web users [55].

[1] Browser chrome refers to the aspects of a Web browser surrounding page content including tool bars, menus, scroll bars, etc.

2.4.1 Visually Impaired Users' Security Concerns

Some researchers have sought to document visually impaired users' security and privacy concerns, and identify technological pain-points and unmet needs particular to this user group.

Ahmed et al. [3] interviewed participants regarding their physical privacy and related computing concerns. One of their key findings suggests that participants found banking and shopping online more accessible than in-person services. While engaging in these in-person services, participants faced several accessibility issues and privacy threats, including shoulder-surfing and eavesdropping. These problems forced visually impaired users to rely on inconvenient coping solutions which ultimately impeded their comfort and potential security including: disabling the screen even if they required visual cues, wearing headphones which minimized their awareness of physical surroundings, and relying on trusted sighted assistants to complete transactions on their behalf.

Inan et al. [56] also surveyed visually impaired individuals to identify their online usage trends and related security and privacy concerns. Like Ahmed et al.'s study, their results suggest that a number of visually impaired users actively bank and shop online but have a number of concerns and consequently face severe accessibility issues. Specifically, Inan et al.'s participants identified viruses, CAPTCHAs, and spam emails among the most frequent security issues they faced while using the Internet. Participants were most concerned with threats to financial and personal information.

Regal et al. [87] also conducted surveys and focus groups with visually impaired users regarding online privacy threats and uncovered similar concerns regarding malicious software (spyware and adware), unauthorized access to search history, and location-based data tracking. Regal et al. suggest that these concerns could be addressed through software which blocks users' data from being tracked. Thus, in the same paper, they further evaluated the accessibility of four popular tracking blockers through task-based user studies with 10 visually impaired users. The results of their usability evaluations suggested that existing tracking blockers are inaccessible and often not compatible with screen reader keyboard short-cuts. The researchers deduced that security software tailored to visually impaired users should emphasize control, feedback, personalization, and effective information.

2.4.2 Evaluation of Security Indicators

Researchers have explored the usability and accessibility issues pertaining to web-based security indicators.

Through an expert evaluation via screen reading software, Buzzi et al. [21] assessed the issues pertaining to completing a purchase through eBay. Their main findings suggested that some important page elements for screen readers, including headings and tables and security information, were not sufficiently described and therefore could impede users' purchasing abilities.

Dosono et al. [39] observed visually impaired users perform login tasks on email, banking, and eCommerce websites via screen reading software. As Buzzi et al. identified in their expert evaluation, each website contained poorly labelled and located page elements which caused usability and accessibility issues. Poorly labelled login elements confused visually impaired users and, at times, misled them to a false sense of security. Additionally, other accessibility issues pertaining to audible password masking, insufficient error messages, and recovery methods negatively impacted users' control of their accounts containing sensitive information.

2.4.3 Novel Solutions

Researchers have also proposed novel solutions to address the security and privacy issues visually impaired users experience. Much of this work has focused on making authentication processes more accessible.

Researchers have proposed observation-resistent password schemes [75, 92] that relate to visually impaired users' physical privacy concerns that Ahmed et al. uncovered. One novel solution, PassChords [12], is an observation-resistant password system specific to the Apple iPhone. The system allowed visually impaired users to access their smartphones three times faster than using traditional PINs. However, since the program requires users to create passwords based on patterns set by combinations of tapping various fingers, the passwords did not yield the entropy required to effectively resist brute-force attacks.

Researchers have also proposed accessible password managers. UniPass [15] aimed to improve their system's accessibility by integrating aspects that lend themselves well to non-visual users, including supporting biometric (finger ID) authentication options, avoiding touch-screen gestures that require visual navigation, eliminating time limits, and using concise audio descriptions for dialogues. During evaluation, visually impaired users preferred the UniPass system over other password managers.

Much work has also gone into designing accessible Completely Automated Public Turing tests to tell Computers and Humans Apart (CAPTCHAs). The SoundsRight CAPTCHA [70] is an audio mechanism that requires users, sighted or not, to identify sounds within a provided clip. This mechanism allows users to engage in a security process through their hearing abilities rather than vision, and thus, proved successful at accommodating visually impaired users.

Researchers have also proposed other methods in improving visually impaired users' online security. The MASPHID model [98] aims to assist visually impaired users in detecting phishing websites through automated checks. However, the model has not been tested with targeted users and the usability of this method has not yet been assessed.

2.5 Summary

In summary, both web accessibility and usable security can be improved. Within web accessibility, experts suggest that researchers and designers must focus on furthering empirical evidence in order to evolve and accurately accommodate visually impaired users. The field of usable security usually relies on documented user behaviours as means to designing user-centered security systems. However, as of now, the domain has not yet sufficiently addressed the unique security needs of visually impaired users.

Current accessible and usable security literature can benefit from further research exploring whether users with visual impairments can adequately handle the cybersecurity and privacy risks that they face while navigating the web. Our research will contribute to the efforts pertaining to collecting empirical information about visually impaired users' behaviours. This research will also provide basis for practical recommendations in developing non-visual security mechanisms tailored to visually impaired users that have not yet been explored in relating literature.

Chapter 3

Expert Evaluation

3.1 Introduction

We begin this chapter by defining a set of heuristics that combine accessibility and usable security principles. Next, we assess 10 websites using two online, automated accessibility checkers. Then, we conduct an expert evaluation including cognitive walkthrough and heuristic evaluation techniques to reassess the 10 websites. Through our expert evaluation, we investigate issues that occur when using screen reading software to identify, and prevent, digital threats on web pages from a usable security perspective.

Our results provide an estimate of the obstacles that may impede the success of visually-impaired users' security and privacy techniques while using a screen reader. They also explore whether websites meeting W3C WCAG guidelines can sufficiently aid visually impaired users in addressing security and privacy concerns while online.

3.2 Proposed Heuristics

Individually, guidelines for accessible web design and usable security systems have existed for quite some time. In 1999, the W3C published the WCAG [28], a set of recommendations in creating web-based content that is accessible to people with a range of disabilities. This same year, Whitten and Tygar [108] proposed four pillars of usable security.

Each of these guidelines have progressed. The WCAG 2.0 [29] solidified web accessibility through the POUR framework, and usable security researchers have added to Whitten and Tygar's definition of usable security; for example, Chiasson et al. [25] proposed additional dimensions addressing users' need for sufficient feedback regarding tasks and system states.

Yet, thus far, related work has not been generalized into a single set of heuristics that explicitly address the design of web-based security cues for users with visual disabilities. Since browsing behaviours differ greatly between sighted users and visually impaired users [2, 8], it is critical for designers to address the unique nuances between these two user groups when creating for usable security. Below we describe our methods in developing a first iteration of accessible and usable security (ACCUS) heuristics which aim to blend best practices of each domain.

3.2.1 Defining the ACCUS Heuristics

We began our process by referring to existing literature within accessibility and usable security. As experts have noted, there is significant overlap between web accessibility and usability concepts [13]. Specifically, much of the Nielsen's usability heuristics [77] can be directly mapped to the four principles of the WCAG. The connections we draw between the WCAG and Nielsen's heuristics are based in Casare et al's comparisons [24] and summarized in Table 3.1.

In brief, the *perceivable* principle within web accessibility focuses on providing users sufficient information to properly understand interface components. This relates most to Nielsen's heuristics including: visibility of system status (H1) and minimalistic design that do not diminish important components (H8). The *operable* principle pertains to ensuring the interface is navigable. Ease of use, and navigability, is most related to Nielsen's user control and freedom (H3) principle. The error prevention (H5) and recognition rather than recall (H6) heuristics are also important factors to easily navigable interfaces. The *understandable* WCAG principle refers to the usability of a system's language, layout, and functionality. Nielsen similarly emphasizes the need for the system to "speak the users' language" (H2) and matching existing conventions that are accustomed to users (H4). *Robust* interfaces are compatible with various assistive technologies. Nielsen's heuristics do not explicitly address these tools but do suggest that systems should be flexible and efficient enough to accommodate a range of users' experiences and abilities (H7).

WCAG Principle	**Description**	**Related Nielsen Usability Heuristics**
Perceivable	All system content (textual and non-textual) and general structure is unambiguously conveyed to users.	**H1**, H2, H3, **H8**, H9
Operable	All functionality is controllable and minimizes potential for error.	H1, H2, **H3**, H4, **H5**, **H6**, H7, H8
Understandable	The system's language, layout, and component behaviour is predictable and not complex.	**H2**, H3, **H4**, H5, H6, H9, H10
Robust	Various alternate technologies are compatible with the system.	H1, H2, H3, H5, H6, H9, H10

Table 3.1: A summary of the relationship between the W3C's WCAG 2.0 and Nielsen's usability heuristics. The most relevant Nielsen heuristics are in bold.

Next, we integrated usable security principles by surveying 25 related peer-reviewed articles published from 1999 to 2017 (Appendix A). These articles included Garfinkel and Lipford's [48] summary of prominent usable security solutions, Balfanz et al.'s [14] lessons learned from the field, Jagatic et al.'s [60] main findings from a phishing experiment targeting 581 university students, and Fogg et al.'s [45] survey of over 2,000 web users' habits in protecting themselves online. We also assessed additional accessibility suggestions from Theofanos and Redish [100], Akhert et al.'s [6] framework to engineering online trust for differently-abled people, and Azenkot et al.'s [12] design guidelines in tailoring passwords for visually impaired users.

We extracted and open-coded [101] 172 usable security and accessibility best practices, expert recommendations, and documented sighted/non-sighted user behaviours (Figure 3.1). We iteratively categorized the data to track common themes and develop heuristics that best reflected the data. We were able to confidently sort 154 pieces of data into relating categories. The remaining 18 excerpts did not fit the themes so we excluded them from our final results.

This process was done by the lead researcher and therefore may have bias towards their single interpretation. Future research may benefit from multiple coders if intercoder reliability is maintained.

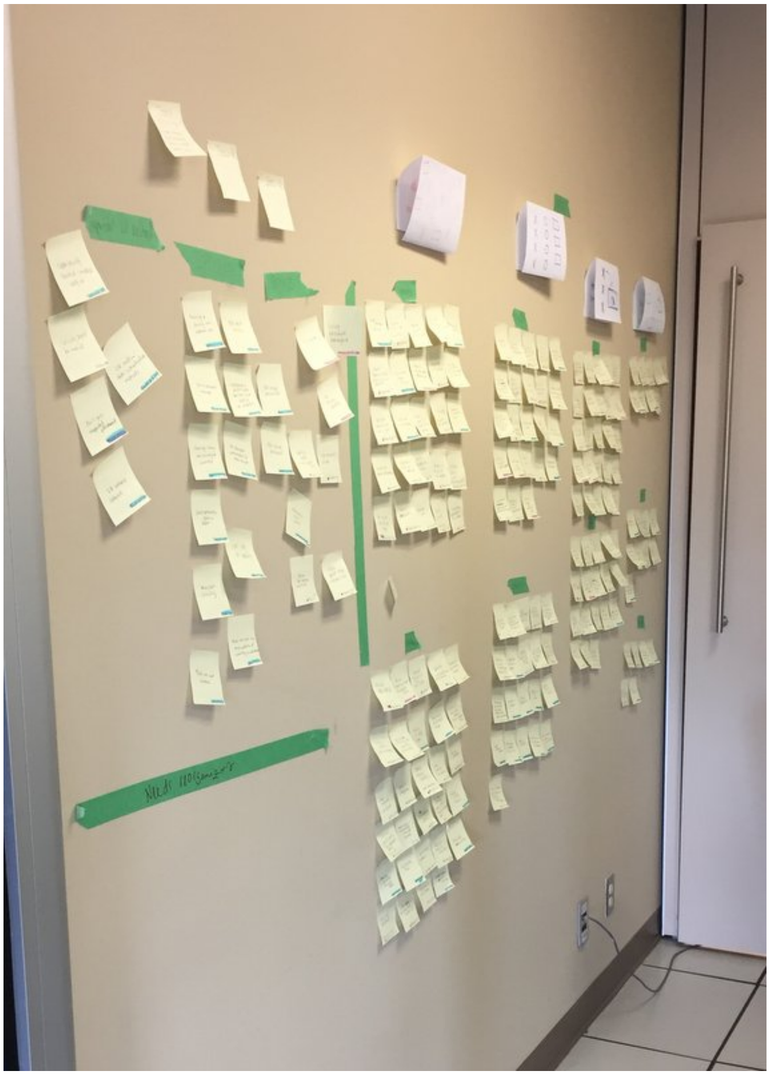


Figure 3.1: Our process in open-coding 172 recommendations from usable security and accessibility best practices.

3.2.2 ACCUS Heuristics

Nine heuristics emerged from our open-coding process. For the purposes of usability evaluations, we describe guiding questions in Table 3.2 to assist experts in assessing interfaces according to our proposed heuristics.

We elaborate on each ACCUS heuristic below. In these descriptions, we mention at least two articles that supported our resulting theme, however our final results are not exclusive to those that are cited. We consider each principle interdependent and do not intend a level of hierarchy when numbering the guidelines. Finally, these heuristics should be interpreted in the context of security and privacy for non-visual usage:

A1. Informative

Across accessibility and usable security literature, there is a particular emphasis on allowing users to make informed decisions when interacting with interfaces. In both domains, experts advise that interfaces should communicate informative, yet brief and parsable messages to users [43, 100]. For visually impaired users specifically, the text of these messages should be available for audible delivery, and should reflect the underpinning contextual connotations that are visible to sighted users through design elements such as colour or symbols [38].

A2. Verifiable

Usable security experts emphasize that the current state of security/privacy and related options should be explicit to users [25, 87]. This security information must be described with plain language and avoid jargon so that it can be comprehensible to range of users with disabilities including visual loss [79, 112].

A3. Recognizable

To improve navigability, the security information and functionalities within the system must be distinguishable and organized in a way that helps the users' mental

No.	ACCUS Heuristic	Guiding Questions
A1	Informative	Are messages clear and represented within appropriate contexts to the user? Is the information organized in a logical way? Does the content reflect keywords the user may expect to find?
A2	Verifiable	Is it clear to the user that security mechanisms are engaged? If not, is it clear how they can enable these options? Are threats presented to the user in manner they can relate to? Can users engage in the system safely based on the information provided?
A3	Recognizable	Is security information identifiable and organized appropriately? Does information appear in the expected order? Do distinct boundaries define important objects and actions? Does the system follow a minimalistic design that is useful and direct to the user?
A4	Assistive	Does the system provide recommendations in behaving safely? Are policies presented to the user? Are secure defaults apparent and customizable? Are available security-related decisions appropriate for the user?
A5	Functional	Do all functions describing the system's security work? Are they compatible with assistive technology?
A6	Controllable	Can the user complete security tasks with their assistive technology? Does the system allow a user to manage their risks with the tools they use? Can the system be personalized to the users specific wants and needs?
A7	Responsive	Does the system give adequate feedback? Can a user verify the success and safety of what they have done? Is feedback clear and non-intrusive?
A8	Diverse	Is security and privacy information clearly designed to meet the varying needs of persons in the target demographic? Is this information flexible enough to be communicated to a range of user abilities?
A9	Memorable	Can a user learn how to use the security and privacy mechanisms? Can a user remember how to use these mechanisms? Will the user be comfortable enough to use these mechanisms again?

Table 3.2: Guiding questions for the nine ACCUS heuristics that emerged from our survey of accessibility and usable security literature.

models [4]. These elements must be clearly apparent and traversable with assistive software such as screen readers or magnifiers when needed [55].

A4. Assistive

Users should be guided through security decisions to be made [6]. Error prevention conventions must be in place to assist users in avoiding detrimental security mistakes [112]. Similarly, security defaults should be appropriate for users' expertise, but can be modified within reasonable confines. Users should be able to recognize, diagnose, and correct mistakes if they occur [2].

A5. Functional

To avoid miscommunicating security states, the security cues in a system should work as expected in a quick and complete manner [2]. No functionalities (such as time-outs or authentication) should impede on users' security, nor privacy.

A6. Controllable

The security cues must be compatible with assistive technology, if needed. The interface should offer robust and customizable means to protect users with various needs [12].

A7. Responsive

All security and privacy actions, errors, and threats are effectively communicated without interrupting users' workflow [25, 87]. Users must be able to identify when a task is completed.

A8. Diverse

All security and privacy content and context is communicated in a way that accommodates users with visual disabilities [59]. Satisfactory alternatives, both visually and aurally, should be available for those with partial or no sight [87].

A9. Memorable

All security and privacy functions and related user actions require a low cognitive load to avoid mental fatigue. The system should be designed for learnability and evoke high recall abilities [100].

3.3 Website Evaluation

To gain initial insight of the accessibility and usability of existing security indicators, we use two evaluation techniques including: automated accessibility checkers, and an expert evaluation via JAWS. As we will elaborate, our results differ and highlight the differences between the two assessment approaches. Our findings also suggest that solely adhering to the WCAG Level AA compliancy may be insufficient in ensuring usable security and privacy mechanisms.

3.3.1 Apparatus

For both stages of the website evaluations we used a Windows 10 computer, a standard keyboard, mouse, and 22-inch monitor.

For the automated testing, we used two online accessibility checkers used in related accessibility literature [49,116]: WAVE [105] and AChecker [10]. When provided with a URL address, these checkers compare a single page's mark-up against the WCAG 2.0 criteria. Any violations are identified as "errors," and therefore suggest potential accessibility issues.

During the expert evaluation, we used the most recent version of screen reading software used in accessibility literature [52], Freedom Scientific's Job Access With Speech (JAWS 18) [94]. Usable security studies involving JAWS usually use Internet Explorer (IE) when performing related experiments because it is most compatible with JAWS [39]; similarly, we used IE 11.64 to browse the web.

In both stages, we assessed the ten websites described in Table 3.3. We chose these sites because they can be vital resources to users who require information for things such as government resources, post-secondary information, eCommerce, and postal services. Many of the sites represent a range of services that a visually impaired user might access. These sites provide the opportunity to exchange sensitive information for services such as updating official identification documents, paying bills, and shopping online. Users expect these sites to provide a level of security and privacy since they involve their associated personal data; thus, we consider these sites suitable for a usable security expert evaluation.

3.3.2 Automated Assessment

Although automated testing methods are limited in their ability to evaluate contextual issues pertaining to Web accessibility adherence [102], a number of related studies have relied on free online checkers to estimate the potential for general accessibility issues on popular websites [117, 118].

Method

Based on past experiences in using online accessibility checkers, there is potential for some systems to over (or under) estimate Level AA errors. To offset these discrepancies, we document the average number of issues identified via WAVE and Achecker. We did not include cautionary alerts because confirming these flags would require further expert evaluation beyond the scope of this research. The counted issues were specific to the HTML files available through the websites' homepages.

ID	Title	URL	Level AA Issues Mean (SD)
W1	Canada Post	https://www.canadapost.ca	8.0 (0.0)
W2	ServiceOntario	https://www.ontario.ca/page/serviceontario	2.5 (2.1)
W3	eCampusOntario	https://www.ecampusontario.ca	11.5 (4.9)
W4	TD EasyWeb	https://easyweb.td.com	2.0 (0)
W5	Carleton Grad Studies	https://gsapplications.carleton.ca	3.0 (1.4)
W6	Hydro Ottawa	https://hydroottawa.com	4.0 (5.6)
W7	Gmail	https://mail.google.com	3.0 (1.4)
W8	Presto	https://www.prestocard.ca	10.5 (13.4)
W9	ViaRail	http://www.viarail.ca	8.0 (1.4)
W10	Facebook	https://www.facebook.com	3.0 (0.0)

Table 3.3: The websites evaluated and the average number of issues identified through automated testing.

Results

The average number of Level AA issues per site ranged from 2.0 to 11.5. Common errors included mislabelled elements and lack of distinguishable content (colour contrast between foreground and background). Based on the results of the online checkers (Table 3.3), we expect the sites containing the fewest errors to also have the fewest ACCUS issues during the next stage of our evaluation.

3.3.3 Expert Evaluation

Within the usable security domain, expert evaluations have been used to gain insight of potential usability issues pertaining to security mechanisms [42, 108]. To better assess the accessibility and usability of the 10 websites websites, we used a task-based hybrid usability evaluation approach which combined aspects of cognitive walkthrough and heuristic evaluation methods.

We chose not to disable the monitor during the evaluation to observe the discrepancies between visual and aural information. We did not use a mouse and only relied on keyboard shortcuts (like the Tab button) to try to complete the tasks.

Method

During a cognitive walkthrough, evaluators assess issues pertaining to a set of predefined tasks and action sequences [95]. Our assessment was guided by three main tasks: 1) verify the site is legitimate, 2) login to the site, and 3) complete a site-specific task (Table 3.4).

To understand how the websites facilitate secure browsing behaviours, the action sequences for Task 1 and 2 followed expert security advice and related documented trends in user behaviours.

Task 1: Specifically, during Task 1 (verify the site is legitimate) we aimed to complete the following actions:

1. Parse URL for domain inconsistencies

2. Check SSL certificates for an encrypted connection

ID	Title	Site-Specific Transaction
W1	Canada Post	Purchase stamps
W2	ServiceOntario	Renew a health card
W3	eCampusOntario	Find details about a computer science program
W4	TD EasyWeb	Pay a bill
W5	Carleton Grad Studies	Register for an application account
W6	Hydro Ottawa	Request electrical services at home address
W7	Gmail	Download an attachment
W8	Presto	Reload a transit pass
W9	ViaRail	Purchase a round-trip ticket
W10	Facebook	Send a private message

Table 3.4: The site-specific transactions (or tasks) attempted during the expert evaluation for Task 3.

3. Scan page content for signs of phishing

4. Find evidence of copyright/authoring information

Task 2: We started Task 2 (log in to the site) by locating and accessing the login page. Then, we attempted to locate the relevant username and password form fields. Finally, we submitted our credentials in order to grant access to related accounts.

Task 3: We expected Task 3 to have the greatest variability in accessibility issues. Since users with sight loss make personal workarounds to overcome obstacles they face online [17,68], Task 3 was not constrained to a specific sequence of actions. However, to manage the scope of our evaluation we limited our assessment to three separate attempts. [1]

Navigating with a screen reader can be a lengthy process due to accessibility issues and the forced sequential nature of information delivery. To manage this, we imposed additional time limits on the assessments if the attempt limitations were not consumed. We allotted ample time for each task with a maximum of 30 minutes to verify the site's legitimacy, 15 minutes to login, and 45 minutes to complete site tasks.

[1] Comparative usability studies [33] have found that visually impaired users take about three times longer, and make three times more errors, than sighted users when completing similar tasks. We argue that browsing with JAWS during our evaluation should not exceed this number of trials.

Like a heuristic evaluation, we evaluated audible feedback against the ACCUS heuristics. We noted each issue and rated its severity as a level 1 (a cosmetic issue that does not greatly interfere with usability), 2 (minor usability issue), 3 (major usability issue) or 4 (catastrophic issue that critically deters the progress of completing a task).

Results

Generally, we spent 60 to 90 minutes evaluating each website. Table 3.5 summarizes the number of issues, and average severity, identified per website. We provide examples of the issues found on each website in Table 3.6. In most cases, the issues we describe violated several heuristics but we list the most relevant heuristic and its corresponding severity.

As illustrated in Figure 3.2, the websites containing the greatest number of ACCUS issues included the Hydro Ottawa (n = 135), TD EasyWeb (n = 106), and ViaRail (n = 109). The ViaRail site also contained some of the most severe usability issues (M = 3.2, SD=0.8). Although fewer, the issues found on Canada Post (M = 3.4, SD=0.8) and ServiceOntario (M = 3.3, SD=0.8) were most severe.

When focusing on issues per heuristic, Figure 3.3 shows that the greatest number of issues discovered were related to the *Controllable* (A6, n = 172.0), *Recognizable* (A3, n = 130.0), and *Responsive* (A7, n = 129.0) heuristics. The most severe issues pertained to the *Functional* (A5, M = 3.5, SD=2.0), *Diverse* (A8, M = 3.3, SD=2.1), and *Assistive* (A4, M = 3.3, SD=2.1) heuristics. These findings suggest that although the most common issues are related to the website's structure and contents, the most problematic issues are related to opportunities for visually impaired users in behaving securely on the website.

We were unable to complete Task 1 on any site. We also faced significant issues during Task 2 and 3 that restricted our ability to complete those tasks on several sites. The greatest number of (n = 362), and most severe (M = 3.2, SD=0.8), issues occurred while attempting to complete site-specific tasks.

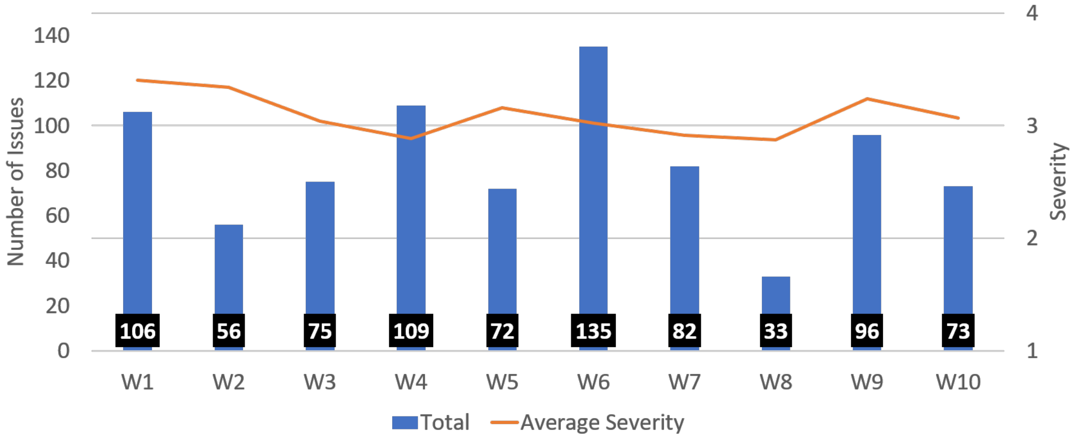


Figure 3.2: The total number and average severity of issues found per website.

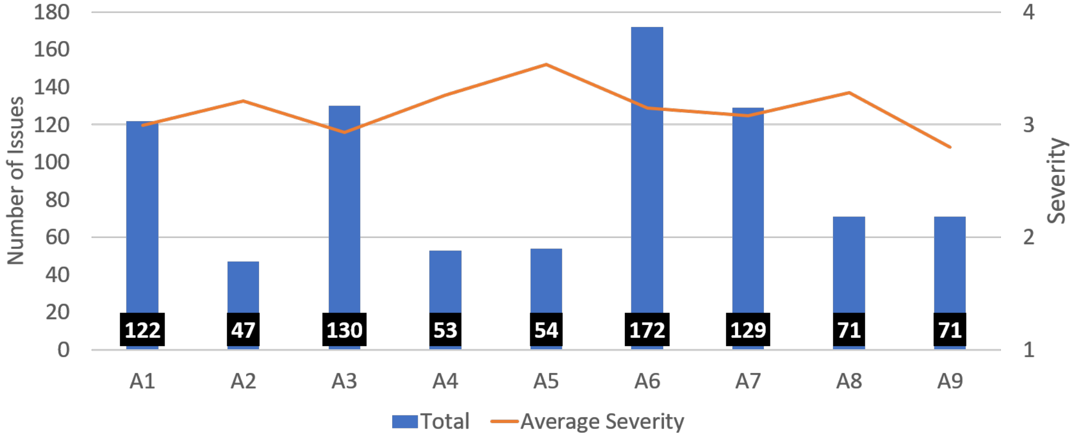


Figure 3.3: The total number and average severity of issues found per ACCUS heuristic.

ID	Title	Verify	Login	Site Task	Task Completed	Total Issues	Mean Severity
W1	Canada Post	*45	*37	*24	0/3	106	3.4
W2	ServiceOntario	*20	N/A	36	1/3	56	3.3
W3	eCampusOntario	*11	35	*29	1/3	75	3.0
W4	TD EasyWeb	*38	21	50	2/3	109	2.9
W5	Carleton Grad Studies	*30	N/A	*42	0/3	72	3.2
W6	Hydro Ottawa	*30	34	*71	1/3	135	3.0
W7	Gmail	*30	32	20	2/3	82	2.9
W8	Presto	*13	8	12	2/3	33	2.9
W9	ViaRail	*18	*30	*48	0/3	96	3.2
W10	Facebook	*20	23	*30	1/3	73	3.1
Tasks completed		0/10	6/8	4/10			
Total issues		255	220	362			
Mean Severity		3.04	3.11	3.15			

Table 3.5: Number of issues identified per website. Asterisks mark the tasks abandoned by the evaluator due to time or trial limitations.

ID	Title	Example of Uncovered Issue	Heuristic	Severity
W1	Canada Post	Cannot properly access nor input information within login pop-up window and therefore impedes the accuracy and safety of the login process.	A6	4
W2	ServiceOntario	Errors pertaining to the formatting of personal information are not read aloud automatically. This impedes users' ability to input sensitive information confidently and accurately.	A7	3
W3	eCampusOntario	No alternative text describing log out button. Impedes users' ability to revoke access to their accounts.	A8	3
W4	TD EasyWeb	When landing on the homepage, automatically redirected to new URL address. Address contains meaningless characters including, "waw" and "execution" which impede methods of checking for domain inconsistencies.	A3	3
W5	Carleton Grad Studies	No alternative text to describe important memo regarding system maintenance and future unavailability.	A1	3
W6	Hydro Ottawa	Alternative text describing the password field repeated 4 times before allowing access and input capabilities which negatively impacts user's cognitive load.	A9	2
W7	Gmail	Inconsistent URLs between website and document host site which interferes user's ability to verify the site's legitimate address.	A2	3
W8	Presto	Upon finalizing purchase, page refreshes and reads irrelevant content before telling the user the purchase has been confirmed.	A7	2
W9	ViaRail	Visual and non-visual cues are misaligned as the reader automatically reads page content behind login pop-up window when attempting to sign in.	A3	3
W10	Facebook	Insufficient alternative text, "[date] 43534634..." in identifying a message's recipient making it very difficult to ensure the message's privacy.	A1	3

Table 3.6: Example issues found per website. We note each issue's most related heuristic and severity out of 4.

3.4 Discussion

We used WAVE and Achecker to assess 10 websites' compliance to the WCAG. The automated accessibility checkers found few web accessibility issues. Yet, through our expert evaluation, we uncovered several severe usability issues regarding the security and privacy information on all websites. Our results suggest that simply complying to the WCAG is not sufficient to enable users to act securely.

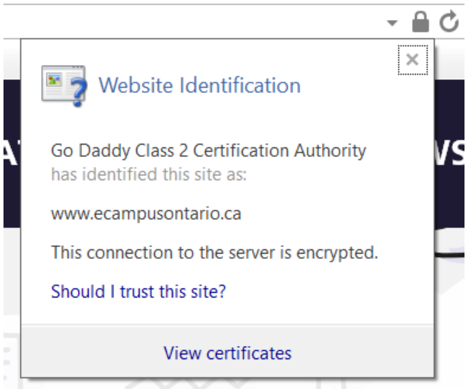
We cannot draw confident conclusions based on the quantitative results of our expert evaluation because each assessment varied greatly depending on the site's general compatibility with JAWS. Some sites had seemingly fewer issues but were not necessarily more accessible nor usable. For example, we were unable to verify the legitimacy of any of the ten sites. This limited the total number of issues we could discover pertaining to Task 1. Additionally, some sites like ViaRail (W9) and Facebook (W10) may contain more issues than we uncovered since several severe accessibility and usability issues impeded our ability to complete Task 2 and Task 3 to properly assess the site.

Therefore, to better understand all of our findings we discuss a few of the most concerning issues uncovered while completing the three assigned tasks. We also discuss their implications on a user's ability to abide to common security expert advice. Finally, we compare the results of our two evaluation methods to interpret which sites may provide visually impaired users the most usable means to behaving securely online.

3.4.1 Verifying Site Legitimacy (Task 1)

When we attempted to verify the legitimacy of each website, we could target address bars with the keyboard, `Alt + D`, and parse through the URL character by character using the arrow keys. This two-step process allowed us to check for security indicators such as familiar domains and HTTPS.

However, JAWS was unable to access the text within Internet Explorer's security report dialogue (Figure 3.4). The browser provided this alternative text when selecting the lock icon: "Tool bar security report button. To activate press the space bar." This information did not describe the lock itself, nor explain the "secured" context

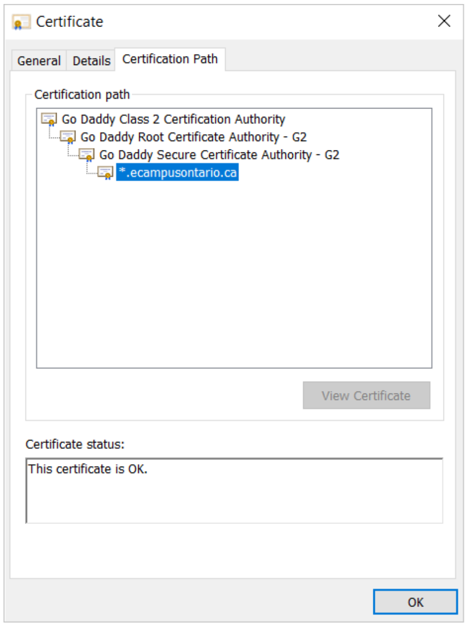

Website Identification

Go Daddy Class 2 Certification Authority
has identified this site as:

www.ecampusontario.ca

This connection to the server is encrypted.

Figure 3.4: Text within Internet Explorer 11's security report unreadable by JAWS.



Certification path

- Go Daddy Class 2 Certification Authority
  - Go Daddy Root Certificate Authority - G2
    - Go Daddy Secure Certificate Authority - G2
      - *.ecampusontario.ca

Certificate status:

This certificate is OK.

Figure 3.5: Navigation required for JAWS to read host certificate.

it visually denoted.

Additionally, the text within the security report pertaining to SSL certificates could not be accessed by various JAWS reading commands, including all four `arrow keys` and `insert + up`. Furthermore, since the close button was automatically selected by default, the system cued users to exit the report immediately by announcing: "Security report. Close button. To activate press space bar."

With further investigation, a JAWS user can find readable text regarding the site's certificate by clicking through the report's *View Certificates* link, selecting the new window's *Certification Path* tab, and finally reading, "Certificate is OK," letter by letter with the left and right arrow keys (shown in Figure 3.5). We found this information through a trial and error process outlined in Figure 3.6. When exploring IE's security report for relevant SSL information, we found that only some information was accessible through JAWS (the blue boxes). The system also triggered automatic transitions through the window's options (the arrows) but these triggered options most usually led to dead ends or text that was not compatible with the screen reading software (white boxes).

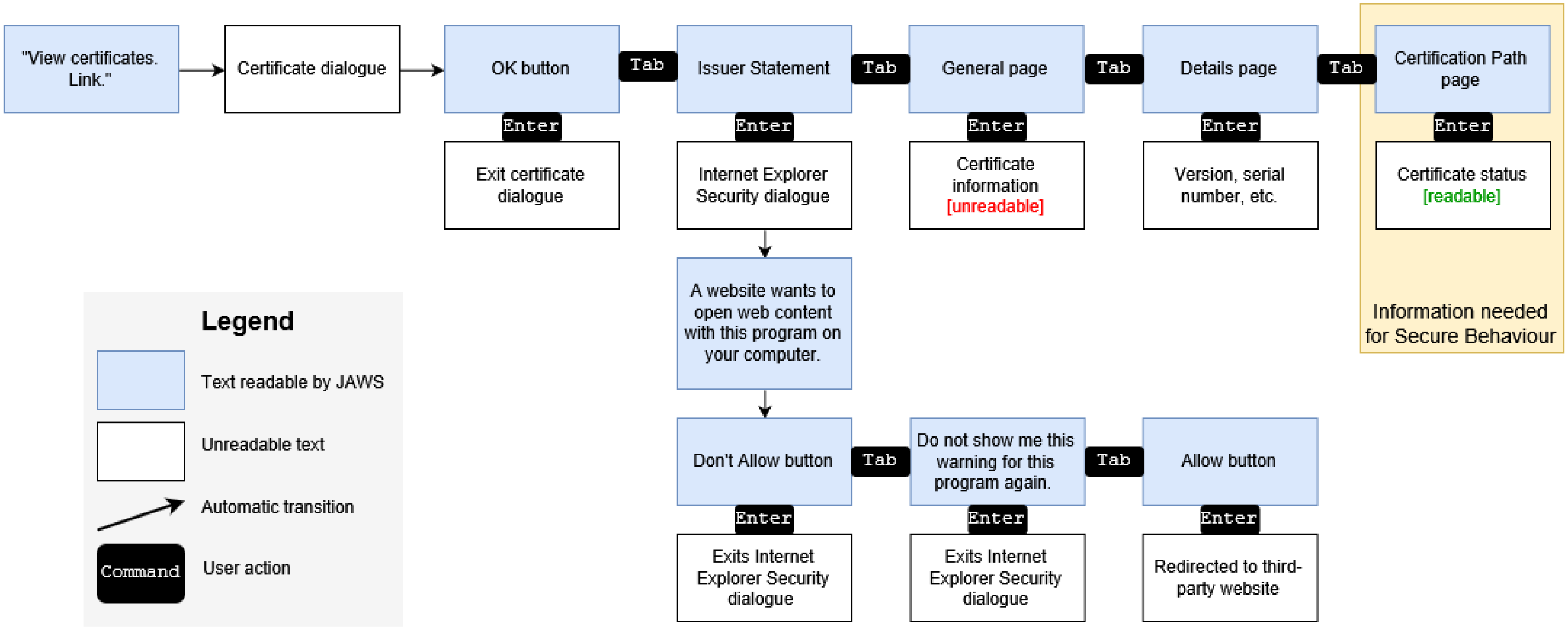

"View certificates. Link."
Certificate dialogue
OK button
Tab
Enter
Exit certificate dialogue
Issuer Statement
Tab
Enter
Internet Explorer Security dialogue
A website wants to open web content with this program on your computer.
General page
Tab
Enter
Certificate information [unreadable]
Details page
Tab
Enter
Version, serial number, etc.
Certification Path page
Enter
Certificate status [readable]
Information needed for Secure Behaviour
Don't Allow button
Tab
Enter
Exits Internet Explorer Security dialogue
Do not show me this warning for this program again.
Tab
Enter
Exits Internet Explorer Security dialogue
Allow button
Enter
Redirected to third-party website
Legend
Text readable by JAWS
Unreadable text
Automatic transition
Command
User action

Figure 3.6: Finding SSL certificate information with JAWS.

3.4.2 Logging into Sites (Task 2)

As illustrated in Vigo and Harper's study [103] on screen reader browsing strategies, users are presented miscellaneous links, headers, and navigation bars before the main content of a page. Users can listen to each section or skip to relevant content. However, communicating change in the main content upon refresh or redirect with JAWS is not as direct as a visual scan since users must first be aware that a change may have occurred, then they must find and listen to changes to notice the update.

During our evaluation, a successful login usually redirected the user to a new page containing personal account information which JAWS would automatically begin reading. The page change was visibly explicit but, for the majority of websites, there was no audible feedback to demonstrate that the credentials were correct and that the user was being directed to a new page. One exception was Gmail, which offered a short high-pitched tone upon successful login. Although this site offered better login feedback than the others, this sound did not explicitly state that the password was correct, nor that the account had been accessed.

Unsuccessful login attempts were also problematic. Typically, the same page would refresh and present an error message visually cuing the user to try again. However, the page refresh was not automatically announced. Instead, JAWS would wrap to the top of the page and begin to reread its contents without explicit explanation. Furthermore, the error messages pertaining to incorrect credentials were not announced unless selected while the user skimmed through the page manually, or were eventually read aloud if the user allowed JAWS to automatically read the page until it passed through the login section. Since there is minimal audible feedback during the login process, users are forced to follow a trial-and-error process of skimming through page content to establish progress towards their goal.

3.4.3 Completing a Site-Specific Transaction (Task 3)

The transactional tasks we attempted could only be successfully completed on 4 of the 10 tested pages. Most tasks were inhibited by accessibility issues such as insufficient alternative text for vital visual cues and limited JAWS compatibility with page modules. These issues prolonged evaluations beyond the established time and trial limits and thus restricted our exploration of completing transactional tasks on the explored pages. These accessibility obstacles would likely also impede non-sighted users' ability to achieve site-specific tasks and abide by security advice.

We uncovered several issues restricting effective use of site information and therefore ability to explore sites carefully. Most concerning, IE presents a pop-up at the bottom of the screen upon initiating a download. This pop-up provides information regarding the site host and the file being offered; the dialogue allows a user to review and confirm the download. However, in some cases, the document host's URL was inconsistent with the main page's URL. For example, a document from "https://mail.google.com" was being hosted by "mail-attachment.googleusercontent.com." This is because in some cases not all site content is hosted on one server/domain. However, the reason for discrepancy between URLs is not provided to the user who has to make a decision about the legitimacy of the file. This may be a severe issue for all users, sighted or not. However, visually impaired users have limited access to other cues that sighted users may rely on to assess the circumstances.

3.4.4 Security Implications

Similar to Buzzi et al.'s [21] assessment of eBay via JAWS, the websites we evaluated did not provide clear information regarding the methods of securing personal information nor elicited a strong sense of control over the interface due to the severe functionality issues between JAWS, the browser, and website features. These issues greatly impede a user from following common security advice while browsing online.

Firstly, security advice often urge users to check SSL certificates to protect against threats such as man-in-the-middle (MITM) attacks [86]. Information about a certificate's validity and the entity establishing the secure connection can also help a user identify potential phishing sites.

During the evaluation, IE did not allow JAWS to read textual information pertaining to the certificate. Since most users tend to be more task-focused than security conscious [48], it is also likely users will exit the security dialogue when cued rather than explore the window to discover the single readable sentence regarding the state of the certificate. Thus, visually impaired users are currently limited in their ability to follow advice pertaining to certificates and may, therefore, be more vulnerable to exposing sensitive information than their sighted counterparts when using Internet Explorer and JAWS.

We also discovered that screen reader users attempting to login to personal accounts are provided insufficient cues to signal that access to their personal information has been granted, and that they are being rerouted to new pages containing such information. This is particularly concerning because they are unable to identify if and when protected information is being visibly shown. Furthermore, the state of their account is usually not explicit. This lack of sufficient feedback reduces the site's usability and could increase their vulnerability to visual eavesdropping (shoulder surfing) and thus nullify commonly suggested precautionary actions like using strong passwords and storing credentials in password managers [86].

Thirdly, security advice also recommends that users be generally thoughtful when clicking on unfamiliar URLs or downloading attachments that may put them at risk. The evident inconsistency between main page URLs and document host URLs can endanger both sighted and non-sighted users. Against either user's better judgement, file host URLs that do not include established trust indicators (HTTPS, or a familiar domain name) must be accepted to progress towards a task. This renders anti-phishing advice regarding parsing URLs or being critical while interacting with websites moot.

Ultimately, the websites that are incompatible with screen readers restrict non-sighted users' ability to analyze information and make informed, secure decisions. Websites with misleading information such as convoluted URLs or authorized sites without evident trust indicators (HTTPS, SSL certificates, or a familiar domain name) can interfere with both sighted and non-sighted users' ability to carefully complete transactional tasks. Yet, these usability issues can more severely impact non-sighted users if they are reliant on audible outputs describing relevant security indicators and are limited in assessing other page characteristics that may aid sighted users in securing their information.

3.4.5 Interpreting and Combining Our Results

Our interpretation of the automated checkers' results is relatively straightforward; the greater number of Level AA issues identified, the less likely the website is sufficiently accessible. Yet, due to the variability of our expert evaluation, we must approach the results of our other assessment more subjectively. To interpret our expert evaluation results, we assessed the websites' sufficiency based on the number of tasks that could be completed, and the number catastrophic (rated 4 out 4) issues found on each website.

ID	Title	Automated Assessment	Expert Evaluation	
		Level AA Issues (Mean)	**Total Task Fails**	**Number of Catastrophic Issues**
W1	Canada Post	8	3	58
W2	ServiceOntario	2.5	1	24
W3	eCampusOntario	11.5	2	10
W4	TD EasyWeb	2	1	21
W5	Carleton Grad Studies	3	2	25
W6	Hydro Ottawa	4	2	25
W7	Gmail	3	1	27
W8	Presto	10.5	1	9
W9	ViaRail	8	3	39
W10	Facebook	3	2	21

Table 3.7: Comparing the results of our automated assessment and expert evaluation. Green cells represent most accessible websites per evaluation and red cells represent least accessible websites per evaluation.

We combine our results to better understand the 10 websites' potential for providing visually impaired users sufficient means to behave securely online. Based on our interpretation, we highlight the "most sufficient" two sites in green and the two "least sufficient" sites in red for each assessment in Table 3.7.

The synthesis of our results demonstrates some inconsistent findings. According to the automated checkers: ServiceOntario (W2) and TD EasyWeb (W4) were most accessible, and eCampusOntario (W3) and Presto (W8) were the least accessible. Yet, per our expert evaluation: TD EasyWeb (W4) and Presto (W8) performed the best, and Canada Post (W1) and ViaRail (W9) were the worst. Since the automated checker is focused on technical WCAG violations and cannot gauge contextual usability issues like the expert evaluation, these inconsistencies are not surprising.

Yet, these findings suggest two main disadvantages of relying solely on WCAG compliance to ensure visually impaired users can behave securely online. Firstly, automated tests can overestimate the implication of WCAG violations on usability issues that users face on a site. For example, the Presto website had an average of 10.5 WCAG violations but, during our expert evaluation, we were able to successfully login and reload a transit pass with few catastrophic issues pertaining to our security and privacy. Secondly, the automated tests can also underestimate the usability obstacles users may face that are not necessarily outlined in the WCAG. Specfically, we found less than a dozen WCAG violations when checking the ViaRail website yet, we could not complete any of the assigned tasks and faced 39 catastrophic issues while conducting our expert evaluation. Thirdly, many severe security issues were associated with the browser and operating system. For example, IE's SSL dialogue window was incompatible with JAWS. Therefore, automated checkers are insufficient when identifying some major usability issues.

Other researchers have argued that solely relying on the WCAG is not enough to develop truly accessible technology [13, 17, 104], and per our results, the popular guidelines alone may be ineffective to assess the accessibility and usability of security information. Therefore, guidelines like the ACCUS heuristics that integrate best practices between accessibility and usable security may better identify potential usability and accessibility issues than automated accessibility checkers. We strongly suggest future research to continue to improve and validate our proposed heuristics in order to accommodate the shortcomings of the WCAG and automated checkers.

3.5 Next Steps

The effectiveness and confidence of expert evaluations can vary based on the researchers' expertise [36]. Nonetheless, expert evaluations are common to usable security domain [108] and are especially valued in the accessibility domain since they possess more stable rates of reproducibility than evaluations conducted by non-experts and are also more likely to identify "true barriers" [113].

However, the unique mental models of visually impaired web users cannot be inferred by sighted evaluators. Our understanding of visually impaired users' abilities to maintain their online security, and the effectiveness of the ACCUS heuristics, can be enriched through observational and feedback methodologies that we use in the next chapter's user study.

Chapter 4

User Study

4.1 Introduction

We aim to validate the usability concerns revealed in the expert evaluation through empirical data collected through a user study. We also aim to identify issues pertinent to visually impaired web users that may not have been identified in our expert evaluation. The user study's findings will inform us of visually impaired users' mental models of web security mechanisms, and the advantages and limitations of using screen readers or screen magnifiers to surf the web safely.

4.2 Method

We describe all study tools, websites, tasks, and data collection methods in detail below. In brief, we collected insight from 14 visually impaired participants' online security and privacy concerns through observation and feedback during 90-minute one-on-one sessions with the lead researcher.

The sessions included three segments: 1) the pre-test, participants offered oral informed consent and demographic information; 2) the task scenarios, participants engaged in three security tasks on one of three randomly assigned websites; and, 3) the post-test, participants engaged in a discussion regarding their online security and privacy concerns.

Eligible participants were from the Ottawa or Toronto area, at least 18-years old, and must have had some degree of visual impairment. In appreciation for their time, the participants were given 50 dollars and their study-related travel expenses were compensated. Our methods were approved by the university's Research Ethics Board and cleared by Canadian National Institute for the Blind's (CNIB) Research Department.

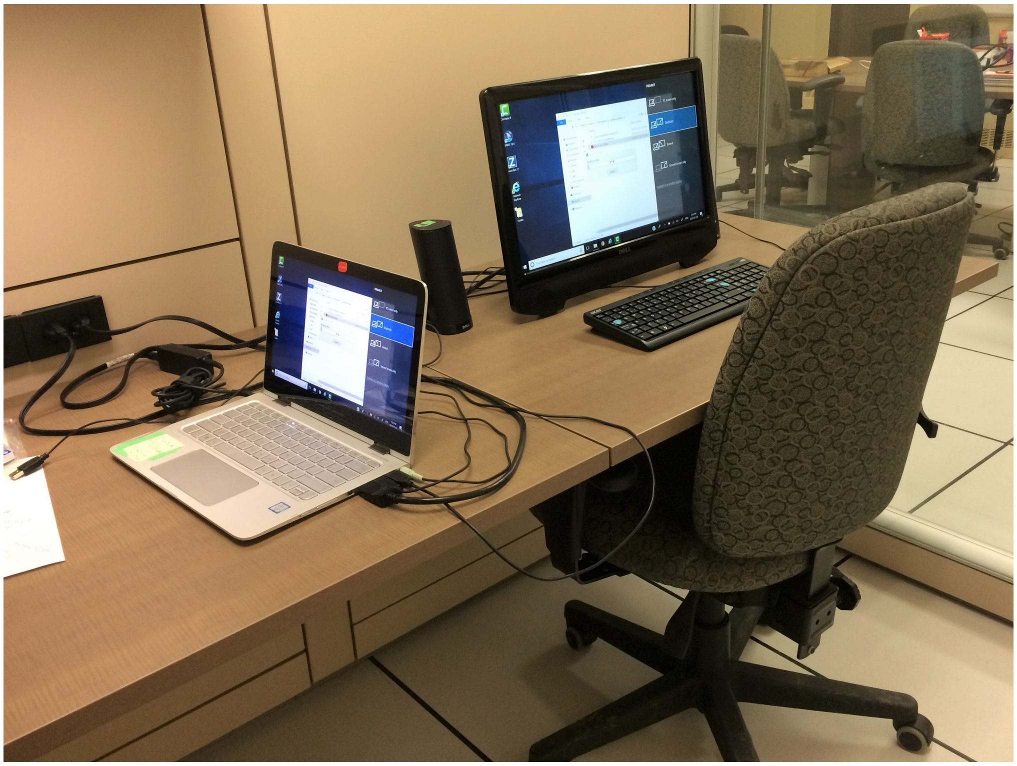


Figure 4.1: An example of the set-up used during the user study sessions.

4.2.1 Devices and Software

The sessions took place in three different locations: Carleton's Human Oriented Research in Usable Security (CHORUS) laboratory (Figure 4.1), a conference room at the Canadian Council of the Blind (CCB) in Ottawa, and an office at the Canadian National Institute for the Blind (CNIB) in Toronto. All study spaces were closed off to minimize interference from others outside the study and help participants focus on the study's tasks and conversations.

The study's main apparatuses varied according to each participant's personal needs and preferences. Six of the 14 participants used a Windows 10 computer, a standard keyboard (K) with tactile markers to enhance important keys, and JAWS 18 screen reading software to complete the study. Of these six participants, one person relied on a mouse (M) and display monitor (D) to gauge and select shapes shown on screen.

Table 4.1 describes the devices, operating systems, and assistive software used by each participant. We also note any customized settings they used. In brief, the seven blind participants used a Windows computer, keyboard, mouse, and screen reading software including JAWS 18 or iOS VoiceOver. The seven partially sighted participants used a similar set-up with a monitor and screen magnifying software, ZoomText 11. Thirteen of the 14 participants used Internet Explorer 11 (IE) or Safari to browse the websites.

Two of 14 participants, both partially sighted, did not use assistive software during the study. One participant, U09, used an iPad running iOS 11 to complete the tasks but did not enable VoiceOver. Instead, she relied on the pinch-in zoom feature to enlarge their view of the test site. The other participant, U12, used the Windows set-up with a keyboard, mouse, monitor but relied on Google Chrome 65 with a dark theme, high-contrast plug-ins, and an enlarged cursor to accommodate his visual impairment.

All participants reported that they could comfortably complete the tasks with the provided set-up. In three cases, participants reported that they would typically use a different device (smartphone), assistive application (NVDA open-source screen reader), or keyboard without tactile markers to similar tasks outside of the study but the provided tools did not impede their performance. In this project, we do not investigate the issues pertaining to these other devices and software, however future work should aim to assess the problems that exist when browsing with these tools.

Additionally, during the study, all devices and software were set to their default settings. Participants were encouraged to customize these settings to reflect their normal set-up outside of the study, as needed. In most cases, any change to default settings were limited to ZoomText's settings as partially sighted individuals toggled through the contrast and zoom levels depending on what they were reading or doing during the tasks.

ID	Sight	Operating System	Accessories	Assistive Software	Settings	Browser
U01	None	Windows	K	JAWS	Default	IE
U02	Partial	Windows	K, M, D, glasses	ZoomText	Voice reader	IE
U03	Low-None	Windows	K, M, D	JAWS	Default	IE
U04	None	iOS	None	VoiceOver	Default	Safari
U05	None	Windows	K	JAWS	Default	IE
U06	Partial	Windows	K, M, D	ZoomText	High-contrast, voice reader	IE
U07	None	Windows	K	JAWS	Default	IE
U08	Partial	Windows	K, M, D, hand-held magnifying glass	ZoomText	Default	IE
U09	Partial	iOS	Book stand	None	Default	Safari
U10	None	Windows	K	JAWS	Default	IE
U11	Partial	Windows	K, M, D	ZoomText	Default	IE
U12	Partial	Windows	K, M, D, glasses	None	High-contrast, cursor enlarge	Chrome
U13	Partial	Windows	K, M, D	ZoomText	Default	IE
U14	None	Windows	K	JAWS	Default	IE

Table 4.1: Devices and software used during user study sessions, per participant. Accessories column represents the technology used during the session where: “K” stands for a keyboard with tactile markers, “M” stands for standard computer mouse, and “D” stands for display monitor.

4.2.2 Websites

Participants interacted with one of three websites: Amazon.ca, Gmail.com, and a spoofed version of CNIB.ca (CCNIB.ca). These websites were chosen because they each elicit opportunities for exposure to security vulnerabilities. Firstly, Amazon requires users to share their full name, home address, and credit card information to fully engage in its eCommerce services. Secondly, many users rely on Google email to communicate and store sensitive information. Gmail accounts are also automatically linked, and therefore permit access to other related services like Google Drive and Google Calendars that may also contain personal information. Thirdly, although the CNIB webpage is intended as an informational resource for visually impaired clients who want to learn more about the organization's services, the CNIB Shop and Donation pages requires users to disclose personal data and credit card information also required for eCommerce services.

To explore any differences in users' behaviours when working with illegitimate sites, we used the official Amazon and Gmail websites, but created an imitation of the CNIB website (here on referred to as CCNIB). We used free software called HTTrack to download and save the site to our local directory. The files were stored, linked, and hosted on the CHORUS research laboratory's server. This allowed us to ensure that no participant information was collected on the imitation site, and any transactions could not be processed. We purchased the following domain to link to our version of the site: http://www.ccnib.ca. Our version was not encrypted by a secure sockets layer (SSL) connection. The CCNIB site was live during the three weeks of testing, taken down after testing, and the URL address does not currently lead anywhere.

We assigned participants to one of three websites in alternating order but assigned tasks, described below, in consistent order for each website. If time permitted, participants were asked to repeat all three tasks on a second website. We input the URL addresses for the test websites on behalf of the participants to mitigate any potential usability issues that could occur in directing to websites. Before beginning the tasks, we did not tell the participant what site they would be working with, nor whether it was legitimate. During the study, four out of the 14 participants had time to complete the tasks on two websites rather than one therefore, six participants interacted with each of the three websites.

4.2.3 Task Scenarios

To ensure participants' security and privacy, we created Amazon and Google accounts specifically for the study and purchased a prepaid credit card. With these credentials, participants were able to complete transactions, such as logging in and completing purchases, without disclosing their personal information.

During the study, we dictated the user names, passwords, and credit card information character by character to all participants regardless of their visual ability. All accounts were clearly associated with the lead researcher. For example, the Amazon's username was "danielanapoli@cmail.carleton.ca" and the credit card holder's name was "Daniela Napoli." However, we did not explicitly claim the authenticity of the credentials nor advised participants to handle the information with particular care (Appendix B.1). We avoided emphasizing security or privacy before and during tasks to mitigate bias on user's typical behaviours while interacting with the websites.

For the user study, participants performed similar tasks completed during the expert evaluation including: 1) verify if the site is legitimate, 2) login if it safe to do so, and 3) complete a transaction. The second and third task somewhat varied depending on the site, but we aimed for a similar level of difficulty across websites. We describe each task variation in Table 4.2.

In brief, The task for the Amazon website was to access a prepared cart and finalize the purchasing process by inputting the lead researcher's billing and mailing information. With Gmail, we asked participants to download and attachment emailed to the account. The CNIB website did not require login credentials so we asked participants to find the donation page and make a ten dollar donation on behalf of the lead researcher with the provided credit card.

After completing each task, participants rated the task's difficulty on a scale of 1 (very difficult) to 5 (very easy), and their level of confidence in completing the task correctly on a scale of 1 (very unsure) to 5 (very sure). Additionally, after the third task, participants rated the website's accessibility on a scale of 1 (very inaccessible)

URL	Task 1	Task 2	Task 3
https://www.amazon.ca	Verify legitimacy	Login	Complete purchase
https://mail.google.com	Verify legitimacy	Login	Download attachment
http://www.ccnib.ca	Verify legitimacy	Find donation page	Make $10 donation

Table 4.2: The websites and tasks completed during user study sessions.

to 5 (very accessible) and security from 1 (very insecure) to 5 (very secure).

4.2.4 Data Collection

All questionnaires used during the session were hosted on Qualtrics and are listed in Appendix D. We delivered questionnaires orally and recorded responses on behalf of the participants to avoid accessibility issues with JAWS and ZoomText discovered while piloting the study. Each session was audio recorded, and screen interactions were recorded with Camtasia for note-taking purposes.

Pre-test Questionnaires

The pre-test questionnaires were used to collect basic information about participants and their online habits. The depth of information gathered about our user group was inspired by Ahmed et al.'s [3] 2015 study on visually impaired users' privacy concerns and behaviours. Similar to their study, we asked for participants' age, gender, education, and occupation. We also asked participants to describe their sight limitations because the term "visually impaired" is broad and includes a range of varying visual disabilities including partial to no sight in one or both eyes. This information is vital to understanding the spectrum of each person's capabilities in working with screens and other accessories like keyboards and mice. Lastly, we asked participants to describe the online services they typically engage in and what technology they most frequently use to participate in these services.

During Tasks

Participants were encouraged to think-aloud and explain the rationale for their actions and methods in achieving goals (including short-cuts or gestures). This information allowed us to gain insight to their mental models of the site's security mechanisms and any related usability issues. We probed participants with open-ended questions, such as "What happened?" or "What do you think you should do?" if their actions were inexplicit or if they asked for guidance while completing a task. We asked participants to rate: 1) the task's difficulty, 2) their confidence in completing the task, 3) their perception of the site's general accessibility, and 4) their perception of the site's general security on 5-point semantic scale questions.

Post-test Questionnaires

After completing the tasks, we asked participants to describe any discrepancy between their usual habits and the actions they took during the session. For the most part, participants said they completed each task as they normally would. They said that the issues encountered were typical to their previous experiences. We asked participants to rate their level of concern for several specific cybersecurity issues on a 5-point scale of not at all concerned (1) to very concerned (5). The list consists of concerns mentioned by other visually impaired web users from a recent related study [56]. These were presented to the participants in random order to mitigate ordering effects:

T1 Someone stealing your identity

T2 Someone gaining access to your financial information

T3 Someone stealing private information about you/your family

T4 Your personal information being made public online

T5 Falling victim to an online scam or fraud

T6 Someone tracking your online activities

T7 Someone hacking into your email

T8 You unintentionally installing malicious software

T9 Your device becoming infected with a virus or malware

T10 Your device becoming infected with key-stroke logging software

T11 Someone eavesdropping (offline) on you

T12 Someone watching your interactions (offline) without you knowing

Similar to Kang et al.'s 2015 [63] study, we asked participants to rate: 1) the perceived effectiveness, and 2) the likelihood they would adhere to a set of protective actions. The following actions were among the most commonly made suggestions from surveys of security expert advice [58, 86]. Again, to mitigate ordering effects, the actions were delivered randomly to each participant:

PA1 Frequently update software and systems

PA2 Enable automatic updates

PA3 Use software from official, trusted sources

PA4 Use antivirus software

PA5 Use strong passwords

PA6 Use unique password between different sites

PA7 Use multi-factor authentication methods

PA8 Use a password manager

PA9 Only use websites that include "HTTPS" in the URL address

PA10 Think before clicking on a link

PA11 Do not open unexpected attachments

Post-Test Interview

During the post-test interview, we asked participants open-ended questions regarding their most pressing concerns, their methods of protecting themselves online, their most frustrating obstacles, and other questions to further supplement the security habits they reported in earlier questionnaires. After the interview, we debriefed the participants that used the spoofed website.

4.3 Results

We downloaded the documented responses from Qualtrics and tallied responses from semantic scale responses. Our analysis focused on the most common responses. As we will elaborate on later, we used a thematic coding approach [18] to analyze recorded participants' comments and researcher's notes. This analysis was completed by the lead researcher and may therefore possess bias towards their single interpretation. Future research may benefit from including multiple coders if inter-coder reliability is maintained.

In sum, 12 out of 14 participants were able to attempt all of the assigned tasks until they believed they had successfully completed the task. The remaining two faced critical accessibility issues when attempting Task 3 (complete purchase) on the Amazon site. Many participants faced issues in inputting passwords on Amazon and Gmail, but all were able to eventually log in during Task 2. No participants identified the CCNIB website as illegitimate during Task 1, meaning that they completed all of the assigned tasks on a "phishing" website.

Their exhibited behaviours were not usually aligned with common security advice. When asked, participants believed the sample of protective actions were effective, but reported that they were unlikely to adhere to this advice. Generally, participants' expressed passive and trusting attitudes towards to their online security and privacy.

4.3.1 Participants

Our outreach for this user study heavily relied on community partners including the CNIB and CCB. After two months of active in-person, snowballing, and email recruitment processes, we secured 14 participants. This is consistent with the smaller, 10 to 15 participants, sample sizes noted in related accessibility literature exploring visually impaired users' perceptions [2, 5].

We considered a sample of this size could sufficiently provide an initial basis for understanding visually impaired users' online security concerns and attitudes and see whether their concerns aligned with the issues uncovered by ACCUS in our expert evaluation. Due to the small sample size, we did not conduct statistical analyses on our results. We describe and compare all of our following results based on observations of questionnaire results rather than statistical significances. Future studies with a larger sample size will allow researchers to validate and supplement our results.

Demographics

Table 4.3 details the participants' demographics. The mean age for the group of 14 participants, six females and eight males, was 50.9 years (SD=15). The majority of our participants are older than those included in common usability studies, but our sample reflects a similar age group noted in related accessibility studies [39, 87, 99]. Furthermore, all participants reported that they were familiar and comfortable completing the assigned tasks on the provided devices. Our observations confirm their technological capabilities were sufficient for the study.

Most participants (n=9) had earned an undergraduate degree, college degree, or higher. Majors included: Human Rights Law, Psychology, Theology, Music Therapy, Computer Science, and Business Administration and Management. Eight participants were categorized as unemployed which included retired individuals, full-time volunteers, those on long-term disability, and active job seekers.

Eight participants were very limited in their visual acuity, or ability to see objects and people. Seven participants had a very limited field of vision. Additionally, eight participants were somewhat limited in their abilities to perceive light. Most participants' affected eye(s) could only gauge drastic changes of light within a room or outdoors. Yet, in one case, a blind individual with some light perception was able to identify page changes and content placement on the tested websites. In brief, six participants were legally blind, and eight participants were partially sighted with some degree vision in one or both eyes.

In addition to a visual impairment, one participant (U06) had a speech impediment and another participant disclosed they had ADHD (U02). No others claimed any associated disabilities.

ID	Sex	Age	Highest Degree	Occupation	Visual acuity limit	FOV limit	Light perception limit
U01	Female	20	High school	Student	Very limited	Very limited	Very limited
U02	Female	55	Under-graduate	Actively seeking	Somewhat	Somewhat	Somewhat
U03	Male	26	High school	Student	Very limited	Somewhat	Not at all
U04	Male	63	Under-graduate	Retired, volunteer	Very limited	Very limited	Very limited
U05	Female	51	Under-graduate	Technology Program Coordinator	Very limited	Somewhat	Somewhat
U06	Female	54	High school	Volunteer	Somewhat	Very limited	Somewhat
U07	Male	51	College	Contractor	Very limited	Very limited	Somewhat
U08	Male	41	Under-graduate	Unemployed	Somewhat	Somewhat	Somewhat
U09	Female	68	High school	Small business owner	Somewhat	Not at all	Somewhat
U10	Male	68	Under-graduate	Retired	Very limited	Very limited	Very limited
U11	Female	70	College	Retired	Somewhat	Not at all	Not at all
U12	Male	51	Masters	Volunteer	Very limited	Very limited	Somewhat
U13	Male	40	High school	Unemployed	Somewhat	Not at all	Somewhat
U14	Male	55	Under-graduate	Customer service	Very limited	Very limited	Very limited

Table 4.3: Demographics of user study participants.

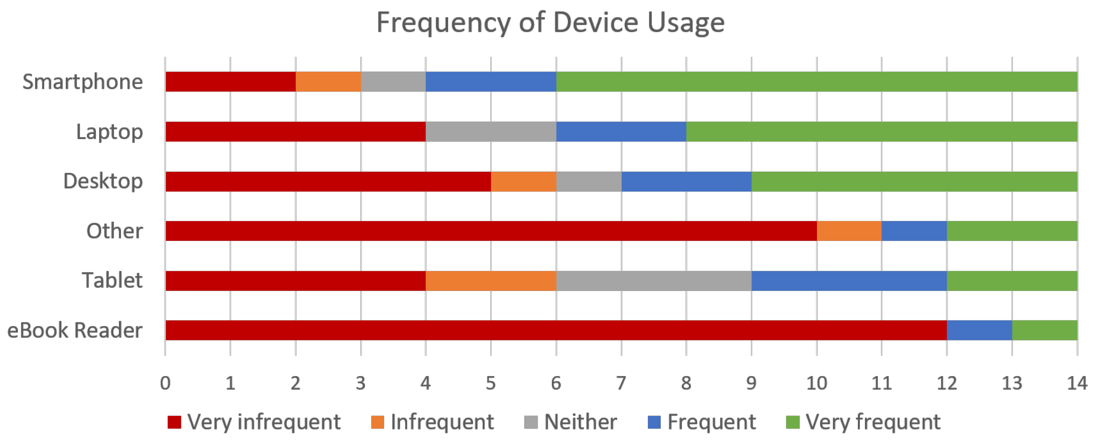


Figure 4.2: Trends in participant device usage, sorted by most frequently used to least frequently used device.

Device Usage Trends

Participants rated the frequency in which they used particular devices for online browsing on a scale of 1 (very infrequently) to 5 (very frequently). Verbal questionnaire responses "never" or "almost never" were considered "very infrequently." All responses are summarized in Figure 4.2.

Ten participants reported that they use their smartphone to surf the web frequently (n=2) or very frequently (n=8). Six of these participants use an iPhone running iOS 11, and four of the mobile users have a device running a recent version of Android.

Eight participants said they use a laptop to surf the web frequently (n=2) or very frequently (n=6). Similarly, seven participants said they use a desktop computer frequently (n=2) or very frequently (n=5). Through conversation, it seemed that the key difference between laptop and desktop users was the need for an external monitor, keyboard and/or mouse. Many participants noted that these aspects of laptop computers were too small or difficult to use comfortably. In either circumstance, 10 participants reported that they use Windows 10, two participants use Windows 7, and one uses Windows 8.

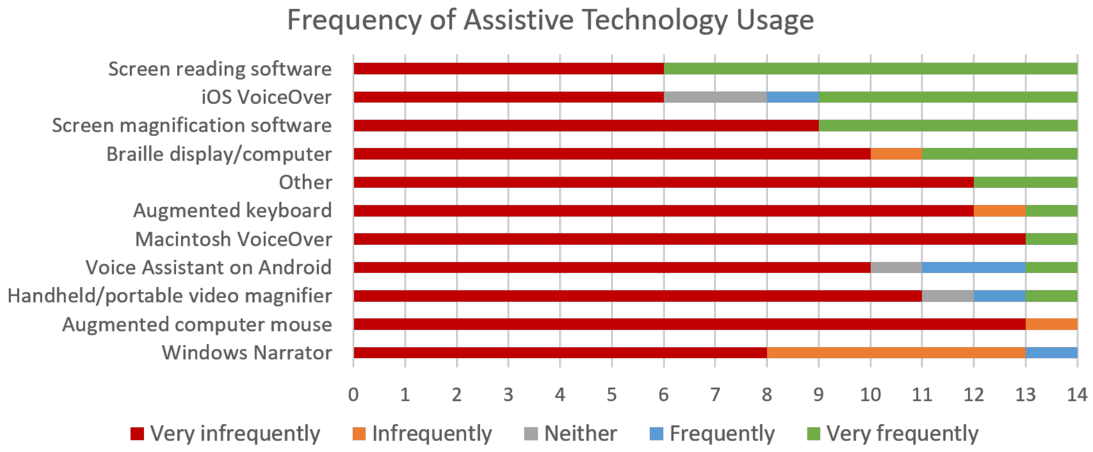


Figure 4.3: Trends in assistive technology usage, sorted by most frequently used to least frequently used technology.

Figure 4.3 summarizes participants' use of assistive technologies. To supplement their device set-ups, most blind participants use screen reading software to surf the web. Eight participants reported that they use JAWS and NVDA very frequently. Six participants reported that they use iOS VoiceOver, the built-in iPhone screen reader. Participants reported that they do not frequently use other screen reader software such MacOS VoiceOver, Windows Narrator, and Android Voice Assistant. Five participants with partial vision used screen reading software such as ZoomText very frequently. The majority of other assistive computer accessories, such as an augmented computer keyboard or mouse and braille display, were not used frequently.

Web Usage Trends

Figure 4.4 summarizes how frequently participants engage in common online services. The most frequently used services were related to banking, shopping, library or information resources, and social media. Many participants said they used designated devices to engage in particular online services. For the most part, our test set-ups seemed to appropriately accommodate our participants' habits as eleven participants reported that they often bank online equally on their computer or smartphone and

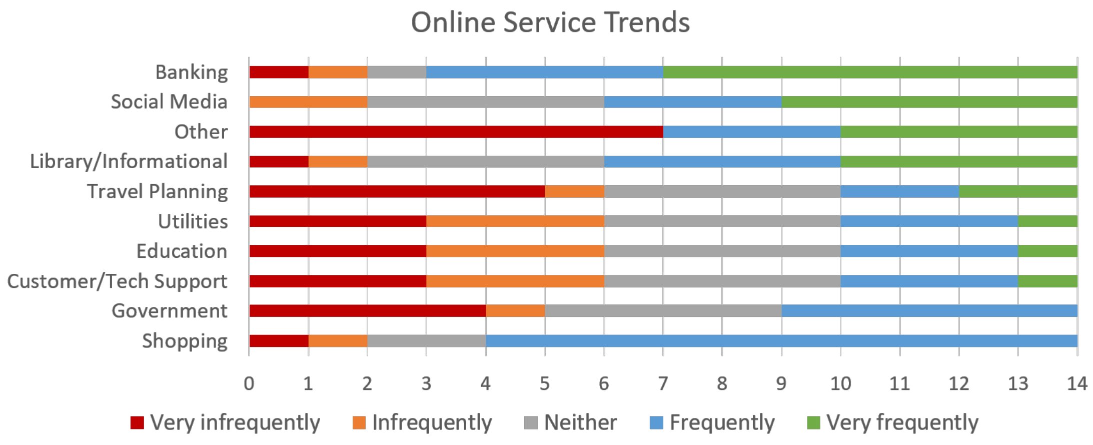


Figure 4.4: Trends in online service usage, sorted by most frequently used to least frequently used service.

access online shops moreso with their computers than with their smartphones.

The least frequently used online services were related to: travel planning, checking basic utilities such as hydro or internet bills, distance education, and customer or technical support. Most participants said they prefer to engage in these services offline and in-person or on the phone.

Figure 4.5 summarizes browser usage. Participants reported that they most frequently use Chrome, Internet Explorer and Safari. Edge, Windows newest iteration of Internet Explorer, was the least used browsers. Many participants were unaware of Edge's existence, and some avoided the browser due to incompatibility with their assistive software.

4.3.2 Tasks

As mentioned, all but two study participants were able to attempt all assigned tasks. Those two, both blind, who were unable to diagnose nor recover from vital errors that were visibly shown (in embolden text or symbols) but not audibly described while completing a purchase (Task 3) on the Amazon website.

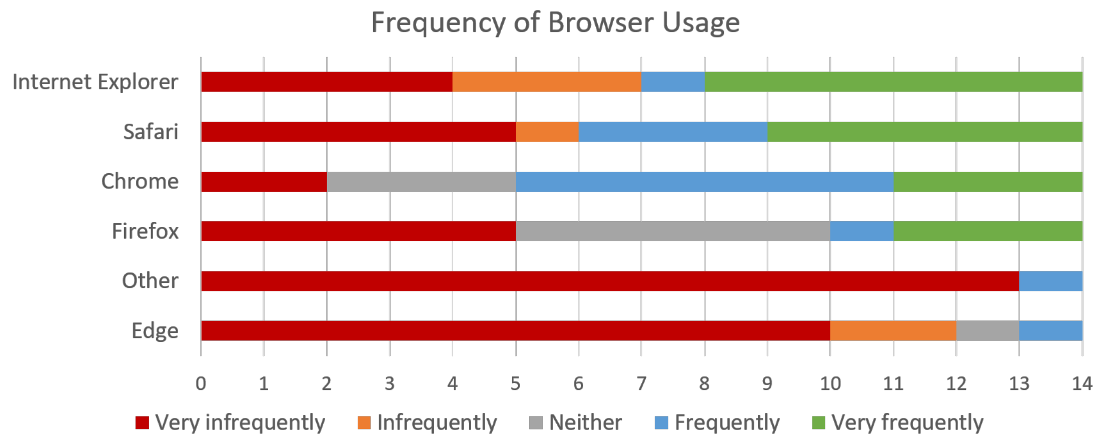


Figure 4.5: Trends in browser usage, sorted by most frequently used to least frequently used browser.

In general, participants found Task 1, verifying the site's legitimacy, (M=4.0, SD=1.0) and Task 2, logging into the site, nearly equally easy (M=4.1, SD=1.1). Task 3, complete a site-specific transaction, posed opportunity to observe challenges but was not generally viewed as difficult (M=3.6, SD=1.2) by participants.

Although we observed accessibility and usability issues that could impede their security and privacy, most participants rated the websites accessible (M=4.0, SD=1.3) and secure (M=4.0, SD=1.2). Figure 4.6 summarizes their responses; there are 18 total responses because four participants completed tasks on two sites.

Task 1: Verify legitimacy

All participants attempted Task 1, verify the website's legitimacy, until they explicitly said they finished the task. For the scope of this project, if a participant claimed a site to be legitimate/illegitimate, and it was, we considered them to complete the task "correctly."

Per our results, the six participants working with Amazon all correctly identified the site as legitimate. Five out of six participants correctly assessed Gmail as legitimate. Zero out of six participants correctly assessed the CCNIB site as illegitimate.

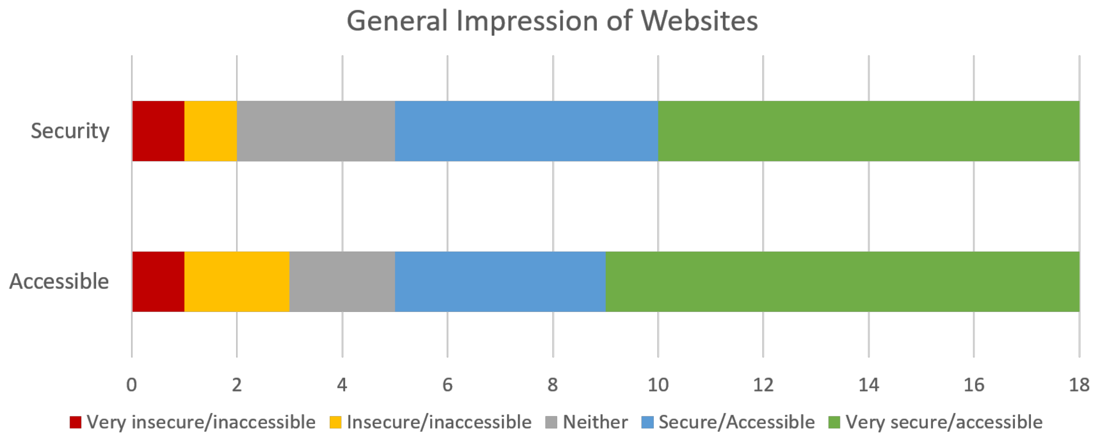


Figure 4.6: Participant ratings of website accessibility and security.

However, this assessment is limited in understanding if participants approached this task in a secure manner. Future analysis which explores the reliability of the indicators participants relied upon will allow us to better assess participants' approaches to verifying website legitimacy.

Figure 4.7 summarizes how difficult participants found Task 1. Figure 4.8 summarizes participants' reported confidence in their performance during Task 1.

Generally, participants found the task easy and were confident in their performance. In particular, participants seemed to find verifying the legitimacy of the CCNIB website the easiest (M=4.3, SD=0.8) out of all sites. Additionally, all six participants reported that they were very sure (M=5, SD=0.0) of their assessment of the CCNIB website.

This is especially worrisome because they suggest that participants believed they were easily and correctly identifying a legitimate website when they were not. As we will discuss later, our qualitative findings in participants' attitudes and behaviours in assessing a website's legitimacy suggest that participants trusted the CNIB organization and therefore were inclined to trust the CCNIB website with little or no scrutiny.

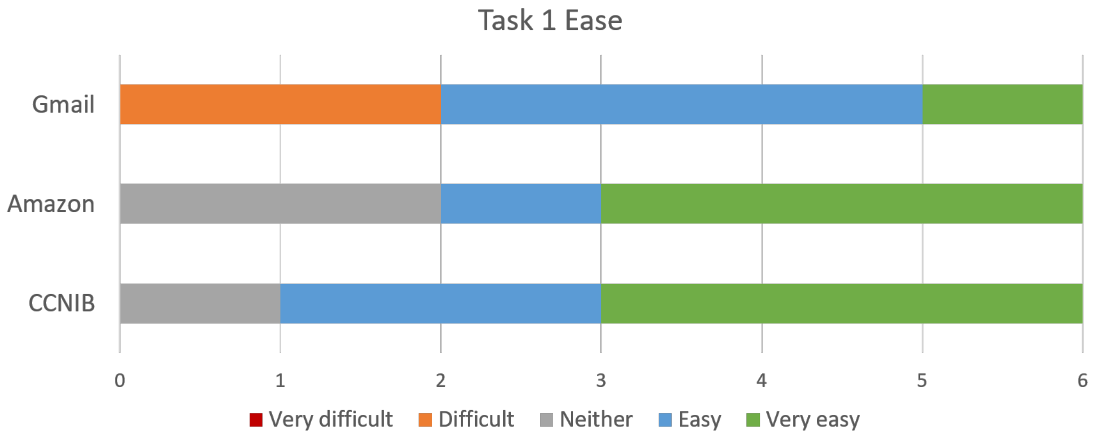


Figure 4.7: Difficulty of verifying legitimacy of sites (Task 1).

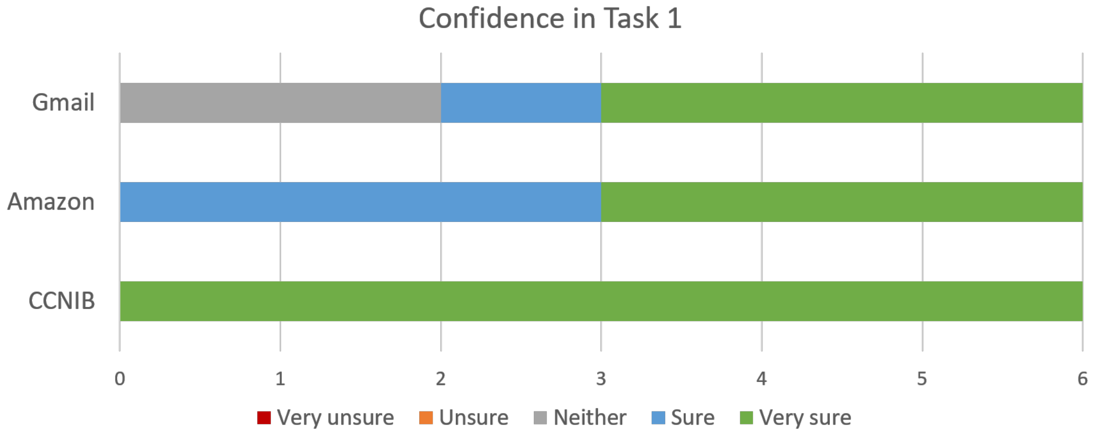


Figure 4.8: Confidence in verifying legitimacy of sites (Task 1).

Task 2: Login (or find donation page)

All participants successfully completed Task 2, login to Amazon or Gmail, or find the donation page on the CCNIB website.

Figure 4.9 summarizes how difficult participants found Task 2. Figure 4.10 summarizes participants' reported confidence in their performance during Task 2.

Task 2 was generally rated as easy despite a few participants' difficulties in logging into Amazon and Gmail. Between the task variations, finding the donation page on the CCNIB website may have been easier (M=4.3, SD=1.2) than logging into Gmail (M=4.0, SD=0.6) or Amazon (M=3.8, SD=1.5). Regardless of the task's variation, participants seemed similarly confident in their performance on all sites during Task 2.

Participants found logging into Gmail easier than logging into the Amazon websites. This may be due to differences between the sites' interfaces. Specifically, the Gmail homepage has minimal content and users are automatically placed in the login form fields. On the Amazon homepage, users must skim through the page's content to locate the login link and then find the form fields after redirecting to the appropriate page.

The difference in reported task ease may also be due to the difference in complexity between the usernames provided for our study's Gmail account, "userstudy2018," and Amazon account, "danielanapoli@cmail.carleton.ca." It is difficult to identify the influence of each factor separately. We suggest future research should use consistent credentials between websites to more confidently assess possible usability issues.

Task 3: Complete transaction

Six out of six participants were able to download an email attachment on Gmail. Six out of six participants were able to make a donation on the CCNIB website. Four out of six participants were able to finalize a purchase through Amazon.

Figure 4.11 summarizes how difficult participants found Task 3. Figure 4.12 summarizes participants' reported confidence in their performance during Task 3.

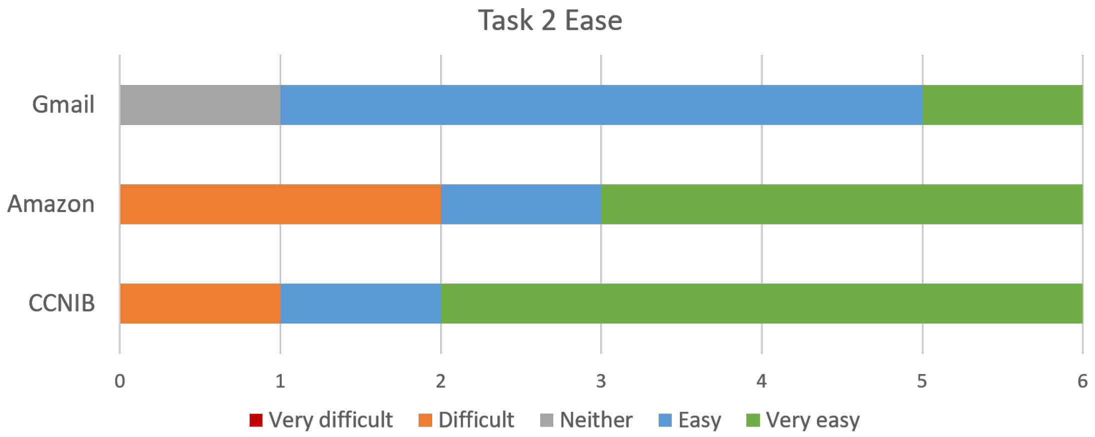


Figure 4.9: Difficulty of login or finding donation page (Task 2).

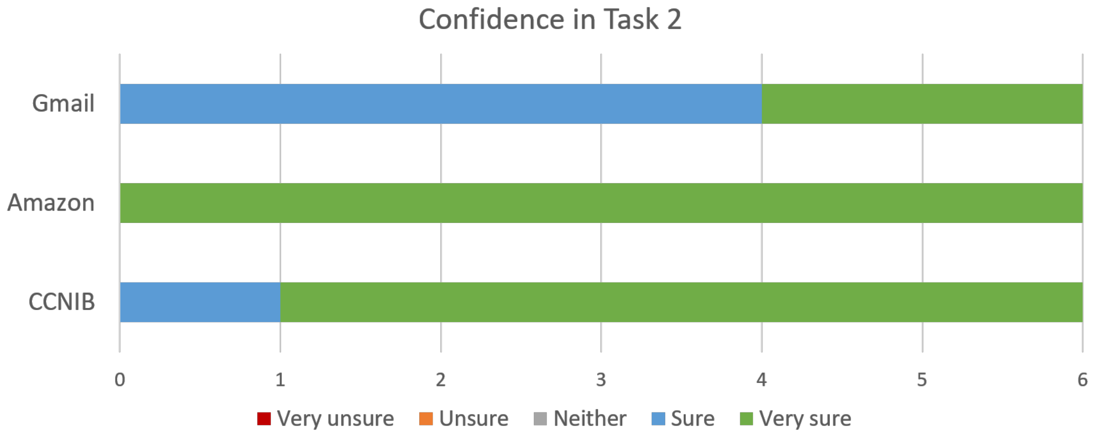


Figure 4.10: Confidence in login or finding donation page (Task 2).

Participants found Task 3 somewhat more difficult than the previous two tasks. Per our results, finalizing a purchase on Amazon (M=2.8, SD=1.3) may have been more difficult than downloading an attachment on Gmail (M=3.7, SD=1.4) or making a 10 dollar donation on CCNIB (M=4.8, SD=0.8). Participants seemed more confident in their performance during Task 3 with Gmail (M=4.7, SD=0.5) than with CCNIB (M=4.0, SD=1.1) or Amazon (M=3.7, SD=1.6).

As mentioned, two participants, U04 using VoiceOver and U14 using JAWS, were unable to complete the Task 3 on Amazon. Specifically, Amazon required the participants to specify the parcel's mailing address. The interface required participants to choose from two offered addresses in order to progress to the task's next step. The nuances between the addresses were highlighted in red, but not described through audible alternate text. As a result, both users ran out of allotted time while trying to identify which address they should use.

Overall, our findings suggest that severe accessibility issues not only negatively affect the users' success but can negatively impact other aspects of their user experience including their perception of task ease and confidence in their performance.

4.3.3 Post-Test Questionnaire

The ecological validity of laboratory studies to observe users' typical security habits, sighted or not, is debatable. A major argument against controlled test scenarios is participants may be inclined to more actively consider their security and privacy during the study than they normally would on a regular basis. Alternatively, some argue that the testing environment evokes a sense of safety that may cause participants to feel they are in less danger than they would be outside of the study.

To mitigate these effects, we did not emphasize security and privacy before or during tasks. The discussion of security was reserved for the post-test questionnaires and interviews. We used 5-point semantic scale questions to measure participants' level of concern (1 = very unconcerned and 5 = very concerned) for the 12 suggested cybersecurity concerns. We also asked participants to rate the effectiveness of (1

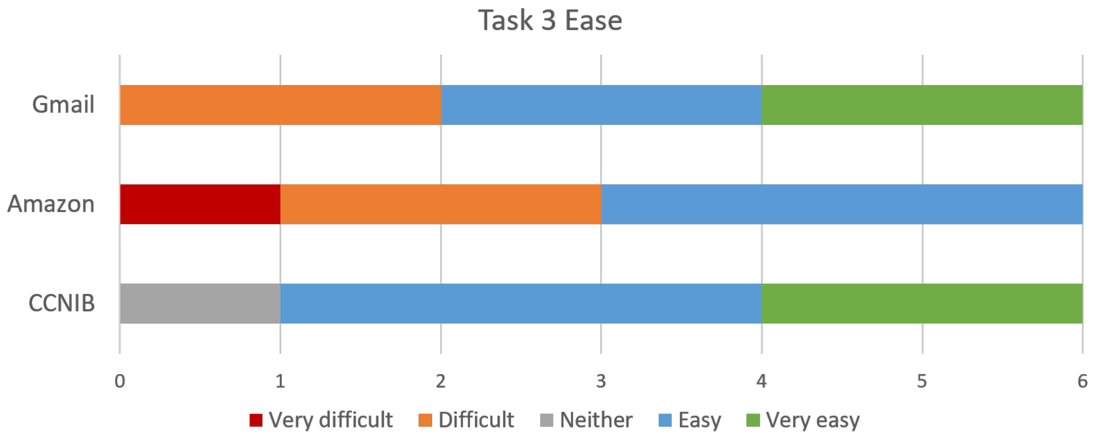


Figure 4.11: Difficulty of completing site-specific transaction (Task 3).

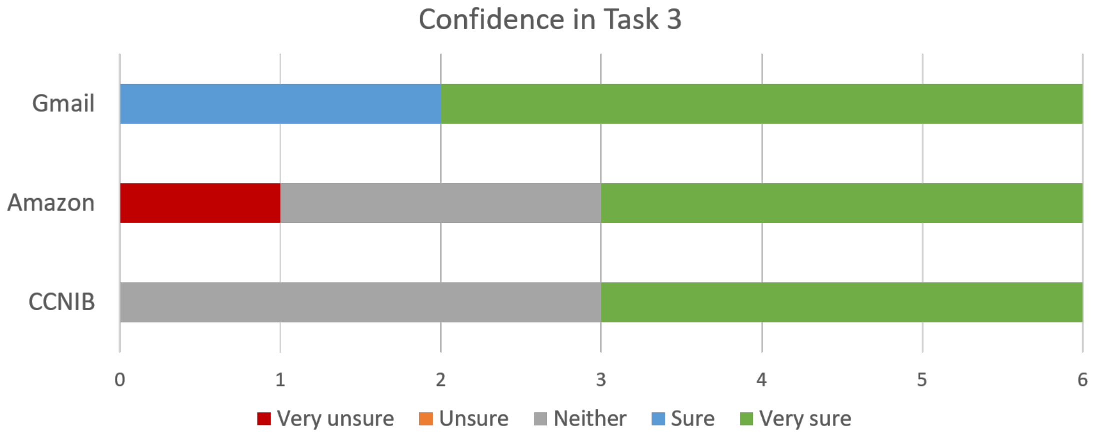


Figure 4.12: Confidence in completing site-specific transaction (Task 3).

= very ineffective to 5 = very effective), and the likelihood to adhere to (1 = very unlikely to 5 = very likely), the 11 suggested protective actions.

Rating Cybersecurity Issues

Figure 4.13 summarizes participants' reported concern towards the listed 12 cybersecurity issues. We sort the issues by participants' ratings of most concerning to least concerning, per the sum of "concerned" and "very concerned" responses.

Participants were most worried about their financial information (T2) and identity (T1) being stolen. Participants were particularly concerned with someone tracking their online activities (T6). Similarly, participants found keystroke logging software (T10) and other malware or viruses (T9) highly concerning.

Participants were least worried about people eavesdropping (T11) or watching their interactions with their device (T12), and their email accounts being hacked (T7).

Our results are similar to related studies regarding visually impaired web users' cybersecurity concerns [56, 87] where participants also expressed great concern with protecting their financial information, identity, and their device from being infected by viruses or malware.

Participants' lower levels of concerns regarding their physical privacy and email accounts differs from Ahmed et al.'s study [3] exploring visually impaired users' security concerns. We think this difference may be due to our study's participants interpreting the severity of these physical threats at home rather than in public spaces. Future studies may want to compare visually impaired behaviours while completing online transactions in public versus at home to understand any nuanced differences in security and privacy perceptions.

Perceived Effectiveness of Protective Actions

Figure 4.14 summarizes participants' perceptions of the listed protective actions. We sort the results from most effective to least effective protective action per the sum of "effective" and "very effective" responses.

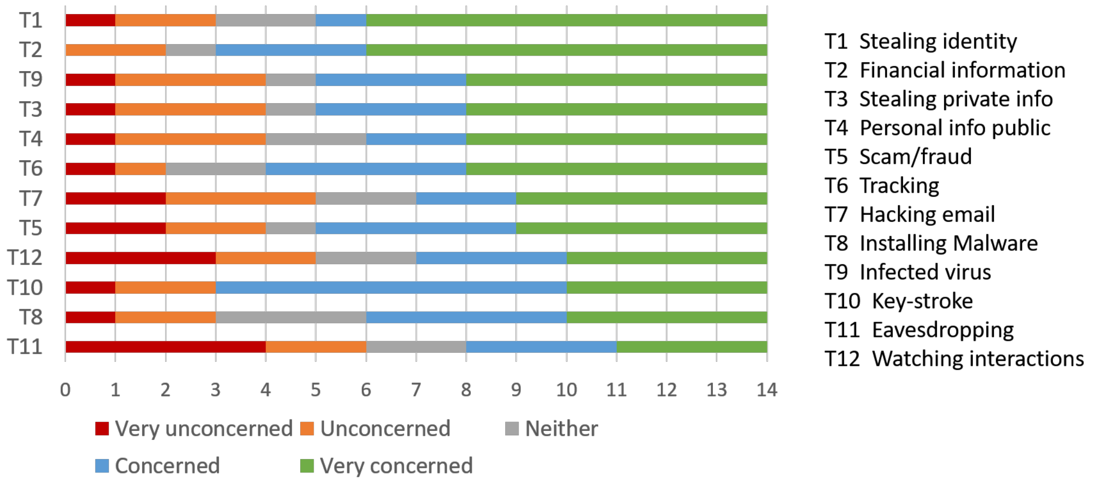


Figure 4.13: Reported concern towards 12 cybersecurity issues, sorted by most concerned to least concerned.

Generally, participants regarded the common security advice as effective or very effective means to protecting themselves while online. Participants believed that using strong passwords (PA5), anti-virus software (PA4) or other software from official trusted sources (PA3), and avoiding unexpected attachments (PA11) to be the most effective.

Participants rated automatic updates (PA2), password managers (PA8), and only using websites with HTTPS (PA9) among the least effective protective actions.

Two of the 14 participants were evidently more knowledgeable of security best practices than the others; U07 had a background in Computer Networking, and U14 had experience in customer service at a banking institution. Yet, neither claimed expertise in cybersecurity.

Our results reflect other studies gauging sighted non-expert users' perceptions of common security advice. Participants in Ion et al.'s study [58] similarly emphasized using strong passwords and anti-virus software.

In the same study, experts emphasized installing software updates and using password managers. Our participants rated these actions as ineffective. Participants cited that enabling automatic updates could be disastrous to the system's accessibility. As

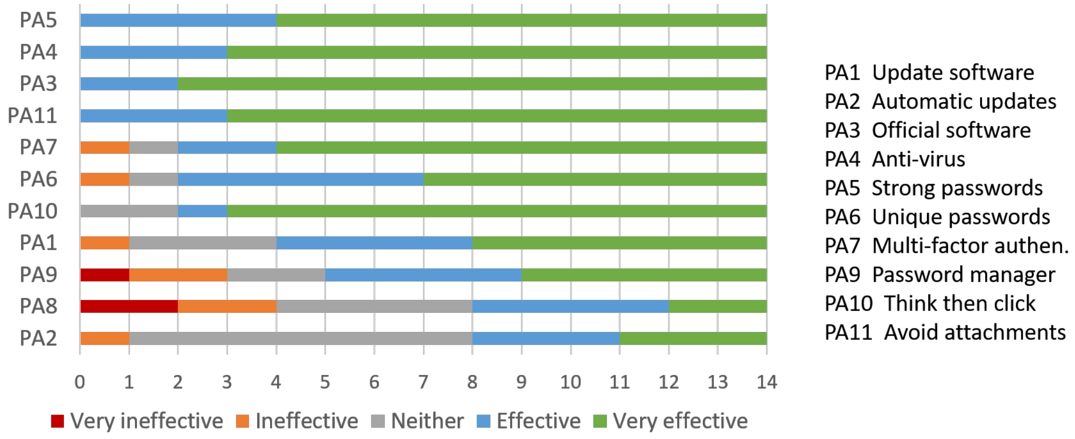


Figure 4.14: Reported effectiveness of 11 protective actions, sorted by most effective to least effective.

we will elaborate on later, participants had similar accessibility concerns with password managers.

Likelihood to Adhere to Protective Actions

Figure 4.15 summarizes participants' likelihood of taking the listed protective actions. We sort the results from most likely to least likely per the sum of "likely" and "very likely" responses.

Participants were likely or very likely to use strong passwords (PA5), official software (PA3), and to think before they click on a link (PA10).

Reflective of the low effectiveness ratings, participants were least likely to use password managers (PA8), automatically update their systems (PA2), and only using websites with HTTPS (PA9). Participants were also unlikely to use unique passwords between different sites (PA6).

Although many noted difficulty in remembering more than a couple of different passwords, three participants were particularly concerned with storing their passwords within browsers. When inputting their passwords, screen readers will not announce the character they are input as a method of protecting their confidentiality, for example JAWS announces "star" when typing within password fields. This masking

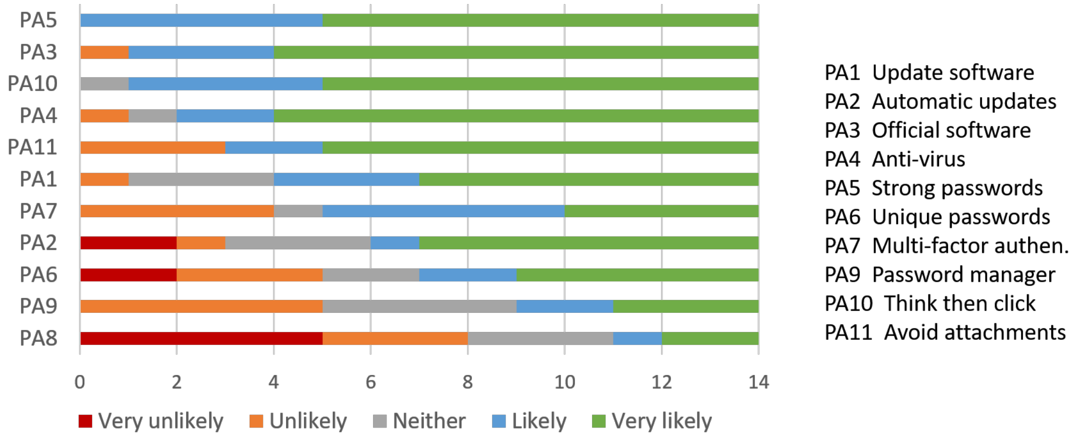


Figure 4.15: Reported likelihood of taking the listed 11 protective actions, sorted by most likely to least likely.

technique is intended to protect the password from eavesdroppers but, many said it caused them to be uncertain they had input the string correctly and therefore were deterred from storing the potentially incorrect password for future use.

Furthermore, some partially sighted participants, who were able to see the keyboard while typing, were also concerned with password managers and believed that the manager would make them more vulnerable to security breaches because hackers would only need to break into one program to get access to all their accounts.

Additionally, participants said they were unlikely to enable automatic updates because the updates can change system features that they have learned to access through their assistive software, or introduce accessibility issues that did not previously exist. Participants also said they unlikely to only use websites that have HTTPS because they do not usually actively seek out HTTPS in URL addresses.

General low levels of adherence to security advice is not exclusive to users with sight loss. Many researchers suggest that any user would reject security advice if it is riddled with exceptions or is perceived as more costly than beneficial [53, 85]. However, our participants are particularly deterred from using suggested security techniques due to accessibility concerns.

Theme	**Number of Excerpts**
Attitudes	112
Behaviours	142
Concerns	72
Desires	15
Total	341

Table 4.4: Number of participant quotes and observatory notes listed per theme and task.

4.3.4 Post-Test Interview and Other Observations

We conducted semi-structured interviews with participants after they had completed the assigned tasks. We asked open-ended questions regarding their main techniques for protecting themselves online, the main obstacles they face while trying to maintain their security and privacy, and what makes them feel safe while working with sensitive information online.

Participants' responses and other comments made during the sessions were recorded and transcribed. We extracted 341 quotes and observational notes taken during the sessions. As pictured in Figure 4.16, we sorted the data by task and coded excerpts thematically to best fit into four a priori themes that reflect our research goals: attitudes, behaviours, concerns, and desires. We used a thematic approach over an open-coding approach to manage our scope. Table 4.4 summarizes how the excerpts were organized per theme.

We grouped excerpts that appeared more than once or were closely related to other excerpts. We identified these groups as "trends" within the coded themes. Our final trend counts, noted in Section 4.3.4, were based on the number of participants with similar perspectives or actions.

The lead researcher completed the analysis and may therefore possess bias towards their single perspective. Future research may benefit from multiple coders as long as inter-coder reliability is maintained.

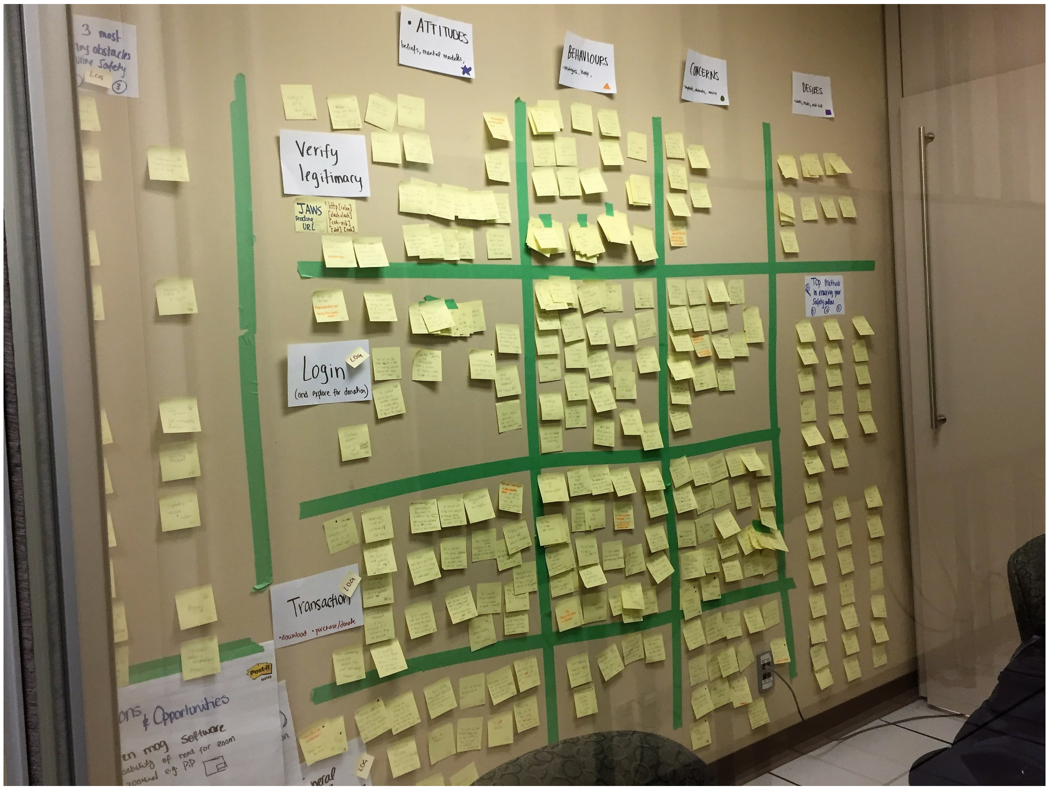


Figure 4.16: Our thematic approach to analyzing the qualitative data collected during each of the 14 sessions.

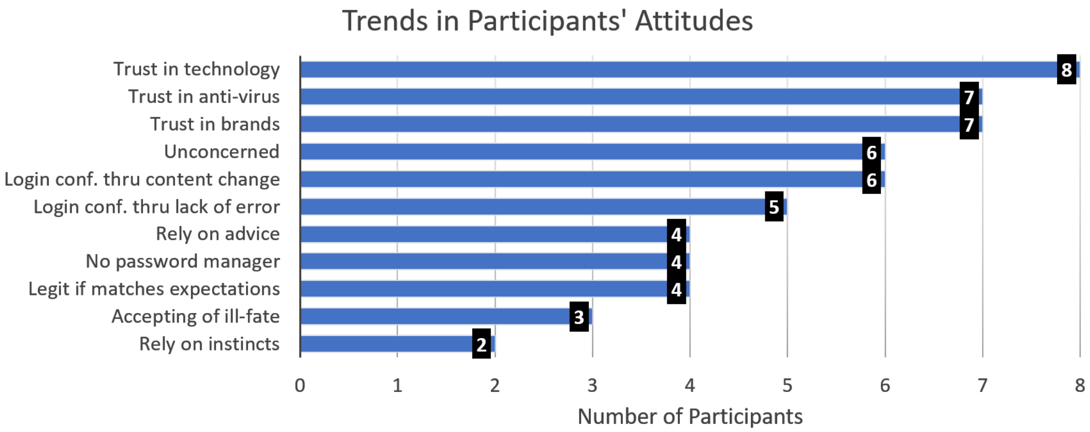


Figure 4.17: Trends in participants' attitudes, sorted by most prevalent to least prevalent.

Attitudes

We describe the 11 trends we found in participants' attitudes in Figure 4.17.

Most trends were pertinent to participants' approaches to their general security and privacy. Two trends, *login confidence through content change* and *login confidence through lack of error,* describe the workarounds visually impaired participants' relied on to assess whether they had been granted access to the Gmail and Amazon accounts. Neither website provided explicit non-visual indication that a login was successful, therefore participants inferred the state of their account if they did not face errors prohibiting their progress or were able to find new content on the page they were seemingly redirected to. We discuss other notable trends in participants' mental models below.

Trust: Three of the most prominent trends in participants' attitudes pertained to trust. Our results suggest that participants placed a large amount of faith in the devices and websites they used to share information online. Specifically, eight participants believed that built-in security mechanisms on their devices were sufficient to maintain their security. Seven participants explicitly noted trust in their anti-virus software:

> "I usually use my iPhone to download attachments because I know it's

> not going to get viruses.” **U05**

> “It felt secure. If the computer had securities on it, and they were checked, going by that, it looks good.” **U11**

> “I know that my anti-virus would block the site if it wasn’t safe.” **U13**

Additionally, seven participants were more inclined to share personal information with websites that contained audible or visual information denoting association with organizations they recognized, regardless of whether the site was really legitimate:

> “With Amazon I felt very confident [in its security] because it is a reputable website.” **U02**

> “I trust Google, so I know it’s legitimate.” **U08**

> “The CNIB website is secure because I know that organization. They have more protection compared to others.” **U06**

Expectations: This uncritical approach to online security and privacy was not often based on legitimate security indicators, but rather was validated by signifiers that fulfilled their expectations. For example, six participants believed that a page was more likely to be legitimate and safe if the page contents were consistent with what they had previously experienced:

> “I would guess it is [legitimate] based on what I’ve seen before when using Amazon’s site.” **U02**

> “I usually use Google so I recognize this site. I’d say it’s legitimate.” **U03**

Four participants who were unfamiliar with one of the test websites were more likely to trust it if it had content they would expect to find on a website that belonged to the purported organization:

> “I think it’s legitimate because it has an edit field to type in your email, a next button, and you’re able to change the language.” **U01**

> “My confidence is higher that this is a legitimate website because of its content. Only the CNIB could have this content.” **U12**

Implications: Once a participant had chose to trust their device, or the website they were interacting with, their general approach to sharing information remained passive. Particularly, five participants were generally unconcerned with their online security and privacy:

> “I don’t usually think about it [security] because then you would become paranoid... You have to take a chance when you do anything on the internet.” **U07**

> “Security is overblown. People hype it too much, but I could be wrong.” **U03**

> “I take all precautions, and once I take them I’m no longer concerned. If those companies do not secure my information then I would be concerned. Based on what’s offered [security mechanisms] to me, once I take part in that, I’m not concerned.” **U04**

Two participants were confident that they would be able to recognize unsafe circumstances based on their instincts:

> “If I get a weird feeling from the site, then I don’t feel safe and I wouldn’t do it [complete a transaction].” **U03**

However, three participants who were less confident in the means they use to maintain their security approached the process of browsing the web almost helplessly:

> “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 anti-virus or security software, it can still be hacked.” **U14**

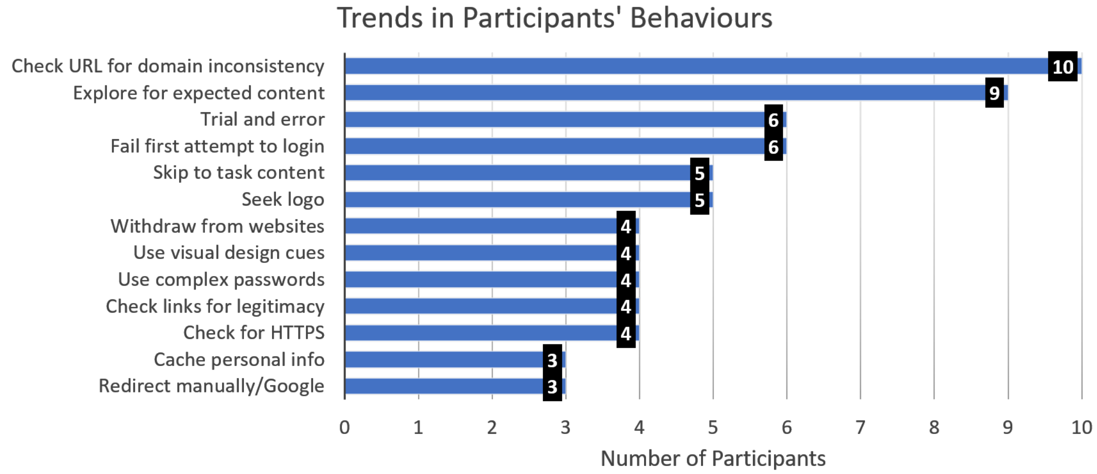


Figure 4.18: Trends in participants' behaviours, sorted by most prevalent to least prevalent.

Ultimately, participants' seemed to believe they could confidently share their personal information online if they used guarded devices to interact with reputable companies. This is concerning because many of the indicators (text, logos, page structure) participants' believed justify the validity of this approach can be easily spoofed. These evident trends also suggest that participants' mental models of online security are somewhat misinformed or incomplete. For example, no participants noted issues that could occur while transmitting information (man-in-the-middle attacks) to trusted websites nor noted that spoof websites could closely imitate legitimate ones.

Behaviours

We identified 13 trends in participants' behaviours. We summarize these trends in Figure 4.18. These trends describe how participants manage their online security and privacy while assessing a site's legitimacy and logging into and completing transactions on websites.

Best Practices: As mentioned, participants did not always use best practices. Only four participants mentioned that they check for HTTPS connections and use passwords that contain a mix of letters, cases, numbers, and symbols. However, we observed 10 out of 14 participants scan the URL address bar to look for domain inconsistencies while completing Task 1. Avoiding websites with misspelled domains can prevent phishing. Yet, this technique did not help participants recognize the spoofed CCNIB site.

Specifically, for blind participants, the audible information made available through screen readers was insufficient to make informed decisions about the site's domain. JAWS announced the site's address in the same way it would read the legitimate site's: "H-T-T-P-colon-slash-slash-W-W-W-dot-cuh-nib-dot-cah;" participants were unaware of the extra "c" and therefore trusted that the domain was correct. To check for misspellings, JAWS users can manually cursor through the URL address to read each character individually but none did so during our study.

The extra "c" was eventually noticed by one partially sighted participant who did not use assistive technology to complete tasks (U12). Yet, the methods in assessing site legitimacy that we mentioned previously took precedence as he ultimately decided to make a donation through the CCNIB website based on the site's content regardless of the misspelled domain.

Risky Practices: Participants relied on unreliable techniques to assess sites' legitimacy. Five participants skipped content in order to find information (logos or text) that met their expectations of what the website *should* include. Four participants clicked on page links in hopes of being redirected to new pages with more expected content. This is particularly concerning since some attacks can disguise malware downloads as URL links through HTML tags and CSS stylization.

Additionally, participants relied on trial-and-error approaches to interact with the site. In order to progress through the tasks, six participants clicked on links or typed in form fields they were not confident would lead to their success. Six participants also made multiple attempts to login to the site. This may have been due to their unfamiliarity with the credentials we provided; however, a few noted that it was common to fail their first login attempt. Approaching sites in an experimental fashion increases chances for critical mistakes. For example, users may unknowingly type and submit private information in unprotected form fields.

Overall, the behaviours we observed were similar to those documented in related literature about sighted users' methods in maintaing their online security and privacy.

Particularly, sighted web users [8, 45] also decided a site was secure if its content included branding associated with trusted businesses or just generally matched their expectations of a professional, legitimate website. These techniques in assessing page legitimacy are ineffective for both sighted and visually impaired users due to the ease of spoofing content, much like we did in our study. Alternative text that blind screen reader users rely on to understand visual content can also be exploited to seem legitimate [54].

Other Notable Behaviours: We noted a few additional trends that inconvenience the processes of engaging in online services. In particular, when faced with uncertainty, four participants noted that they refrain from sharing information online. Some participants reported that they avoid using a website entirely or use a fake name and address in order to trick the system into providing the service regardless of the information's validity. Yet, this may only protect privacy on social media or email when this information does not need to be checked by external entities like the bank or government.

Three participants noted that they are most confident in interacting with websites by manually entering the page's URL address, or by using a Google search. This strategy was used to follow-up with urgent emails from trusted organizations but avoid potentially malicious links embedded in the message. Through this method, these participants believed the sites would most likely be safe. However, participants did not consider additional threats that exist outside of phishing.

Concerns

Figure 4.19 summarizes the nine trends we identified in participants' online security and privacy concerns.

Sufficient Protection: Like in the post-test questionnaires, the trends in participants' comments regarding their concerns suggested emphasis on protecting their financial information and their devices from malware and viruses:

> "A big concern is visiting a site that has some spyware or malware on it, but I won't know... I feel like a lamb to the slaughter." **U02**

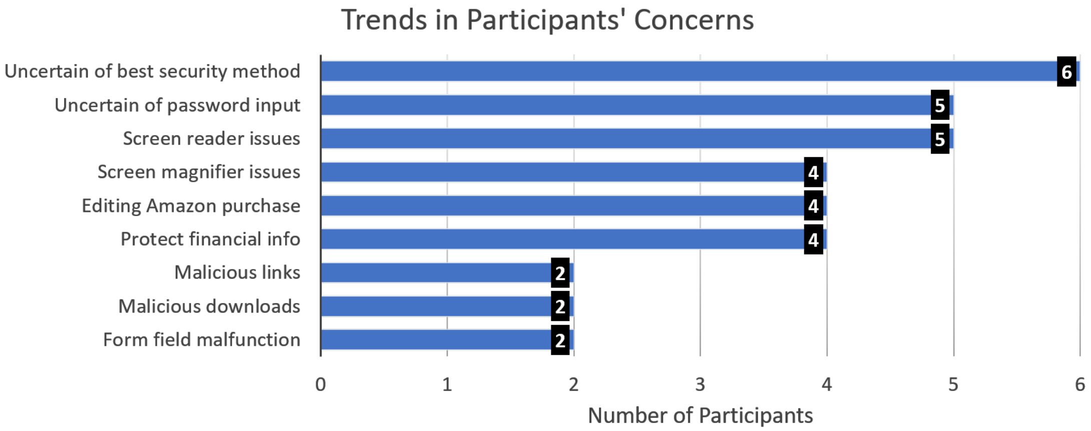


Figure 4.19: Trends in participants' concerns, sorted by most prevalent to least prevalent.

Yet, what is particularly concerning is that six out of 14 participants reported that they were unsure of how to best protect themselves or recover after their security or privacy had been breached. Furthermore, participants are not always confident in the advice they receive:

> "Sometimes it's almost like you don't know... It's like security systems in your house. Of course security companies are going to tell you that you need them, and if you didn't get that they will tell you something that might happen. So you don't know if something is important or if you can get by without it. It's knowing what to do that's hard." **U05**

> "I personally have experiences where random technology 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 do take a lot of risks, it's just a reality. I have to be safe and smarter about it... I often rely on [blind] people who have been using it [JAWS] longer than me." **U01**

Accessibility and Usability: Prominent trends in participants' concerns also pertained to general accessibility and usability issues. Four partially sighted ZoomText users noted that the magnifier is needed to read text on a page but, due to the intense magnification, it is often difficult to properly keep their place on the page or recognize important surrounding information.

Additionally, five participants noted that their screen reading software (JAWS or VoiceOver) is not always compatible with other sites and software, and therefore does not always provide sufficient information to properly assess their security:

> "When they [anti-virus software] give the message that they have found a virus or malware, they don't say what is actually wrong. JAWS doesn't read it either. You have to get someone else to read it. Or, you have to click quarantine not knowing what programs are actually protected." **U14**

Participants also relied on content changes (N=6) and lack of error messages (N=5) to assess whether their login attempts were successful and access to account information had been granted. A lack of definitive login feedback can contribute to the risky experimental behaviours we previously mentioned.

Desires

Due to the design of our study, we uncovered more evidence supporting participants related attitudes, behaviours, and concerns than participants' desires. Below, we discuss a few interesting notes regarding participants' preferences with security interfaces.

More Instructions and Visual Cues: Although all participants possessed some level of sight loss, visual cues were particularly important to understanding the websites.

Five partially sighted participants heavily relied on distinct call-out buttons and other visual cues to find pages and information they needed to complete the assigned tasks. One participant noted that heavy reliance on colour to quickly understand the meaning of security warnings. This important to note as there may be a tendency to de-emphasize visual aspects of an interface when designing for users with sight loss:

> "The colour of that [dialogue], orange or red, you suspect something. If it's green, you make it more safety [sic] and I have more confidence." **U08**

Two participants noted that they wanted emails or other concluding feedback to confirm that they completed a transaction successfully. Additionally, one participant mentioned that they prefer the convenience of biometric authentication methods (finger ID on iPhone) rather than passwords or PINs.

4.4 Discussion

We asked seven blind and seven partially sighted participants to complete three tasks on websites that elicited opportunities for security and privacy concerns. All participants were able to fully attempt all tasks but, some failed to finalize a purchase on Amazon to insufficient alternative text describing an error on the page. Furthermore, none were able to detect the spoof website and shared sensitive information including addresses and credit card information with the website.

Additionally, participants' task ease and confidence ratings were generally high when interacting with the spoofed website we created for the study. Participants mainly trusted the CCNIB website because it was supposedly affiliated with an organization they were familiar with, and it contained content they expected CNIB to include on their legitimate website.

Questionnaire results and the trends in participants' security attitudes, behaviours, and concerns we identified through our qualitative analysis suggest that: 1) there are severe issues in participants' perceptions of assessing website legitimacy and security, and 2) despite recent Web accessibility advances, visually impaired users are still facing detrimental usability obstacles while engaging in online services.

4.4.1 Awry Security Indicators

It took us a few days and twenty dollars to create and host a phishing website that was trusted by people in the visually impaired community. The ease of successfully phishing our participants is alarming. Our results suggest that visually impaired participants rely on erroneous methods to browse securely. Their security and privacy browsing strategies were often a result of website accessibility or usability issues, and in many cases, limited their ability to properly assess suggested security indicators.

Consistent with documented sighted users' habits [48], partially sighted participants were also task-focused rather than security-focused; they did not emphasize visible security indicators when completing tasks. Specifically, the majority of partially sighted users did not actively seek, nor notice the absence of, evidence of HTTPS while assessing a site's legitimacy or processing a financial transactions. This behaviour could have contributed to the fact that no partially sighted participants identified the illegitimate website.

Due to their task-focused behaviours, visually impaired users zoomed in on portions of the page that were specific to meeting their goals such as form fields or page content. Passive browser chrome indicators did not aid visually impaired users in behaving securely. Our results suggest that emphasizing browser chrome indicators may not be enough to help partially sighted users in behaving securely because they can only see a small portion of a website at a time when using a screen magnifier, and this small field of view is more likely to focus on page content rather than other areas of the browser. Passive indicators may also not be sufficient in addressing visually impaired users' need because, in the circumstances where partially sighted participants ignored extraneous page content in order to mitigate eye fatigue, it becomes necessary for some users to avoid information that is not directly pertaining to their goals.

Blind participants using screen readers also did not emphasize browser security indicators. Instead, to comprehend the page as a whole, they skimmed pages while completing tasks and skipped over large portions of content to find relevant information pertaining to their goals. This behaviour is also noted in related literature [17,84] pertaining to blind screen reader users, and is sometimes a necessity to alleviate heavy cognitive loads associated with browsing websites audibly.

However, this habit is concerning because it could increase the likelihood of missing vital security-related information. Simply providing alternative text to describe security indicators like lock icons and SSL certificates is not sufficient in aiding blind users because they are not likely to actively seek out this information while trying to understand and manage the website's information. Since passive indicators cannot be read without manually accessing related portions of the screen through a keyboard short-cut, security information can potentially go unnoticed by blind screen reader users.

Other existing visual security indicators, and corresponding alternate text, are also ineffective. As mentioned, all visually impaired participants checked domain addresses, but this action did not deter them from trusting the phishing website. All but one partially sighted user who interacted with the CCNIB site did not seem to notice URL's inconsistency when relying on their sight and the screen magnifier. Additionally, JAWS announced "ccnib.ca" the same way it would dictate "cnib.ca," and therefore blind users who assessed domains with the screen reader could not realize the URL's inconsistency without taking further steps to meticulously parse the address.

The one partially sighted participant who noticed the CCNIB domain continued to trust the website nonetheless. The fact that no one noticed URL inconsistencies, took further actions to explore them, or heeded the red flag, could suggest that participants may not have generally approached our study critically. This could be due to the test environment or, as Schechter et al. [93] suggest, participants who do not use their personal data during security studies may disregard attack clues more than those who use their personal credentials. However, participants' most prominent trends in assessing page legitimacy based on its content, and generally trusting technology and site owners to keep them safe online, lead us to believe that their uncritical behaviours may not differ greatly when completing similar transactions with their own credentials outside of the study. Furthermore, the content-based assessments our participants were engaged in are prevelant among other sighted [45] and visually impaired [8] users, and contrary to prior research [96], participants of all ages, genders, and education levels equally exhibited this risky browsing behaviour.

Our participants relied on page content to complete security tasks online. This suggests that visually impaired users are considerably vulnerable to malicious carbon copies of legitimate websites because existing security indicators, and alternative text describing these visual indicators, are not sufficiently accommodating their unique abilities, behaviours, and assistive technology.

4.4.2 Poor Accessibility

Insufficient web browser security indicators are not the only limitations affecting visually impaired users. Participants cited several accessibility and usability obstacles pertaining to security software which impede their efforts in maintaining their online security and privacy.

Automatic updates can patch security vulnerabilities on an operating system or other software without relying on users to properly configure or apply changes. However, participants reported that they did not enable these updates because they can ruin the accessibility of their system. Therefore, it was necessary for our participants avoid updates to their systems.

Password managers can create and store passwords for users so that they have strong account credentials. Yet, participants reported that they were not likely to use password managers because they are often incompatible with their assistive software. Additionally, participants were unlikely to cache their passwords within a browser because both visual and audible masking techniques ultimately render them uncertain about whether they have correctly entered their password.

Anti-virus software can notify users of potential security and privacy breaches. The majority of participants cited that they rely heavily on this software to protect them while completing tasks online as a fail-safe measure. However, blind participants reported that this software is inaccessible through screen reading software and that they are forced to make decisions based on the limited available information.

Ultimately, our results suggest that in many cases visually impaired users are faced with the decision between security or accessibility, and choose the latter in order to continue to engage with technology.

4.4.3 Unclear Advice

Participants were uncertain of how to best manage online security and privacy. This uncertainty stemmed from accessibility and usability obstacles they faced when attempting to engage in security behaviours. When faced with an issue, participants seemed determined to find a solution but reported that their last resort usually relied upon sighted individuals to complete a task on their behalf. This is not ideal and ultimately diminishes their perception of a security measure's effectiveness.

Visually impaired participants were also unsure of how to approach their online security and privacy due to the contradictory nature of some security advice. Some participants cited best practices, such as noticing missing HTTPS to pin-point phishing websites, but would then mention that they realize evidence of encryption is not a guarantee for their security.

Furthermore, some participants did not always trust the security professionals which offer this advice. In particular, one participant was sceptical of advice which seemed to lack an understanding of their unique visually impaired experiences. She mentioned that the accessibility obstacles she faced forced her to approach online interactions in a more careful manner than those who are sighted and not privy to these same issues. Therefore, she believed that professionals who were not familiar with the issues she faced would provide advice that would result in less security than she required.

Each of these sentiments play into the "rational rejection" of security advice. In line with participants' concerns, Herley [53] suggests that truly beneficial security advice should better acknowledge that best practices can be arbitrary and therefore, engage users in security matters so that resulting advice better fits their computing needs. Considering the minimal literature that addresses accessibility and security, this is especially important for developing future advice tailored to visually impaired users.

Chapter 5

Discussion and Conclusion

Through an expert evaluation using JAWS and a user study including visually impaired users including seven blind and seven partially sighted individuals. We uncovered usability issues that greatly impede visually impaired users' opportunities to verify a site is legitimate, log in, and complete transactions securely. We revisit our original research questions to frame our findings.

5.1 Research Questions

We aimed to contribute to research at the intersect of web accessibility and usable security. We approached this goal through three main questions pertaining to visually impaired users' web-based security and privacy concerns.

Q1: What types of online security/privacy concerns and barriers exist? When asked, participants in our study were most concerned with securing their personal data including identification and financial information. They were also particularly concerned with protecting their device from viruses and malicious software.

These concerns do not differ greatly from those documented in relating literature pertaining to their sighted counterparts [58]. However, we uncovered significant barriers in addressing these concerns during our expert evaluation and user study.

Most prominently, many security indicators and software are not accessible nor easy to use via screen readers or screen magnifiers. Additionally, participants were unsure of how to best protect themselves online or how to recover if their security and privacy had been breached.

This uncertainty stemmed from: 1) the usability issues faced when using assistive software, and 2) distrust in advice from experts without evident knowledge of the nuances in visually impaired users' experiences.

Q2 Are web security cues easily accessible and interpretable? Per our expert evaluation using JAWS and guided by the ACCUS heuristics, there are significant issues with the accessibility of security cues. The most common issues pertained to the *Controllable, Recognizable,* and *Responsive* aspects of the website which allow a user to access and manoeuvre the interface confidently. The most severe issues pertained to the *Functional, Diverse* and *Assistive* aspects of the website which impeded a user's opportunities to behave securely, including accessing and reading Internet Explorer's lock icon and SSL dialogues describing whether a connection was encrypted.

Our user study confirmed these issues as all visually impaired, both blind and partially sighted, participants could not easily engage in secure behaviour. In particular, blind users were unable to read lock icons, SSL dialogues, and properly decipher phishing URLs due to JAWS limitations.

Additionally, participants noted usability issues pertaining to the web-based mechanisms intended to protect their security; specifically, blind participants reported that they must input passwords through a trial-and-error process since screen readers commonly mask character feedback while typing. As suggested by our expert evaluation, users received insufficient visual and aural feedback pertaining to successful logins; participants had to carefully explore page to find whether access to the account had been granted.

Q3 How do these users perceive and manage web-based risks and threats? Generally, our visually impaired participants approached security passively. Much of their trust was uncritical and based in incomplete or erroneous perceptions of their device's built-in security mechanisms and the organizations that were seemingly affiliated with the test websites.

When the visually impaired users tried to manage web-based risks according to security best practices, it was ultimately ineffective. For example, the majority of participants noted reliance on anti-virus software to protect them from malicious sites, yet were unable to properly configure and monitor the software due to incompatibility issues with screen readers and screen magnifiers.

Our expert evaluation focused on assessing security information pertaining to commonly advised protective actions. However, participants did not use all advised actions nor reported that they were likely to do so outside of the study because of the severe accessibility issues they faced and their ultimate distrust in the action's effectiveness. Furthermore, some noted that no amount of cautionary actions could guarantee their security and thus approached their online security and privacy with resignation that it would be violated.

5.2 Main Takeaways

Our results identify several inefficiencies in existing security mechanisms. Both of our studies uncovered severe issues which violate basic accessibility and usability principles are impeding users' abilities to behave securely online.

As our expert evaluation suggests, chrome-based indicators within Internet Explorer do not effectively communicate the current states of security; SSL dialogues are ultimately unreadable and lock icons are poorly described. Furthermore, there is minimal available feedback to tell users that they have accessed their account. These issues were also mentioned by visually impaired users during our user study who regularly use Internet Explorer.

Feedback from our user study further emphasizes that security mechanisms including password managers, automatic system updates, and anti-virus software are not accessible via assistive software. Due to these accessibility issues, visually impaired users rely on unreliable techniques to identify potential phishing sites. These users can benefit from improved security literacy however, they face legitimate concerns regarding advice and interfaces that evidently lack of a deeper understanding of their unique perspectives.

Without addressing these issues, visually impaired users may continue to be vulnerable and approach their online security with passive and uncritical attitudes.

5.3 Recommendations

Our research provides an initial basis to understanding visually impaired users online experiences. Our results suggest that merely adhering to the common web accessibility guidelines, the W3C WCAG, may not ensure sufficient security and privacy cues for visually impaired users. We believe that progress towards accessible and usable security must first address the severe accessibility issues pertaining to security software and indicators that are currently impeding visually impaired users' abilities to behave in a secure manner.

Particularly, screen reader users require systems that more reliably cooperate with their assistive software and offer more informative alternative text. Screen magnifier users would benefit from visual and audio security cues which are better positioned within their available field of view to avoid missing these critical indicators since the extreme level of page magnification needed to read text also isolates this information from surrounding context.

Our first iteration of the ACCUS heuristics aims to address the drawbacks of common accessibility and usable security guidelines. In this thesis, we proposed a single set of guidelines combining the best practices within these two fields. With ACCUS, designers may have a better understanding of how to support to visually impaired users' mental models and ensure sufficient opportunities for secure behaviours. These heuristics should be improved with further empirical evidence and should be validated by other accessibility and usable security experts.

We discuss initial considerations for improving the ACCUS heuristics and general methods in designing security information tailored to the visually impaired users' mental models we observed during our study.

5.3.1 Prioritize Security Information

Originally, the *reliable* heuristic was based in literature that advised security interfaces should describe the current state of security and related available functions in simple and clear language. Based on our findings, much of this information is available but cannot not be accessed by visually impaired users or is neglected while working around other accessibility issues. Therefore, we suggest that this information should not only be clear and simple but automatically pushed to users in order to ensure the explicitness of information required to engage in the system safely.

Examples of implementing the revised *reliable* heuristic on a web page would include prioritizing security related information over page content. For blind users, this would mean that the state of reliable security indicators, such as evidence of SSL encryption, is read aloud before domains, page titles, or page content. For partially sighted users, this information would be pushed into, and emphasized within, their default field of view. In other words, address bars or other visual cues should be automatically shown on screen rather than the page's header or navigation bar.

In each of these circumstances designers should take advantage of the sequential nature of visually impaired users' experience of web pages. If properly implemented, users will be forced to pass through security indicators before accessing the content they are seeking. This will inform users of potential risks before seeking this information in other aspects of page content. Like pop-ups, there is opportunity for users to be annoyed by these forced warnings or ignore the messages entirely. However current usable security studies are exploring methods in reducing user habituation within visual security warnings [9, 43] and equivalent work regarding audible warnings may assist in defining the most effective methods of prioritizing non-visual security information. At the very least, security information should be grouped in a prominent and predictable location for users to access.

5.3.2 Provide Proactive Assistance

The *assistive* heuristic was based in literature suggesting that systems should be designed in a way that users can diagnose and recover from security errors. Our studies show that screen reader users were not provided sufficient audible information to properly diagnose errors that were visibly shown on the tested websites. Furthermore, many mentioned that they were unable to access and comprehend the problems being flagged by their anti-virus software. Since most users demonstrated a willingness to resolve issues, but were uncertain of how to properly recover from the errors they faced, we conclude that cues which help users in fixing security issues should be accessible and *directive*.

Directive systems will pro-actively suggest solutions to users while providing enough context that they can understand the current state of security and how to improve it, if needed, without negatively impeding their cognitive load.

This suggestion is based on the evident mental models of our visually impaird participants but is reflective of Felt et al.'s "suggestive design" approach to SSL dialogues [43]. They argue that users are more likely to adhere to security warnings if the dialogues highlight the advised steps in doing so. Furthermore, Felt et al. suggest that users are more likely to comprehend and find urgency in an SSL warning if it explains the threat sources and the data at risk.

Although Chrome certificate dialogues include this directive information, it is not available through Internet Explorer nor Safari on iOS. Since many blind participants reported these browsers are the most compatible with the screen reading software they most frequently use (JAWS or VoiceOver), we strongly urge the certificates on IE and Safari be improved accordingly.

5.3.3 Improve Security Literacy

Additionally, future work should emphasize improving visually impaired users' security literacy to motivate these users to engage with online services in a more active and critical manner than we have observed.

Our results suggest that users could benefit from clarifying security misunderstandings and better emphasizing protective behaviours. As previously discussed, most visually impaired participants completed online transactions with an inherent trust in their devices and/or the organizations that supposedly owned the websites. Additionally, the majority of participants underestimated the effectiveness of some security techniques and therefore underused common security advice. To address this, we suggest that security advice tailored for the visually impaired population should be focused on more reliable methods of detecting phishing and the advantages of using unique passwords and password managers (given they are usable and accessible). Furthermore, this security advice should be devised in close collaboration with visually impaired individuals who are knowledgeable about security to ensure that it properly reflects their perspective.

5.4 Lessons Learned

Conducting user studies with vulnerable populations requires particular considerations. These studies are relatively more difficult to conduct than those including a more easily accessible demographic. We discuss the main lessons we learned from conducting our research in hopes of making accessibility research less daunting and to encourage future researchers in approaching the topic with confidence because, as mentioned, the state of current accessible and usable security research requires further empirical evidence.

5.4.1 Expert Evaluations with Screen Readers

This study emphasized our immense respect for visually impaired users' unique mental dexterity. Conducting an evaluation based on audible cues rather than visual cues was fatiguing for the lead researcher and sighted peers who piloted our user study. Yet, the JAWS users we observed did not seem strained when using screen readers to complete online tasks. This suggests that the habits of this demographic cannot be simply rehearsed or empathized by sighted evaluators in the same way they may conduct walkthroughs via normative users' perspectives. Our experience underlines the necessity of involving visually impaired users in the process of improving web accessibility. Since this may not always be possible, we offer other sighted evaluators three main tips in improving evaluations via screen readers.

Practice

There are a number of readily available online resources that can guide researchers in testing with screen readers. Freedom Scientific provides an extensive list of JAWS shortcuts[1], and Apple provides an online VoiceOver tutorial[2].

Not all visually impaired users are expert screen reader users; some novice users may face usability issues that an expert screen reader user may not. However, we found it very useful to become well acquainted with the software used by visually impaired individuals to reduce the likelihood that uncovered usability issues are due to personal unfamiliarity.

[1] http://www.freedomscientific.com/training/training-JAWS-keystrokes.htm

[2] https://www.apple.com/ca/accessibility/iphone/vision

Spread Out Evaluations

As we mentioned, exercising audio-based mental capacity can be difficult for individuals who typically rely on their vision to use technology. To mitigate the effects of potential fatigue on the assessment, we took regular breaks in between evaluations.

Additionally, we enforced strict time limits to further mitigate the fatigue of using screen readers. Reasonable time limits also helped inform our assessment of the interface. For example, if a task like entering a username and password cannot be done within 15 minutes, this reflects poorly on the website's accessibility and usability.

Assess Both Visual and Audio Cues

Disabling the screen while testing websites with screen readers can be helpful when focusing on the audible cues used by some visually impaired users. However, we found that keeping a screen on while using screen reading software was critical in understanding the discrepancies between the visual and non-visual aspects of an interface. These discrepancies are important to identify since some visually impaired users use JAWS or VoiceOver to supplement their sight while exploring an interface and therefore require both visual and audio cues. Therefore, we do not suggest sighted evaluators to completely neglect their sight abilities during an assessment.

Furthermore, sighted researchers may benefit from including visually impaired individuals as expert evaluators, or as users in a supplemental observational study, to enhance the richness of the assessment and mitigate any bias resulting from vision-based assessments.

5.4.2 User Studies with Visually Impaired Users

The success of our study can be attributed to a number of factors.

Firstly, collaborating with community partners that are regularly engaged with visually impaired people greatly advantaged our recruitment efforts. Integrating community partners improved our outreach and seemed to foster initial trust which may have ultimately increased the likelihood of actual participation.

Secondly, community collaborators offered specialized insight from experience with the targeted demographic. Integrating collaborators' expertise during the study design process ensured our study was appropriate for visually impaired people and had maximum potential of addressing their various abilities.

Thirdly, our collaborators from CNIB and CCB generously provided space for conducting our research. These study spaces were more accessible to our visually impaired participants because most people regularly visited these locations and were confident in manoeuvring around the building. Conducting the user study in familiar spaces that participants seemed to increase participants' willingness, and ability, to engage in our research.

Finally, our participants' vision abilities varied greatly. As mentioned, some were legally blind and others were partially sighted in one or both eyes. We found that providing an array of tools to support various abilities was a necessity. We learned that vision-based tools like a monitor and computer mouse should not be discounted when testing with visually impaired users.

5.5 Limitations and Future Work

We recognize the limitations in our research. Each of our studies were conducted and analyzed solely by the lead researcher and therefore may be biased towards their single interpretation. Future research can address this limitation by integrating additional perspectives in relating expert evaluation and user studies. Additionally, our user study included fewer participants than typical usability studies and therefore may not accurately reflect the visually impaired population. Also, our laboratory settings may have impacted participants' approaches to their online security and privacy. Usable security studies have mitigated the laboratory effects through indirect observation [60], and future research can address our user study's limitations through similar approaches with a larger sample size.

We encourage future researchers to continue to conduct expert evaluations in order to assess the usability of security information available via screen readers and magnifiers. Since our study is based in one researchers' perspective, future expert evaluations should integrate more experts that are well versed in accessibility and security.

We also encourage future researchers to continue to integrate visually impaired users in their assessments to better understand users' mental models and reasons for security behaviours. Future related user studies should include a larger population sample, and further mitigate the laboratory effects on participants.

In the coming years, we aim to further refine the ACCUS heuristics to more specifically address evident visually impaired users concerns such as those pertaining to verifying website legitimacy or login processes. After establishing an improved set of heuristics we will assess its efficiency and reliability with feedback from other research who will apply the heuristics in similar expert evaluations we conducted in this thesis. Additionally, we aim to further explore non-visual security indicators – such as thermal feedback [109] – which can address visually impaired users' needs and also potentially improve security adherence for sighted users.

5.6 Conclusion

There is an evident gap in understanding visually impaired users' online security and privacy perceptions and behaviours. We combined best practices from the field of accessibility and usable security to create a first iteration of heuristics that can guide the design and evaluation of security interfaces for visually impaired users. With the ACCUS heuristics, we conducted an expert evaluation via JAWS to assess security information made available through websites and browsers. We uncovered severe issues impeding users' abilities to abide by common security advice. These issues were reiterated during our user study involving both blind and partially sighted users. To overcome these barriers, security systems and advice must take into account the unique perspectives of visually impaired users.

Bibliography

[1] A. Abbasi, F. Zahedi, and Y. Chen. Impact of anti-phishing tool performance on attack success rates. In *Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on*, pages 12–17. IEEE, 2012.

[2] 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.

[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] A. Aizpurua, M. Arrue, and M. Vigo. Uncovering the role of expectations on perceived web accessibility. In *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility*, page 74. ACM, 2013.

[5] A. Aizpurua, S. Harper, and M. Vigo. Exploring the relationship between web accessibility and user experience. *International Journal of Human-Computer Studies*, 91:13–23, 2016.

[6] F. Akhter, M. Buzzi, M. Buzzi, and B. Leporini. Conceptual framework: How to engineer online trust for disabled users. In *Proceedings of the 2009 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology-Volume 03*, pages 614–617. IEEE Computer Society, 2009.

[7] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. Cranor, and Y. Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 787–796. ACM, 2015.

[8] 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.

[9] B. Anderson, C. Kirwan, J. Jenkins, D. Eargle, S. Howard, and A. Vance. How polymorphic warnings reduce habituation in the brain: Insights from an fmri study. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2883–2892. ACM, 2015.

[10] AChecker Web Service API. Web accessibility checker. Web, 2011.

[11] The National Archives. Disability discrimination act 2005. Web, 2005.

[12] S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock. Passchords: Secure multi-touch authentication for blind people. In *ASSETS*, pages 159–166. ACM, 2012.

[13] 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.

[14] D. Balfanz, G. Durfee, D. Smetters, and R. Grinter. In search of usable security: Five lessons from the field. *IEEE Security & Privacy*, 2(5):19–24, 2004.

[15] 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.

[16] R. Biddle, P. Van Oorschot, A. Patrick, J. Sobey, and T. Whalen. Browser interfaces and extended validation ssl certificates: an empirical study. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 19–30. ACM, 2009.

[17] 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.

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

[19] C. Bravo-Lillo, S. Komanduri, L. Cranor, R. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the 9th Symposium on Usable Privacy and Security*, page 6. ACM, 2013.

[20] J. Brudvik, J. Bigham, A. Cavender, and R. Ladner. Hunting for headings: Sighted labeling vs. automatic classification of headings. In *Proceedings of the 10th International ACM SIGACCESS Conference on Computers and Accessibility*, Assets '08, pages 201–208, New York, NY, USA, 2008. ACM.

[21] 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.

[22] SO 2005 c 11. Accessibility for ontarians with disabilities act, June 2005.

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

[24] A. Casare, C. da Silva, P. Martins, and R. Moraes. Usability heuristics and accessibility guidelines: a comparison of heuristic evaluation and WCAG. In *Proceedings of the 31st Annual ACM Symposium on applied computing*, pages 213–215. ACM, 2016.

[25] 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.

[26] 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. Citeseer, 2007.

[27] J. Clark. To hell with WCAG 2. *A List Apart*, 217, 2006.

[28] World Wide Web Consortium. Web content accessibility guidelines 1.0, 1999.

[29] World Wide Web Consortium. Web content accessibility guidelines 2.0, 2008.

[30] World Wide Web Consortium. ARIA techniques for WCAG 2.0, 2012.

[31] M. Cooper. Web accessibility guidelines for the 2020s. In *Proceedings of the International Cross-Disciplinary Workshop on Web Accessibility (W4A)*, page 5. ACM, 2016.

[32] M. Cooper, D. Sloan, B. Kelly, and S. Lewthwaite. A challenge to web accessibility metrics and guidelines: putting people and processes first. In *Proceedings of the International Cross-Disciplinary Workshop on Web Accessibility (W4A)*, page 20. ACM, 2012.

[33] K. Coyne and J. Nielsen. Beyond alt text: Making the web easy to use for users with disabilities. Technical report, Nielsen Norman Group, 2001.

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

[35] M. de Borba Campos and J. Oliveira. Usability, accessibility and gameplay heuristics to evaluate audiogames for users who are blind. In *International Conference on Universal Access in Human-Computer Interaction*, pages 38–48. Springer, 2016.

[36] H. Desurvire, J. Kondziela, and M. Atwood. What is gained and lost when using evaluation methods other than empirical testing. *People and computers*, pages 89–89, 1992.

[37] R. Dhamija and D. Tygar. The battle against phishing: Dynamic security skins. In *Proceedings of the Symposium on Usable Privacy and Security*, pages 77–88. ACM, 2005.

[38] A. Dias, R. Fortes, P. Masiero, W. Watanabe, and M. Ramos. An approach to improve the accessibility and usability of existing web system. In *Proceedings of the 31st ACM international conference on Design of communication*, pages 39–48. ACM, 2013.

[39] 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.

[40] M. Egele, T. Scholte, E. Kirda, and C. Kruegel. A survey on automated dynamic malware-analysis techniques and tools. *ACM Computing Surveys (CSUR)*, 44(2):1–42, 2012.

[41] S. Egelman, L. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1065–1074. ACM, 2008.

[42] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:1802.04351*, 2018.

[43] 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.

[44] A. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, pages 3–14. ACM, 2011.

[45] B. Fogg, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, J. Shon, and P. Swani. What makes web sites credible?: a report on a large quantitative study. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 61–68. ACM, 2001.

[46] A. Freire, C. Russo, and R. Fortes. A survey on the accessibility awareness of people involved in web development projects in brazil. In *Proceedings of the 2008 international cross-disciplinary conference on Web accessibility (W4A)*, pages 87–96. ACM, 2008.

[47] M. Friedman and D. Bryen. Web accessibility design recommendations for people with cognitive disabilities. *Technology and Disability*, 19(4):205–212, 2007.

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

[49] G. Gay and C. Li. Achecker: open, interactive, customizable, web accessibility checking. In *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A)*, page 23. ACM, 2010.

[50] United States General Services Administration Federal Government. Section 508 law and related laws and policies. Web, 1973.

[51] VFO Group. Zoomtext magnifier/reader. Web, n.d.

[52] J. Hailpern, L. Guarino-Reid, R. Boardman, and S. Annam. Web 2.0: blind to an accessible new world. In *Proceedings of the 18th international conference on World wide web*, pages 821–830. ACM, 2009.

[53] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144. ACM, 2009.

[54] H. Hochheiser, J. Feng, and J. Lazar. Challenges in universally usable privacy and security. In *Proceedings of The Symposium on Usable Privacy and Security.* USENIX, 2008.

[55] J. Holman, J. Lazar, and J. Feng. Investigating the security-related challenges of blind users on the web. In *Designing Inclusive Futures*, pages 129–138. Springer, 2008.

[56] 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.

[57] Apple Inc. Accessibility. Web, n.d.

[58] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the 11th Symposium On Usable Privacy and Security*, volume 15, pages 1–20, 2015.

[59] 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.

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

[61] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y. Lim. What instills trust? a qualitative study of phishing. In *International Conference on Financial Cryptography and Data Security*, pages 356–361. Springer, 2007.

[62] S. Kane, C. Jayant, J. Wobbrock, and R. Ladner. Freedom to roam: a study of mobile device adoption and accessibility for people with visual and motor disabilities. In *Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 115–122. ACM, 2009.

[63] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. “my data just goes everywhere:” user mental models of the internet and implications for privacy and security. In *Proceedings of The Symposium on Usable Privacy and Security*, pages 39–52. USENIX Association Berkeley, CA, 2015.

[64] P. Kelley, S. Komanduri, M. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Security & Privacy*, pages 523–537. IEEE, 2012.

[65] B. Kelly, D. Sloan, L. Phipps, H. Petrie, and F. Hamilton. Forcing standardization or accommodating diversity?: A framework for applying the WCAG in the real world. In *Proceedings of the International Cross-Disciplinary Conference on Web Accessibility (W4A)*, pages 46–54. ACM, 2005.

[66] I. Kirlappos and M. Sasse. Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2):24–32, 2012.

[67] M. Kliehm. To hell with joe clark. *Learning the World*, 31, 2006.

[68] 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.

[69] J. Lazar, A. Dudley-Sponaugle, and K. Greenidge. Improving web accessibility: a study of webmaster perceptions. *Computers in Human Behavior*, 20(2):269–288, 2004.

[70] J. Lazar, J. Feng, T. Brooks, G. Melamed, B. Wentz, J. Holman, A. Olalere, and N. Ekedebe. The soundsright captcha: An improved approach to audio human interaction proofs for blind users. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 2267–2276. ACM, 2012.

[71] S. Lewthwaite. Web accessibility standards and disability: developing critical perspectives on accessibility. *Disability and Rehabilitation*, 36(16):1375–1383, 2014.

[72] NV Access Limited. What is NVDA? Web, n.d.

[73] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2075–2084. ACM, 2011.

[74] Dolphin Computer Access Ltd. Dolphin supernova magnifier and screen reader. Web, n.d.

[75] 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.

[76] L. Moreno and P. Martinez. Overlapping factors in search engine optimization and web accessibility. *Online Information Review*, 37(4):564–580, 2013.

[77] J. Nielsen and R. Mack. *Usability Inspection Methods*. Wiley, 1994.

[78] J. Nielsen and R. Molich. Heuristic evaluation of user interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 249–256. ACM, 1990.

[79] 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.

[80] Accessibility Ontario. Accessibility for ontarians with disabilities act, n.d.

[81] World Health Organization. Global data on visual impairments, 2012.

[82] K. Pernice, J. Nielsen, S. Farrell, S. Mizobuchi, N. Ishida, U. A. Stover, M. Yohay, E. Franko, and A. Richardson. Usability guidelines for accessible web design. Technical report, Nielsen Norman Group, 2001.

[83] H. Petrie, A. Savva, and C. Power. Towards a unified definition of web accessibility. In *Proceedings of the International Cross-Disciplinary Workshop on Web Accessibility (W4A)*, page 35. ACM, 2015.

[84] 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.

[85] E. Redmiles, S. Kross, and M. 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. ACM, 2016.

[86] 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.

[87] 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.

[88] J. Richards and V. Hanson. Web accessibility: a broader view. In *Proceedings of the 13th international Conference on World Wide Web*, pages 72–79. ACM, 2004.

[89] K. Ringland, C. Wolf, L. Boyd, M. Baldwin, and G. Hayes. Would you be mine: Appropriating minecraft as an assistive technology for youth with autism. In *Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 33–41. ACM, 2016.

[90] 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.

[91] 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.

[92] N. Saxena and J. Watt. Authentication technologies for the blind or visually impaired. In *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec)*, volume 9, page 130, 2009.

[93] S. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators. In *Security & Privacy*, pages 51–65. IEEE, 2007.

[94] Freedom Scientific. Blindness solutions: Jaws. Web, n.d.

[95] H. Sharp, Y. Rogers, and J. Preece. *Interaction Design: Beyond Human-Computer Interaction*, chapter 15 Evaluation: Inspections, Analytics, and Models. Wiley, 2012.

[96] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382. ACM, 2010.

[97] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium On Usable Privacy and Security*, pages 88–99. ACM, 2007.

[98] G. Sonowal and K. Kuppusamy. Masphid: a model to assist screen reader users for detecting phishing sites using aural and visual similarity measures. In *Proceedings of the International Conference on Informatics and Analytics*, page 87. ACM, 2016.

[99] 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.

[100] M. F. Theofanos and J. G. Redish. Bridging the gap: between accessibility and usability. *Interactions*, 10(6):36–51, 2003.

[101] D. Thomas. A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, 27(2):237–246, 2006.

[102] T. Thompson, D. Comden, S. Ferguson, S. Burgstahler, and E. Moore. Seeking predictors of web accessibility in us higher education institutions. *Information Technology and Disabilities*, 13(1):18, 2013.

[103] 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.

[104] W. Watanabe, R. Fortes, and A. Dias. Acceptance tests for validating aria requirements in widgets. *Universal Access in the Information Society*, 16(1):3–27, 2017.

[105] WebAIM. Wave web accessibility evaluation tool. Web, 2001.

[106] B. Wentz, H. Hochheiser, and J. Lazar. A survey of blind users on the usability of email applications. *Universal Access in the Information Society*, 12:327–336, 2013.

[107] T. Whalen and K. Inkpen. Gathering evidence: use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, pages 137–144. Canadian Human-Computer Communications Society, 2005.

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

[109] Graham Wilson, Harry Maxwell, and Mike 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.

[110] S. Wu and L. Adamic. Visually impaired users on an online social network. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 3133–3142. ACM, 2014.

[111] H. Xia and J. Brustoloni. Hardening web browsers against man-in-the-middle and eavesdropping attacks. In *Proceedings of the 14th International Conference on World Wide Web*, pages 489–498. ACM, 2005.

[112] K. Yee. Aligning security and usability. *IEEE Security & Privacy*, 2(5):48–55, 2004.

[113] Y. Yesilada, G. Brajnik, and S. Harper. How much does expertise matter?: a barrier walkthrough study with experts and non-experts. In *Proceedings of the 11th International ACM SIGACCESS conference on Computers and accessibility*, pages 203–210. ACM, 2009.

[114] Y. Yesilada, G. Brajnik, M. Vigo, and S. Harper. Understanding web accessibility and its drivers. In *Proceedings of the International Cross-Disciplinary Conference on Web Accessibility (W4A)*, page 19. ACM, 2012.

[115] Y. Yesilada, G. Brajnik, M. Vigo, and S. Harper. Exploring perceptions of web accessibility: a survey approach. *Behaviour & Information Technology*, 34:119–134, 2015.

[116] N. Youngblood and J. Mackiewicz. A usability analysis of municipal government website home pages in alabama. *Government Information Quarterly*, 29(4):582–588, 2012.

[117] N. Zaparyniuk and C. Montgomerie. The status of web accessibility of canadian universities and colleges: A charter of rights and freedoms issue1. *International Journal on ELearning*, 4(2):253, 2005.

[118] N. Zaparyniuk and C. Montgomerie. The status of web accessibility of canadian universities and colleges: A follow-up study 10 years later. In *EdMedia: World Conference on Educational Media and Technology*, pages 2498–2507. Association for the Advancement of Computing in Education (AACE), 2013.

[119] J. L. Zeldman. An angry fix. Web, 2006.

[120] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Password advice shouldn't be boring: Visualizing password guessing attacks. In *eCrime Researchers Summit (eCRS), 2013*, pages 1–11. IEEE, 2013.

Appendix A

ACCUS Literature

A.1 Peer-reviewed Articles

Table A.1 describes the usable security and accessibility literature used to formulate the first iteration of the ACCUS heuristics.

Author(s)	**Year**	**Accessibility**	**Usable Security**	**Number of Excerpts**
Whitten and Tygar [108]	1999		●	5
Yee [112]	2002		●	10
Fogg et al. [45]	2003		●	9
Theofanos and Redish [100]	2003	●		25
Balfanz et al. [14]	2004		●	1
Chiasson et al. [25]	2006		●	3
Jakobsson et al. [61]	2007		●	5
Babu et al. [13]	2009	●		4
Akhert et al. [6]	2009	●	●	2
Nurse et al. [79]	2011		●	16
Kirlappos and Sasse [66]	2012		●	5
Azenkot et al. [12]	2012	●	●	4
Jaferian et al. [59]	2014		●	6
Dias et al. [38]	2014	●		10
Garfinkel and Lipford [48]	2014		●	5
Almuhimedi et al. [7]	2015		●	2
Ion et al. [58]	2015	●	●	2
Kang et al. [63]	2015		●	4
Felt et al. [43]	2015		●	6
Alsharnouby et al. [8]	2015		●	1
Dosono et al. [39]	2015	●	●	3
Abdolrahmani and Kuber [2]	2016	●	●	6
Regal et al. [87]	2016	●	●	15
de Borba Campos and Oliveira [35]	2016	●		3
Reeder et al. [86]	2017		●	2

Appendix B

Recruitment Materials

B.1 Email Invitation

This is an invitation to participate in a study about Web accessibility and usable security.

What is this study about?

This study aims to understand the safety obstacles that people with sight loss may experience while using the Internet. We hope to learn more about the security and privacy implications of these users habits so that we can create advice and web design guidelines to help enhance their safety and privacy while online.

Who is leading this study?

This study is led by Daniela Napoli, a Masters student in the Human-Computer Interaction program at Carleton University. She is working under the supervision of Professor Sonia Chiasson from the School of Computer Science.

Who can participate in this study?

Eligible participants must be: at least 18-years old, visually impaired, comfortable using the Internet, and have familiarity with using screen-reading or screen-magnifying software (such as JAWS, ZoomText, or VoiceOver).

How will this study be conducted?

This study will take approximately 90 minutes to complete. It involves two segments: 1) a 60-minute session to complete tasks online, and 2) a 30-minute interview to collect more information about your security and privacy concerns while surfing the Web.

Where will this study be done?

It will take place at Carleton University or a suitable mutually convenient location, that can include a CNIB site in Ottawa or Toronto.

As appreciation for your involvement, you will be given $50 for your time. We will also reimburse you for your reasonable travel expenses. You are welcome to bring a companion to help guide you to and from the studys location. We will reimburse your companions travel expenses as well.

Do I have to participate?

Your participation is voluntary. If you choose to participate, the data collected from you will be anonymized.

Notice for CNIB clients: Decisions you make around participation will have absolutely no impact on the services you receive from CNIB, either now or in the future. You can end the interview at any time, and you can choose not to answer certain questions. And, of course, there are no consequences to you if you choose not to participate.

Id like to join the study! Who do I contact? If you would like to participate, or have any questions, please contact Daniela through email at daniela.napoli@carleton.ca.

Ethical Clearance

The ethics protocol for this research has been reviewed and approved by the Carleton University Research Ethics Board (CUREB-B Clearance: 108304). If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 extension 4085, or by email at ethics@carleton.ca).

This project was also reviewed by the CNIB's Research Department, which provided approval. If you have any ethical concerns with the study, please contact Dr. Mahadeo Sukhai, Head of Research and Chief Accessibility Officer at CNIB (by phone at 416-486-2500 extension 8668, or by email at mahadeo.sukhai@cnib.ca).

B.2 Facebook Invitation Template

Volunteers needed for web accessibility study!

We are looking for volunteers for a study that explores Web accessibility and security. Participants will receive $50, and their reasonable travel expenses will be reimbursed.

To be eligible to participate, you must have some visual impairment, be comfortable using the Internet, and at least 18 years of age.

The study will take place on campus (or another mutually convenient public location) and should not take more than approximately 90 minutes to complete.

Participants will be asked to complete a few tasks online, complete related questionnaires, and engage in discussion.

If you are interested, or know someone who might be, please email Daniela at daniela.napoli@carleton.ca for more details.

The ethics protocol for this research has been reviewed and approved by the Carleton University Research Ethics Board. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca)

B.3 Twitter Invitation Template

Doing accessibility user study in Ottawa Toronto. Must have some sight loss. Youll get $50 and well cover travel. https://goo.gl/RgRD3c a11y research

Privacy Web accessibility? Lets explore. User study in Ottawa Toronto. DM for more details. a11y research https://goo.gl/RgRD3c

ATTN: screen-readers/magnifiers users. We need your insight! DM for more details about our a11y research. https://goo.gl/RgRD3c

Appendix C

Protocol Script

C.1 Task Protocol Script

In this study you will complete three tasks on a website. You are welcome to complete the tasks as you normally would. Be sure to think-aloud while you are completing each task. Explain to me your thought processes and which short-cuts/gestures you are using. You are free to choose to stop at any time. Are you ready? I will enter the URL for you, now.

Task 1 Introduction: The first task is to verify that the site I've provided is legitimate.

Have you completed the task? *Complete post-task questionnaire.*

Task 2 Introduction: Based on your assessment, would you continue to use this website?
If not, we will move on to the next website. If yes...

- *If on Google Mail or Amazon*, login using the following credentials
- *If on CNIB*, find the page in which you can make a donation to CNIB.

Have you completed the task? *Complete post-task questionnaire.*

Task 3 Introduction: Lastly...

- *If on Google Mail*, download an attachment that I sent to this account.
- *If on Amazon*, I will now put an item in your cart and ask you to check out. You will have to explore the page and complete the purchasing process. Before filling in a field, ask me the information you have to input.
- *If on CNIB*, make a $10 donation using the following credit card information.

Have you completed the task? *Complete post-test questionnaire and interview.*

Appendix D

User Study Questionnaires

D.1 Oral Informed Consent Script

My name is Daniela and I am a Masters student in the Human-Computer Interaction program at Carleton University. I am working under the supervision of Professor Chiasson.

I would like you to participate in a study on Web accessibility and usable security. This study aims to understand the safety obstacles that people with sight loss may experience while using the Internet. Funding for this study was provided by the Ontario eCampus Digital Inclusion Research grant.

This research is beneficial because learning the security and privacy implications of visually impaired users habits can help improve accessibility design guidelines and cyber-security advice for people with sight loss.

This study involves two parts: a 60-minute session to complete tasks online, and a 30-minute interview to collect further information. Both will take place at Carleton University or another public location if necessary. With your consent, the study will be audio-recorded. Once transcribed, the audio-recording will be destroyed.

We do not expect you to face any risks while completing this study. I will take precautions to protect your identity. This will be done by keeping all responses anonymous and allowing you to request that certain responses not be included in the final project.

You may withdraw before we start the session by letting me or my research supervisor know. If you choose to withdraw, all the information you provided thus far will be destroyed. In order to preserve the data we collect, you will not be able to withdraw after participating in the study.

As a token of appreciation, I will provide you with $50.00 to reimburse you for your time. I will reimburse you and your companion (if applicable) for reasonable travel expenses involved in coming to, and leaving from, our study. It is yours to keep, even if you withdraw.

All research data, including audio-recordings and my notes will be stored on an password protected computer and only accessible by me and my supervisor. Some of the questionnaires are hosted by Qualtrics. Your data will be stored and protected by Qualtrics but may be disclosed via a court order or data breach.

Once the project is completed, the research data will be kept for presentations, publications, and future research.

If you would like a copy of the finished research project, please let me know. I will then provide you with an electronic copy.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research (CUREB-B Clearance: 108304). If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

This project was also reviewed by the CNIB's Research Department, which provided approval. If you have any ethical concerns with the study, please contact Dr. Mahadeo Sukhai, Head of Research and Chief Accessibility Officer at CNIB (phone: 416-486-2500 x8668 or by email at mahadeo.sukhai@cnib.ca).

My supervisor and I can provide you with our email address or telephone number if you would like to discuss the study further. Do you have any questions or need clarification?

Do I have your permission to begin:

- Yes
- No. If no, thank them for their time.

Do you agree to be audio-recorded:

- Yes
- No If no, continue with study and rely on observational notes only.

Date:

Participants name/Pseudonym/Initials:
Researchers Signature:

D.2 Pre-testing Questionnaire

For convenience, the user study questionnaires were designed with and hosted on Qualtrics. In order to deter interference during the sessions from potential accessibility or usability issues between the interface and users' assisstive technology, each questionnaire was delivered orally to the participant and the researcher noted their responses on their behalf.

D.2.1 Demographics

1. What is your sex?
   - Male
   - Female
   - Other
2. How old are you?
3. What is the highest level of education you have achieved?
   - Elementary
   - High school
   - College
   - Undergraduate
   - Masters
   - Doctorate
   - Professional Degree
   - Other
4. If applicable, what was your major(s)?

5. What is your current occupation? If unemployed, please note ”N/A.”

6. How limited is your ”visual acuity” (ability to see objects/persons)? Please feel free to elaborate if needed.

   - Very much so
   - Somewhat
   - Not at all

7. How limited is your ”visual field” (the width of area you can see without moving your eyes or head)? Please feel free to elaborate.

   - Very much so
   - Somewhat
   - Not at all

8. How limited is your ”light perception” (ability to see light and gauge brightness)? Please feel free to elaborate.

   - Very much so
   - Somewhat
   - Not at all

9. Would you like to describe your visual abilities further? If so, please explain.

D.2.2 Technology Usage

Note: Although the ordering of questions remained consistent between participants, each option was randomized per session to avoid any pattern that may indirectly bias or influence responses.

1. Rate the frequency in which you use the following types of technology to surf the web:

	Very infrequently	Infrequently	Neither	Frequently	Very frequently
Desktop computer					
Laptop computer					
Tablet					
Smartphone					
eBook reader with built-in browser					
Other (please specify)					

2. What operating system do you use most frequently? (State which version, if known.)

    - Macintosh OS
    - Microsoft Windows
    - Ubuntu
    - Linux
    - Other (please specify)

3. Rate the frequency in which you use the following types of assistive technology to help surf the web:

	Very infrequently	Infrequently	Neither	Frequently	Very frequently
Desktop video magnifier					
Handheld/portable video magnifier					
Screen magnification software					
JAWS screen reading software					
Android VoiceOver					
iOS VoiceOver					
Windows VoiceOver					
Macintosh VoiceOver					
Augmented keyboard					
Augmented computer mouse					
Braille display/computer					
Other (please specify)					

4. Rate the frequency in which you use the following web browsers:

	Very infrequently	Infrequently	Neither	Frequently	Very frequently
Internet Explorer					
Mozilla Firefox					
Google Chrome					
Microsoft Edge					
Safari					
Other (please specify)					

5. Rate the frequency in which you use the following online services:

	Very infrequently	Infrequently	Neither	Frequently	Very frequently
Online banking					
Government services					
Online shopping					
Customer/technical support					
Online education					
Library/informational services					
Social media					
Travel planning					
Basic utility services (e.g. hydro, water, telephone, television, internet)					
Other (please specify)					

6. Some people use specific technology to achieve certain tasks. Describe the technology you use to engage in the following online services:

	Computer with no assistive tools	Computer with built-in accessibility options	Computer with add-on assistive technology	Tablet with no assistive tools	Tablet with built-in accessibility options	Tablet with add-on assistive technology	Smartphone with no assistive tools	Smartphone with built-in accessibility options	Smartphone with add-on assistive technology
Online banking									
Government services									
Online shopping									
Customer/technical support									
Online education									
Library/informational services									
Social media									
Travel planning									
Basic utility services (e.g. hydro, water, telephone, television, internet)									
Other (please specify)									

7. How comfortable are you in completing Web-based tasks with JAWS?

   - Extremely uncomfortable
   - Uncomfortable
   - Neither uncomfortable nor comfortable
   - Comfortable
   - Extremely comfortable

D.3 Post-task Questionnaire

D.3.1 Google Mail website

1. This website is...

   - Legitimate
   - Fake

2. How easy or difficult was it to check the legitimacy of the website?

   - Very difficult
   - Difficult
   - Neither
   - Easy
   - Very easy

3. How confident are you of your assessment?

   - Very unsure
   - Unsure
   - Neither
   - Sure
   - Very sure

4. How easy/difficult was it to log into the website?

    - Very difficult
    - Difficult
    - Neither
    - Easy
    - Very easy

5. How confident are you that you logged in correctly?

    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

6. How easy/difficult was it to download an email attachment?

    - Very difficult
    - Difficult
    - Neither
    - Easy
    - Very easy

7. How confident are you that you completed the task correctly?

    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

8. Overall, how would you rate the website's accessibility?
    - Very inaccessible
    - Inaccessible
    - Neither
    - Accessible
    - Very accessible
9. Overall, how would you rate the website's security?
    - Very insecure
    - Insecure
    - Neither
    - Secure
    - Very secure
10. How does this activity compare to your typical experiences with similar tasks outside of this study?
11. What other steps might you take if you were to complete these tasks in real life?
12. Do you have comments or concerns relating to security, privacy, or accessibility when completing this task?

D.3.2 Amazon website

1. This website is...
    - Legitimate
    - Fake
2. How easy or difficult was it to check the legitimacy of the website?
    - Very difficult

- Difficult
- Neither
- Easy
- Very easy

3. How confident are you of your assessment?
    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

4. How easy/difficult was it to log into the website?
    - Very difficult
    - Difficult
    - Neither
    - Easy
    - Very easy

5. How confident are you that you logged in correctly?
    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

6. How easy/difficult was it to complete your online purchase?
    - Very difficult

- Difficult
- Neither
- Easy
- Very easy

7. How confident are you that you completed the task correctly?

   - Very unsure
   - Unsure
   - Neither
   - Sure
   - Very sure

8. Overall, how would you rate the website's accessibility?

   - Very inaccessible
   - Inaccessible
   - Neither
   - Accessible
   - Very accessible

9. Overall, how would you rate the website's security?

   - Very insecure
   - Insecure
   - Neither
   - Secure
   - Very secure

10. How does this activity compare to your typical experiences with similar tasks outside of this study?

11. What other steps might you take if you were to complete these tasks in real life?

12. Do you have comments or concerns relating to security, privacy, or accessibility when completing this task?

D.3.3 CCNIB website

1. This website is...

   - Legitimate
   - Fake

2. How easy or difficult was it to check the legitimacy of the website?

   - Very difficult
   - Difficult
   - Neither
   - Easy
   - Very easy

3. How confident are you of your assessment?

   - Very unsure
   - Unsure
   - Neither
   - Sure
   - Very sure

4. How easy/difficult was it to log into the website?

   - Very difficult
   - Difficult
   - Neither

- Easy
- Very easy

5. How confident are you that you logged in correctly?

    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

6. How easy/difficult was it to make a donation?

    - Very difficult
    - Difficult
    - Neither
    - Easy
    - Very easy

7. How confident are you that you completed the task correctly?

    - Very unsure
    - Unsure
    - Neither
    - Sure
    - Very sure

8. Overall, how would you rate the website's accessibility?

    - Very inaccessible
    - Inaccessible
    - Neither

- Accessible
- Very accessible

9. Overall, how would you rate the website's security?
    - Very insecure
    - Insecure
    - Neither
    - Secure
    - Very secure

10. How does this activity compare to your typical experiences with similar tasks outside of this study?

11. What other steps might you take if you were to complete these tasks in real life?

12. Do you have comments or concerns relating to security, privacy, or accessibility when completing this task?

D.4 Post-test Questionnaire & Semi-structured Interview

D.4.1 Ranking Protective Actions

Note: Although the ordering of questions remained consistent between participants, each option was randomized per session to avoid any pattern that may indirectly bias or influence responses.

1. Rate your level of concern with the following digital threats:

	Very unconcerned	Unconcerned	Neither	Concerned	Very concerned
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 tracking your online activities					
Someone hacking into 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					

2. What are your top 3 methods in ensuring your safety online?

3. What are your top 3 most frustrating obstacles in ensuring your safety online?

4. Rate the effectiveness of the following protective actions:

	Very unconcerned	Unconcerned	Neither	Concerned	Very concerned
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-factors authentication methods					
Use a password manager					
Only use websites that include ”HTTPS” in the URL address					
Think before you click a link					
Do not open unexpected attachments					

5. Rate the likelihood of you taking the following protective actions:

	Very unlikely	Unlikely	Neither	Likely	Very likely
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-factors authentication methods					
Use a password manager					
Only use websites that include ”HTTPS” in the URL address					
Think before you click a link					
Do not open unexpected attachments					

D.4.2 Interview Questions

I noticed you encountered an obstacle when completing...

1. Can you tell me more about what happened?

2. What do you think caused this issue?

3. How did this problem affect your mood?

4. How do you think this problem affected your security/privacy?

   Note: Repeat this set of question for each major obstacle if time permits.

5. How often do you consider your personal security/privacy when surfing the Web?

   - Very infrequently
   - Infrequently
   - Neutral
   - Frequently
   - Very frequently

6. What are your most pressing concerns when browsing online? (If any)

7. How safe do you usually feel when offering sensitive information online?

   - Very infrequently
   - Infrequently
   - Neutral
   - Frequently
   - Very frequently

8. What makes you feel safe online?