A RESEARCH FRAMEWORK AND INITIAL STUDY OF BROWSER SECURITY FOR THE VISUALLY IMPAIRED

A Thesis

presented to

the Faculty of California Polytechnic State University,

San Luis Obispo

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

Elaine Lau

May 2022

COMMITTEE MEMBERSHIP

TITLE: A Research Framework and Initial Study of Browser Security for the Visually Impaired

AUTHOR: Elaine Lau

DATE SUBMITTED: May 2022

COMMITTEE CHAIR: Zachary Peterson, Ph.D.
Professor of Computer Science

COMMITTEE MEMBER: Franz Kurfess, Ph.D.
Professor of Computer Science

COMMITTEE MEMBER: Bruce DeBruhl, Ph.D.
Professor of Computer Science

ABSTRACT

A Research Framework and Initial Study of
Browser Security for the Visually Impaired

Elaine Lau

The growth of web-based malware and phishing attacks has catalyzed significant advances in the research and use of interstitial warning pages and modals by a browser prior to loading the content of a suspect site. These warnings commonly use visual cues to attract users' attention, including specialized iconography, color, and an absence of buttons to communicate the importance of the scenario. While the efficacy of visual techniques has improved safety for sighted users, these techniques are unsuitable for blind and visually impaired users. This is likely not due to a lack of interest or technical capability by browser manufactures, where universal design is a core tenet of their engineering practices, but instead a reflection of the very real dearth of research literature to inform best practices, exacerbated by a deficit of clear methodologies for conducting studies with this population.

Indeed, the challenges are manifold. In this paper, we present the results of our study analyzing the experiences of the visually impaired with browser security warnings, detail the development and advancement of the methodological best practices when conducting a study of this kind, and ultimately identify some initial approaches that could improve the security for this population.

ACKNOWLEDGMENTS

My deepest gratitude to:

- Dr. Zachary Peterson, for being the best advisor and mentor throughout the years. I am very thankful for your unwavering patience and constant positive affirmations that always kept me going.
- Dr. Franz Kurfess and Dr. Bruce DeBruhl, for staying on my committee for so long and taking an interest in my thesis.
- Dr. Erika Rogers, for offering me helpful guidance whenever I needed it, even long after your Thesis Clinic ended.
- My parents for making this possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

The increasing prevalence of web-based malware and phishing attempts [4, 45] has necessitated significant advances in the client-side detection of such attacks. It is now common for web browsers to display an interstitial warning page prior to loading the content of a suspect site. Following W3C user interface guidelines, warnings should provide distinct options for how to proceed and a recommended course of action [66]. Specifically, the user can decide to either adhere to the warning and return to safety, or ignore the warning and proceed with her original task [2].

Commonly, warnings use visual cues to capture the user's attention and make the "safe" option more attractive. Desolda *et al.* observe that the primary differences in the interstitial security warnings in major browsers are visual in nature; these include background color, the alert icon, the message text, and the placement and size of the button for proceeding through the warning [20]. Bravo *et al.* detail a mental model of warning response behaviors for advanced and novice users, and found that novice users immediately pay attention to the look and feel of the warning [10]. In a set of research-based guidelines for warning design, Wogalter *et al.* identify salience as the first requirement for an effective warning, which is achieved by using bold type, adding color, thick borders, pictorial symbols, and special effects [80]. Similarly, Bauer *et al.* suggest a common visual layout for structuring information in a warning, which includes a single icon that conveys the severity level of a message [7]. In a study of Google Chrome's SSL warning, Felt *et al.* attribute a dramatic improvement of adherence rates to the use of opinionated design, applying visual design techniques to promote a recommended course of action [23].

While the efficacy of visual techniques has promoted safety for sighted users, these techniques may be unsuitable to blind and visually impaired users. Many visually impaired users browse the web with a screen reader, which converts text on the computer screen to synthesized speech [37]. Such assistive technologies can make websites technically *accessible* but not necessarily *usable*, leading screen reader users to employ different browsing strategies to cope with usability problems [9]. Indeed, the challenge of communicating security cues to this population is not unique to web browser warnings [37]. Hochheiser *et al.* note that graphical passwords, icons, images, and pop-up dialogs are often not interpreted by screen reader software [35, 37]. Further, screen readers cannot read image-based CAPTCHAs, which the W3C has identified as a major problem for blind and visually impaired users [52].

The World Wide Web Consortium (W3C) Web Security Context Working Group (WSC) is the first standards effort in the area of usable security to provide guidelines for presenting security-related information to end users [66] with accessibility as a top concern. For example, Zurko and Johar discuss possible additions to WSC recommendations, including the use of aural interfaces in warning design [86].

The W3C Web Accessibility Initiative (WAI) also provides the Web Content Accessibility Guidelines (WCAGs), which are internationally regarded as the standard for web accessibility. Petrie and Khier asked blind, screen reader users to rate the importance of usability problems on a website and found little relationship between the participants' ratings and the priority levels assigned to problems in version 1.0 of the WCAG [61]. The match between actual problem severity and priority levels in the latest version of these guidelines (WCAG 2.0) was also shown to lack empirical basis when Romen and Svanes tested the usefulness of WCAG 2.0 as a heuristic for web accessibility with a broader population of users with disabilities. Visually impaired users, in particular, reported problems with redundant and indistinguishable links

that the WCAG 2.0 does not address [65]. Their study suggests that conformance to guidelines may not guarantee accessibility for all, and that there is potential for improvement through more detailed research into how users with disabilities interact with the web.

While existing research repeatedly illustrates the need to evaluate browser security warnings for users with visual impairments, very few concrete solutions or paths forward exist. This may not be, exclusively, a reflection of poor technologies or researcher disinterest, but rather indicative of a more fundamental challenge in conducting usable security research with this specific population. As evidence, we have not found any work related to appropriate research methodologies to use, nor the "right" questions to ask, in such an evaluation. Challenges include ensuring ecological validity, providing an accurate account of experiences with respect to the vast variability in browser security warnings and personal computer set ups, and participant recruitment—all research challenges that are not unique to the visually impaired population, but require more consideration when conducting research of this kind.

In short, there is a gap in the literature with regards to how users with visual disabilities experience web browser security warnings, generally. Our work aims to fill this gap.

The contributions of this thesis are threefold: (1) we investigate how individuals with visual disabilities perceive and interact with web browsers' security warnings and indicators, in an authentic setting, while also undertaking an inclusive security and privacy research perspective that captures visually impaired users' security experiences more broadly; (2) we reflect on the methodical challenges of conducting browser security warning research with visually impaired users, and advance the state of the art in conducting research with this population; and (3) we draw upon our empirical results to suggest some rudimentary technical solutions that may substantially improve the

security and usability of the web for visually impaired users. A long-term goal of this study is to contribute toward conceptualizing and designing inclusive security research methodologies and mechanisms with the needs and concerns of marginalized populations in mind.

Chapter 2

RELATED WORK

To the best of our knowledge, there are no studies that investigate browser security warnings with users who are visually impaired. However, there have been several studies over the past decade on the evolution of browser security warning effectiveness. Although our study is not squarely focused on testing browser security warning effectiveness with users who are visually impaired *per se*, prior work has guided us in asking our subjects important questions about their experience with generally accepted criterion for successful warnings. Beyond browser security warnings specifically, there have been numerous studies investigating other security and privacy mechanisms, behaviors, and concerns with users who are visually impaired. In this section, we provide an overview of these works that inform our approach.

2.1 Browser Security Warnings Research

Akhawe and Felt performed the first large-scale field study of user decisions upon encountering three types of browser security warnings in Google Chrome and Mozilla Firefox: malware, phishing, and SSL warnings [2]. All three of these warnings are full-page, interstitial warnings that caution the user against proceeding to the next page. Both Chrome and Firefox display malware and phishing warnings when a website is identified as unsafe by the Google Safe Browsing List. SSL warnings appear in the event of a man-in-the-middle attack, as well as benign scenarios, such as server misconfigurations, since the browser often cannot distinguish between the two. Although all three types of warnings have a potential for false positives, low

click-through rates close to 0% were ideal, as this indicates that users observe and heed the warnings. In order to measure click-through rate, *i.e.* the rate at which users bypass a warning, Akhawe and Felt used the browsers' telemetry frameworks to collect pseudonymous data from users unobtrusively. Akhawe and Felt observed that Mozilla Firefox users clicked through all three types of browser warnings at a lower rate than Google Chrome users, and cited warning appearance as a possible, but not sole explanation. For example, they noted that the SSL warning in Mozilla Firefox displayed an image of a policeman and the word "untrusted" in the title—a frightening design that may have lead to a lower click-through rate. In our study, we focused on the same three types of browser security warnings and were also interested in what factors might influence a user who is visually impaired to bypass a warning, and how they might go about it. However, we were less interested in the rates at which our participants bypassed a warning, but the steps in which the user would need to take to either bypass or adhere to a warning using their assistive technologies, in addition to the unique factors that would lead them to doing so.

There have also been studies examining the effectiveness of one type of browser security warning as they evolve in their design. When browsers evolved from using passive phishing indicators to full-page interstitial phishing warnings that forced the user to take notice, Egelman *et al.* performed an empirical study examining their effectiveness [22]. The researchers recommended that an effective phishing warning design must interrupt the primary task, provide clear options on how to proceed, fail safely, prevent habituation, and draw the user away from trusting the phishing website. These recommendations provide important context for our study, in which we interview users who are visually impaired about their interaction with a phishing warning example. It is unclear whether phishing warnings meet these recommendations when they are accessed via assistive technologies, such as screen readers. Through semi-structured task-based interviews, we sought to understand how visually impaired users process

the information in browser security warnings using their assistive technologies. We believe this is an important step towards evaluating warning effectiveness with this population and potentially identifying the elements of a universally effective warning design.

Browser security warning effectiveness is also affected by a user's trust in whether a warning is genuine. Bravo *et al.* interviewed advanced and novice users about their reactions to computer security warnings and observe that both novice and advanced users made security judgments based on whether a warning appeared authentic [10], aligning with other studies' findings that the look and feel of a website is often the most significant factor in gaining user trust [82, 25]. When one of the novice participants in their study was presented with an SSL certificate warning when accessing a bank website, he said about the warning, "*I guess the message looks authentic in terms of just the design, the icon used, and the font and the text and the gradient for the bar up top.*" Novice users cited appearance as a reason to trust a warning, whereas for advanced users, appearance was a reason not to trust a warning. It is unclear how visually impaired users make security judgments when encountering warnings, for example, if and how they determine authenticity or trustworthiness. In our study, we ask open-ended questions in our semi-structured interviews to gain insight about the non-visual factors by which visually impaired users make security judgments, such as authenticity and trustworthiness, and whether these factors are considered in the decision to bypass or adhere to a warning.

Other studies on browser security warning effectiveness also provided guidance for our research design. Sotirakopoulos *et al.* use an experimental study design to investigate SSL warning effectiveness and learn about participants' reactions to SSL warnings in general [69]. The authors make important recommendations to consider regarding the impact of the study environment when observing user behavior and reactions. Due

to a number of the study participants reporting that they ignored a warning either because they trusted the researchers to provide a safe environment to complete the task, or simply because they wanted to complete the task, the authors suggest moving away from laboratory studies towards field studies when the usable security research is focused on user practices and behavior. This is because the lab environment may provide the user with high conviction that it is a safe environment and would therefore not always yield true reactions to the warning, even when the purpose of the study is concealed. Studies taking place in a setting that is natural and not artificial can yield more accurate findings. Given these recommendations, we decided not to simulate real threats in a lab environment nor conceal the purpose of the study. Our study design employs task-based interviews, not to test their true reaction to a warning, but to ask the participants directly about their reactions and *reasoning* about their reactions to an example of a warning, as Sotirakopoulos. We hypothesize that their research design recommendations would be appropriate, if not crucial, in our study with users who are visually impaired, given that there is potential for resentment or embarrassment when the study design is not transparent to the participants.

2.2 Experiencing the Web via Screen Reader

There is a body of literature outlining the accessibility and usability issues that visually impaired users encounter while browsing the web, along with the navigation strategies they employ with their assistive software in various contexts. Lazar *et al.* found that one of the leading causes of frustration of 100 blind users was confusing screen reader feedback due to the page layout [48]. Screen reader users develop their favorite strategies for web browsing, based on their individual preferences or on the task they are trying to accomplish [8]. Vigo and Harper identified seventeen strategies that screen reader users employ to overcome situations of uncertainty, reduced

mobility, confusion, and information overload, and we discuss a few of them below [76]. While these studies explore navigation strategies in more common website scenarios such as online shopping, they provide a strong foundation for understanding the possible interactions that might occur and mental models formed when visually impaired users encounter browser security warnings.

Theofanos and Redish interview sixteen blind users as they navigated websites using a screen reader and observed that just as sighted users do not read every word, most blind users do not listen to every word on a web page. Instead, they "scan" a website with their ears by listening at a high speed and rapidly explore the page by jumping directly to headings and links through heading lists or link lists provided by the screen reader [72]. These strategies are known as *previewing* or *probing* a web page [76]. Similarly, Buzzi *et al.* examine how blind users interact with an e-commerce website via screen reader and observed that they will often stop the screen reader at the beginning of the page in favor of jumping to different portions of the page either link by link using the tab key, or row by row using arrow keys [13]. Blind users will often employ *gambling scanning* in this fashion until they encounter desired content, and thereafter will navigate sequentially [76].

Takagi *et al.* investigate blind users' behaviors while navigating online shopping websites and found that blind users strongly rely on scanning for "landmarks"[1] on a page rather than logical navigation [71]. For example, the "add to cart" button on a product page can be a landmark for efficiently accessing the product price, when the user knows that the price element typically precedes the button [8]. Screen reader users have also been found to remember the amount of content that needs to be skipped to reach their desired content on websites that they frequent [76].

[1] A *landmark* is an element or fragment of a page that can serve as a point of reference, such as a link, button, or a main content area.

It could be said that warning habituation, the tendency of a user to ignore a warning after having seen it and interacted with it multiple times [22], is a concern with visually impaired users just as it is for sighted users. The navigation strategies that blind users employ for accomplishing a task, including remembering landmarks and jumping to desired sections of a web page, could lead the user to easily bypass a warning without accessing important information about the warning. However, context-independent and self-explanatory links, content, and buttons on browser security warnings can help with the loss of context that blind users face when probing a web page [13].

The fact that blind users do not perceive the overall contents of a web page at once may present challenges, but can also potentially have benefits when it comes to browser security warnings. Sighted users can easily connect objects and text on a page that are meant to be displayed in proximity, while blind users navigate linearly, one line at a time and one word at a time [48]. Navigation through the page by listening to content in a sequential fashion, a tactic known as *exhaustive scanning* [76] could be frustrating on websites that are more complicated such as shopping or banking websites. However, this navigation strategy could possibly be helpful if the warning page has a well defined structure in which there is no confusion between objects and neighboring text, and the user does not skip any important elements, because all of the important warning information would be conveyed to the user. In our study, we observe visually impaired users encounter examples of warnings to gain clues to whether visually impaired users are more likely to adopt exhaustive scanning, gambling scanning, landmarks, or other strategies when encountering browser security warnings and their possible implications for warning compliance.

The screen reader also narrates structural elements of the page alongside meaningful content; for example, descriptions of elements such as decorative bullets may or may

not add meaning while requiring additional cognitive effort to interpret. Images such as icons and logos often have excessively lengthy descriptions which disrupt the flow of information [27]. When navigating through site content and meta information, visually impaired users have to split their cognitive energy in three ways between interpreting the website contents, screen reader, and browser. Theofanos and Redish describe the experience as akin to always being inside a help system in which the user must pay attention to both their task as well as the system that is assisting them [72]. This information overload often ends up being very time consuming, and in the context of browser security warnings, it could be detrimental for warning compliance. However, the structure of warning pages is typically simpler than other websites such as online shopping websites, with only one or two links for proceeding to the next page, or returning to safety, so it is not certain that information overload is an issue that occurs when browser security warnings are interpreted via screen reader. Given these unknowns, our study aims to gain insight into the issues that are present and the navigation strategies employed when visually impaired users encounter browser security warnings.

Vigo and Harper's work challenging information foraging theory, which assumes that user behavior on the web is driven by the need for foraging for information, found that problematic situations can play a role in navigation strategies. In problematic situations, screen reader users employ navigation tactics to escape from the situation, rather than pursue their goal. For example, in scenarios of confusion or reduced mobility, screen reader users were found to employ tactics of backtracking to a shelter[2], re-checking whether the link they clicked was a good choice, re-tracing the steps that led to their problem, or giving up [75]. Encountering browser security warnings could involve the use of some of these tactics, since browser security warnings cause

[2]A *shelter* is a familiar web page that does not challenge the user or cause any problems.

problematic situations such as confusion and stopping the user from their original task. In our study, we leverage Vigo and Harper's discovery of web navigation models employed by screen reader users in problematic situations to better understand how they might interact with browser security warnings.

2.3 Web Security and Privacy Research with Visually Impaired Users

There have been few studies investigating the privacy and security experiences of users with visual impairments. Of those studies that have been conducted, most document the most common security and privacy related concerns and challenges that visually impaired users encounter on the web [37, 1, 39, 56], while others evaluate specific security mechanisms or behaviors for users with visual disabilities, such as audio-based CAPTCHAs and other authentication experiences [21, 49]. In contrast, we document visually impaired users' experiences with browser warnings, of which there are currently no studies. We have gleaned methodological approaches from these prior works, especially the work focusing on documenting their experiences of interacting with a specific security mechanism, and incorporate them into our study methods. We discuss these approaches in the following sections.

2.3.1 Contextual Inquiry

Dosono *et al.* examine visually impaired users' experiences with authentication mechanisms using a contextual inquiry approach, asking participants to perform a set of five common authentication scenarios and encourage them to think aloud while completing the tasks. There are three main facets of contextual inquiry: (1) data is collected in the context of the user performing real tasks, (2) the researcher and participant form a partnership for exploring issues together, and (3) the inquiry focuses

on a set of concerns with the flexibility of following promising directions [63]. This enables researchers to form a complex picture of the participant's in-the-moment experience, including opinions and insight into their everyday experience with the specific task. For example, while completing the task of logging into their email account, one participant voiced their frustration with locating the authentication area and said "*unfortunately, this is somethin' that we run into a lot, is, you don't know what they call things, and every time they update the website, you have to re-learn how to do it*" [21]. In our study, we adopt contextual inquiry as a methodology in order to focus on visually impaired users' potential issues and concerns when navigating browser security warnings. Similarly, we conduct a task-based semi-structured interview and ask participants to think aloud while navigating examples of browser security warnings, while allowing room for further conversation about concerns and issues.

2.3.2 Questionnaires

Contextual inquiry has often been used in conjunction with questionnaires. Napoli *et al.* investigate visually impaired users' real world privacy and security concerns with three phases of data collection; a demographic pre-test, task-based observation, and questionnaires with semi-structured interviews [56]. An initial questionnaire or interview at the beginning of a study involving users with visual impairments helps to inform the subsequent parts of the research protocol, as it can be used to identify key demographic information about the participants, explore issues and concerns for further investigation, and for informing the researcher of a participant's technology setup, including any preferences for assistive technology. Hayes *et al.* study how people with visual impairments work closely with allies in privacy and security contexts, and include an initial interview asking participants to describe their daily life and

demographics, as well as general experiences with the Internet and computers. The visually impaired users' allies provide additional information about the tasks that they assist with in the initial interview [33]. Ahmed *et al.* employ a questionnaire asking visually impaired users to provide background information, including their use of assistive technologies and level of assistance needed in privacy and security contexts. The questionnaire is modified as needed when new concepts are identified from early participants. For example, early participants in this study reported privacy concerns about medical records, and a question about this was later added to the questionnaire [1]. These studies demonstrate that questionnaires have been useful for providing relevant background and context. Similarly, we ask participants to complete an initial questionnaire about their computer setup; specifically, the browser, operating system, and assistive technologies that they typically use.

A questionnaire is also an avenue for screening potential participants based on variables of interest. At a minimum, Gerber advises organizing groups of blind or visually impaired participants based on three factors: (1) "whether they use visual (*i.e.* screen magnification) or non-visual means (*i.e.* screen readers) to access the web", (2) level of computer experience or use of the web, and (3) language and literacy [29]. In our study questionnaire, we include questions regarding these three variables in order to be informed and prepared.

2.3.3 Study Environment

Prior studies in this domain either involve participants in their natural environments or provide specific computer setups. In a study of visually impaired users' authentication experiences, Dosono *et al.* assess participants in the typical settings where they regularly use their devices; *e.g.* their home, workplace, or public library. The participants had the option of skipping any of the authentication tasks if they did

not feel comfortable performing them. The researchers protected the study subjects' privacy while recording video by turning the camera focus away when they entered their credentials [21]. In their task-based observations of visually impaired users' privacy behaviors, Napoli *et al.* offered participants two technological setups: a desktop computer with JAWS and ZoomText, or an iPad with accessibility features, with the option of using their own devices and tools such as a physical magnifying glass [56]. A predetermined setup runs the risk of the participant not being as familiar with the provided tools as they would be with their own devices, and thus may not interact the same way as they would normally. In our study, we ask participants to navigate examples of browser security warnings with their own computer setup, so that they are not limited to a predetermined setup and the concerns that go with them. We offered to travel to participants' homes or workplaces, ensuring their comfort with either option. As Dosono, we ensure privacy by not capturing on video any sensitive tasks, such as authentication. However, besides logging into their own computer, participants did not need to use their own credentials for any of the tasks involved.

Previous studies that focus on *visual* elements in warnings have maintained ecological validity due to the foundational work in conducting experiments in human-computer interaction, which often rely on the visual representation of a user interface. For example, Sunshine *et al.* include screenshots in an online survey to examine users' perceptions of SSL warnings [70] and Almuhidemi *et al.* display screenshots in an online survey with Amazon Mechanical Turk to investigate why users ignore malware warnings [3]. This approach of distributing surveys online that display the image of a warning is suitable with sighted users because viewing the image of a warning closely matches the way in which the user would encounter the actual warning. However, depending on the assistive technologies used, an image of a warning does not resemble how screen reader users would encounter the warning. In contrast to previous studies, we met subjects in person, in order to observe how a warning page, when rendered as

HTML, was consumed via the specific assistive technologies that participants use on a daily basis. We adopted an approach that we believe better simulates the warning scenario with visually impaired users.

Gathering data in a natural setting in which visually impaired participants interact with the warnings in their typical context is essential to this work. In a study of how SSL warnings affect user behavior during tasks, Sunshine *et al.* ask participants to interact with the warning on a laptop with a virtual machine provided in a laboratory environment to ensure that the browser and operating system settings were exactly the same [70]. This setup may be suitable for non-sighted users if the necessary assistive technology for the user is also provided. However, current assistive technologies are expensive, and people with disabilities often have highly personalized computer setups [32]. Users might utilize a combination of assistive technologies and switch among them for different tasks. The assistive technology and the user's level of proficiency can have a large impact on how the user interacts with a product [34]. In our study, we conducted interviews in an environment that best matches that in which participants experience warnings (and, thus avoiding inaccuracies in results due to potential differences in computer setup, assistive technologies, and settings that a lab computer might have). We traveled to the participant's home or work environment to observe their interaction with warnings using the browser, operating system, and computer that typically use.

The vast variability in browser security warnings by browser also presents a challenge in developing a research protocol that can be used with every participant consistently. Warnings differ across browsers and browser versions, and the page layout of one type of warning may not be the same as a different warning type in the same browser. For example, the page hierarchy of the malware warning is different from the SSL warning in the same browser in Internet Explorer 9+ and Safari. Furthermore, browsers do

not have the same level of screen reader accessibility, as each browser has their own Accessibility API that is queried by screen readers [51]. Internet Explorer 9+ includes a feature called SmartScreen Filter that must be activated for certain warnings to be available. In our study, we noted which warnings would be applicable to the user based on the browser that they typically use, and prepared the tasks for the in-person task-based interview accordingly. We developed a research protocol that anticipates the potential variety of computer and assistive technology setup, and which also accounts for the variability of warnings.

Chapter 3

METHODOLOGY

3.1 Research Design

3.1.1 Generic Qualitative Inquiry

To understand visually impaired users' experiences of interacting with web browser security warnings, we adopted a generic qualitative approach. Qualitative research is an investigative process with the intent of understanding a particular situation or interaction, focusing on participants' perceptions and experiences [19]. Percy *et al.* describe a generic qualitative research approach that is used to explore people's attitudes, opinions, and beliefs about a particular experience, and examines the content of what participants report about their experiences. This generic approach differs from a more focused, phenomenological qualitative inquiry that studies a participant's cognitive processing and captures their psychological experience [60]. While phenomenology explores the participant's inward process during a task, a generic approach investigates what occurred in the outer world [60]. We sought to discover the opinions, attitudes, and beliefs towards browser security warnings through participants' own reflections about their interactions with the warnings, and was less focused on the structure of their inner experiences. This work was thus guided by an open-ended, exploratory research question using a generic qualitative inquiry approach.

Table 3.1: Website sources that represent an example of each warning type, for each browser that the examples were identified for.

Browser	Warning Example Source URL
Phishing	
Safari	http://phishing.safebrowsingtest.com/
IE 9+	None (same as Malware Warning)
Malware	
Chrome	http://malware.testing.google.test/testing/malware
IE 9+	http://malvertising.info
Safari, Firefox	http://itisatrap.org/firefox/its-an-attack.html
SSL	
Safari, IE 9+	https://expired.badssl.com

3.1.2 Warning Types

We focus on three types of warnings, as did Akhawe and Felt in the first large-scale field study of browser security warning effectiveness: phishing, malware, and SSL warnings [2]. Browsers display a full page interstitial warning when the user is attempting to visit a website that is found on a blacklist of reported phishing or malware sites, or when there may be a problem with a website's security certificate. Google Chrome and Mozilla Firefox check websites against the Google Safe Browsing List, while Internet Explorer 9+ checks websites against the Microsoft SmartScreen Filter for phishing and malware sites. At the time this study was conducted, Internet Explorer 9+ browsers were showing the same warning for both phishing and malware sites. Apple Safari, Google Chrome, and Mozilla Firefox had separate warnings for each of the three types of warnings. For each type of warning, we identified a website that served to represent an example of the warning, that users could navigate to and interact with without any real security threat. See Table 3.1 for the website sources of warnings that were used as examples for each type of warning and browser.

3.2 Participant Recruitment

Our participant criteria aligns with Gerber's three recommended screening variables for research with blind and visually impaired users [29]. First, while we did not ask participants to document their level of vision loss as Gerber suggests, we recruited individuals who were considered to be "blind or visually impaired" by themselves and their organization. We decided to focus on individuals who use a screen reader to access the web non-visually, as The Disability Rights Commission has reported that blind screen reader users encounter the most difficulties on the Web compared to non-disabled users [17]. Second, we recruited individuals who had current access to the internet on their own browser and computer, either at their home or work place. Third, all potential participants were presumed to be English-speaking and literate.

From August 2015 through October 2015, we recruited potential participants by contacting and forming a relationship with service organizations throughout California that provide resources to people who have visual disabilities, as well as the Accessibility team at a technology company. We also reached out to potential candidates by utilizing a mailing list maintained by our university that includes individuals who have visual disabilities, and by word of mouth.

The invitation to participate was an email message along with a link to a questionnaire for individuals who satisfied the participation criteria (Appendix A). The questionnaire includes questions regarding demographics, computer profile, and web security perceptions. At the end of the questionnaire, the respondent was asked to provide their preferred method of contact and contact information if they agreed to participate in an in-person interview.

We arranged in-person interviews with interested respondents on a rolling basis. Prior to the interview, we requested that the participant have access to a computer and screen reader they frequently use, and the address of their preferred meeting location. We offered to travel to their preferred location. We did not provide monetary incentives.

3.3 Data Collection

Our study underwent a full review process and was approved by our University's Institutional Review Board (IRB). As did similar studies [1, 56, 21], our data collection consisted of multiple phases. The first was an electronic questionnaire delivered to potential participants upon receiving electronic informed consent, and the second was a task-based contextual interview with each individual who chose to participate. We were prepared for the in-person interview by using a questionnaire, by becoming aware of the computer setup and warning types that were applicable to the participant, as well as any additional questions or comments that the participant wanted to discuss. The full research protocol and artifacts can be found in Appendices A, B, and C.

3.3.1 Phase 1: Questionnaire

The questionnaire was hosted on the Section 508-compliant website SurveyMonkey, which ensures user-friendliness with screen readers. Section 508 is a United States federal law that requires that Federal agencies' electronic and information technology is accessible to people with disabilities. The University Human Subjects Committee reviewed and approved our informed consent form (See Appendix B.1). The informed consent document on the first page of the questionnaire disclosed the purpose and procedure of the study, reported minimal risk to the participant, cited potential ben-

efits, and provided the option to exit the questionnaire or continue to the questions. These elements of the informed consent were in accordance with non-deceptive user research [18]. This study did not pose any real threats to users' data since participants did not have to install new software or undergo an attack to navigate to canonical warnings in their browser. We noted in the informed consent form as well as the in-person interview the potential benefits for participants. Benefits included an increased understanding of how accessible and usable browser security warnings are via screen reader, which can lead to potential improvements to the design of browser security warnings in the future. At the expense of ecological validity, we opted for full disclosure to be able to have an open discussion with participants about the warnings.

The questionnaire asked respondents what browser, operating system, and screen reader they typically use. Also included were questions about demographics, screen reader proficiency and customization, and perceptions of web security. These questions and options were drawn from the Web Accessibility In Mind (WebAIM) Screen Reader User Survey, an annual survey of screen reader user preferences [40]. Lastly, the questionnaire includes a field for the preferred method of contact for the respondent to indicate whether they would agree to participate in an in-person interview. The informed consent form helped us to prepare for the follow up interview. See Appendix B for our informed consent form and the complete list of questions.

3.3.2 Phase 2: Contextual Inquiry

To recreate the user's working conditions for the in person task-based interview, we adopted a contextual inquiry approach to qualitative research, a research design commonly used to learn what is important to users in the context of their own environment [64]. The interviews were conducted in a natural setting, as is common with qualitative data collection techniques employed in inclusive privacy and security

research, in order to focus on participants' experiences in their typical work or home settings where they regularly use their devices [19].

For each of the three warning types, we leveraged existing websites that served to represent an example of the warning in a specific browser. By accessing an example of a warning, the user could navigate to and interact with a warning without the website posing any real risk to the user. Table 3.1 lists the website source URLs of the examples for each warning type and browser that was tested.

See Appendix E for screenshots of the example warning pages or popup that participants interacted with. We set up an appointment with each participant and traveled to their preferred location for the in-person interview. All of the participants in this study preferred to conduct the interview at their home. We began the in-person contextual interview by disclosing the purpose of the study, and reminding the participant that they may choose to end the study at any time, for any reason. Participants were tasked with navigating to each warning type that was available as a canonical example in the browser that they use. These tasks were chosen to minimize the task duration and necessary steps, while also covering the applicable types of warnings available from the browser, in a way that would also pose no real danger to the participant. A full chronological description of events that occurred during the in-person interview is included in Appendix C.2.

Potential power imbalances that are present in any user research study deserve extra attention in studies with participants who have visual impairments. We encouraged the participant to think aloud about what they were doing and their reasoning in reaction to a warning, acknowledging the participant as the "master" and ourselves as the "apprentice." We communicated our understanding of what participants reported back to the participant throughout the interview, in order to check for the accuracy

of our immediate interpretations. This ensured that the participant was playing an active role in the research findings, as is best practice [18].

Our semi-structured interview approach leveraged a series of open-ended questions to ask about the participant's reaction, whether they have encountered the warning before, the steps that are necessary to bypass a warning or return to the previous page, and whether the participant had suggestions for improving these interactions or the available information on the warning page. We took notes during the in-person meeting labeled with a unique ID number assigned to the participant. We asked for and were granted permission to capture each participant's computer screen and keyboard during the interview, in order to document what was happening on the computer screen in case there was a mismatch with the participant's experience of the warning. Interviewing and observing participants navigating one warning type took approximately 10 minutes, making each session with a participant approximately 10 to 30 minutes depending on the warning types available to be tested.

3.3.2.1 Phishing Warning Scenario

In the phishing warning scenario, participants were asked to view an example of a phishing e-mail, by logging into an e-mail account with credentials provided, that contained one single unread e-mail. The contents of the phishing email were sourced from an example of a common phishing email provided by Cornell University's Phish Bowl website, a repository of common phishing emails targeting Cornell University students and staff [74]. The participant was informed that the phishing email example demonstrates a common phishing scenario that would lead to the browser's phishing warning page, if detected. The phishing warning scenario was not conducted for Internet Explorer users because at the time of this study, there was not a separate phishing warning from the malware warning in Internet Explorer.

3.3.2.2 Malware Warning Scenario

To minimize task duration, participants were asked to navigate directly to the example of a malware warning. We instructed the participant to navigate to the website by reading the URL aloud to the participant.

3.3.2.3 SSL Warning Scenario

To minimize task duration, participants were asked to navigate directly to the example of an SSL warning. We instructed the participant to navigate to the website by reading the URL aloud to the participant. In Safari, an SSL warning pop up instead of a web page is displayed. For participants using Safari, navigating to the example SSL warning page triggered the SSL warning popup to appear in Safari and interrupt the user.

3.4 Ethical Considerations

Security warning research carries risks of psychological and emotional distress, which can be compounded for users with disabilities. The Nielsen Norman Group reports that the web is three times easier for sighted users than for users who are blind or visually impaired [44, 58]. On the electronic informed consent form, we assured potential participants that if they chose to participate they may end the study at any time, for any reason. For those who chose to participate, we reminded the participant of this in-person. We included our University's Health and Wellbeing Center's phone number on the informed consent form, and our contact information was also made available to non-students as an emotional support resource in accordance with our University IRB requirements. We developed the research protocol to minimize

task duration and steps to avoid undue stress or confusion, while ensuring that each action was possible for the user with their particular computer set up and assistive technology.

During the in-person contextual interviews, we asked for permission to make any changes in the environment: permission was requested and granted in every session to displace or place objects such as extra lighting, for a higher volume of sound on the computer speakers, for us to grab an extra chair and sit in it, start a video recording with audio, place a video camera in a described location, and include only the participant's computer screen and keyboard in the video recording. During each step of the interview, participants were made aware of where the camera was placed and what was being captured in the video frame, as suggested by Henry [34]. We also alerted the participant to any unusual noises from her activities, including starting, pausing, or stopping a video recording. Interactions with service animals in the vicinity were avoided, as suggested by Henry [34].

During all stages of the research, we took measures to ensure that participants' privacy was protected. We used pseudonymous identifiers in our study to protect participants' personal data to ensure that any personally identifiable information that was collected would be kept confidential and discarded when appropriate. It is normative for researchers to protect a participant's anonymity by associating their data with a numerical study code that can uniquely identify participants without the use of their name [18]. Every questionnaire response was assigned a unique number (01 through 16). We maintained a mapping of these numerical pseudonymous identifiers to the interview participant's first name, without contact information. The only link between a participant's name and contact information was stored as responses in SurveyMonkey and in e-mails with participants, which could only be accessed by us. The pseudonymous identifier was used in place of any identifying information for

all remaining stages of the study, including taking notes, labeling video recordings, labeling video transcriptions, performing data analysis, and reporting results. Any non-identifying response data was labeled with the pseudonymous identifier.

3.5 Thematic Analysis

We began analysis of each session by transcribing each video recording to text, and developed an open qualitative coding scheme. Quotations from participants, selected from video transcripts, were labeled with the participant study ID number and assigned study codes. Quotations were then categorized into high level themes. This produced a set of common themes when compared across all participants for which the warning type was applicable, revealing a summary of key findings. Experiences that were specific to participants' computer set up or internet browsing behaviors were also documented.

Chapter 4

RESULTS

4.1 Participants

Of the sixteen subjects who responded to our questionnaire, eight individuals agreed to an in-person interview. This small sample size comes close to that of similar studies investigating visually impaired users' security experiences that involved 10-15 participants [21, 55]. All respondents considered themselves to have a level of visual impairment. See Tables D.1, D.2, D.3 for the complete set of questionnaire response data.

4.1.1 Demographics

Table 4.1: Participant demographics and computer profile response data from questionnaire respondents who participated in a follow-up interview. Browser represents the browser that the respondent indicated was the browser that they use when using their primary screen reader.

ID	Sex	Age	OS	Screen Reader	Browser
U01	F	35 to 44	Windows	JAWS	IE 9+
U04	M	55 to 64	Windows	Windows-Eyes	IE 8
U07	M	45 to 54	Mac	VoiceOver	Safari
U08	M	25 to 34	Mac	NaturalReader	Safari
U09	M	35 to 44	Windows	JAWS	IE 9+
U10	M	18 to 24	Windows	Windows-Eyes	IE 9+
U11	M	45 to 54	Windows	JAWS	Firefox
U12	F	45 to 54	Windows	JAWS	IE 9+

Table 4.1 includes participant demographics and computer profile data from questionnaire respondents who also participated in the follow up interview. The group of eight individuals consisted of two females and six males. All but two participants used

Microsoft Windows as their operating system. Two participants used Windows-Eyes as their screen reader during the interview tasks, four participants used JAWS, and one participant used VoiceOver. One participant, U08, indicated NaturalReader as their screen reader, but did not use a screen reader during the follow-up interview. Four participants indicated Internet Explorer 9+ as the browser that they use when using their primary screen reader, two participants indicated Safari, one indicated Internet Explorer 8, and one indicated Firefox. U11, who indicated Firefox as the browser that they use when using their primary screen reader, chose to use Internet Explorer during the interview tasks. Researchers should note that the response data regarding primary computer profile may not reflect what the participant chooses to use during an in-person interview, and prepare accordingly, if the interview tasks are dependent on those factors.

We compared the browser, operating system, and screen reader used by our sample of study participants to the most commonly used computer setups indicated by respondents of a screen reader survey conducted in 2015 by WebAIM, in which the majority of the 2515 respondents were blind or low vision/visually impaired (64% and 38.7% respectively) [40]. The WebAIM Screen Reader User Survey found Windows to be the most common operating system, Internet Explorer to be the most commonly used browser, and JAWS to be the most commonly used screen reader among respondents, as is the case in our sample of study participants.

4.2 Warning Scenarios

4.2.1 Obstacles to Completion of Warning Scenarios

None of the eight participants completed all three types of warning scenarios. Table 4.2 charts the warning scenarios that were completed by each participant. The six

Table 4.2: Warning scenarios that were successfully completed ("C"), or not completed, ("N") by each participant during the in-person interview, by warning type. "N" indicates that the user did not complete the warning scenario due to an obstacle. At the time this study was conducted, there was not a separate phishing warning from the malware warning in Internet Explorer 9+.

ID	Browser Used	Phishing	Malware	SSL
U07	Safari	C	N	C
U08	Safari	N	C	C

ID	Browser Used	Phishing/Malware	SSL
U01	IE 9+	C	C
U04	IE 8	N	C
U09	IE 9+	N	C
U10	IE 9+	C	C
U11	IE 9+	C	C
U12	IE 9+	C	C

participants who used Internet Explorer during the in-person interview did not participate in a separate phishing warning scenario because Internet Explorer displays a malware warning for websites that are suspected of both phishing and malware, and does not display a phishing-specific warning. Otherwise, warning scenarios were not completed when the warning example webpage could not be accessed at the time of the interview for various reasons. For example, U08 did not participate in a phishing warning scenario because the example phishing warning website did not display its usual contents at the time on Safari, and instead displayed a Google Sites website skeleton. This was a temporary occurrence, as the same example phishing warning website loaded its usual contents, displaying an example of a Safari phishing warning, for the interview with U07. Due to this issue, U07 was the only participant who completed a phishing warning scenario.

U04 and U09, both using Internet Explorer, were not able to participate in the malware warning scenario because the example warning website hosted by Malvertising.info did not load at the time, due to the website being down. The same example

malware warning website was available for the four other interviews using Internet Explorer. U07 did not participate in a malware warning scenario, as the example malware warning page hosted by Google did not load in his Apple Safari browser at the time of the interview (despite having tested the Google hosted website prior to the interview). After the interview with U07, we found that another example malware warning hosted by Mozilla was available, and was later used in an interview with U08, the other participant who used Safari.

All eight participants completed the SSL warning scenario without any obstacle as the same source URL for the example SSL warning was compatible with all browsers. See Appendix E for screenshots of each of the warnings that participants interacted with.

4.3 Common Themes

4.3.1 Initial Reaction to a Warning

At the expense of ecological validity, we fully disclosed the purpose of the study and asked participants to navigate to an example of a warning and think aloud about the steps that they would take. In this approach, the scenarios did not pose any real threat to the user and minimized duration of the tasks involved. Because the warnings did not occur in a real world context in which users are blocked in their attempt to access a certain website, and instead are navigating directly to a warning, their initial reaction to the warning from the interview task may not be representative of what their reaction would be if they encountered a warning organically. Our approach in asking the participant what they would have done if they encountered the warning, however, provided insight into what factors would influence their reaction in a real world context.

For each warning, the first question in our semi-structured interview format inquired about participants' initial reaction to that warning. Our interviews indicated that the reaction is often dependent on the user's familiarity with the website they are trying to visit or whether they have visited it before. In six of the fourteen total warning scenarios, the users communicated that their familiarity with a website was a reason to ignore a warning. In the malware warning scenario, U01 (mistakenly) expressed her belief that certificate errors were a common occurrence, and stated that if a website was familiar, she would ignore the warning: "*I get a lot of certificate errors and things like that. To tell you the truth, usually I just ignore stuff like this because if I know the website that I'm going to, I know a lot of the smaller websites and things like that have trouble paying to keep up with their certificates and stuff so this kind of stuff I just say whatever.*" U01 reacted to the malware warning based on her recollection of SSL warnings. U01 expressed the same sentiment with regards to the SSL warning scenario, although the SSL warning was more familiar: "*This I've seen before, many many times. And again I'd look for some way to skip past this, because I've noticed a lot of smaller websites have trouble keeping up with this.*" Although the SSL and malware warnings were two different types of warnings, with only the SSL warning type encompassing the certificate warnings that she had seen previously, U01 was inclined to ignore both of them.

Similarly, when evaluating the malware warning example, U08 expressed that familiarity with the website he was trying to visit would lead him to ignore the warning, while he would heed the warning in the case of visiting a website from a search result: "*If I was familiar with the site and knew that it was a safe site...I'd ignore the warning. If I was googling for a new pair of shoes or something, then I would follow the warning.*"

When discussing his reaction to an SSL warning example, U04 stated that he would read more details or proceed through to a website, ignoring a warning, based on whether he had visited the website previously: "*If it was something that...I had been to before, that I had a pretty good idea was okay, I would probably either read the information or just go to the website if it was a website that I trusted.*" U07 expressed that an SSL warning is likely to be superfluous in cases when he had knowledge of the website he was trying to visit: "*It's probably okay...especially because I probably knew the website that I was going to, that it's just some over-excessive Safari security precaution. I would just go to the continue button...because I probably knew something about this page before going there.*" Similarly, U11 expressed no cause for concern when confronted with an SSL warning, especially if the website was a familiar one: "*I don't think much of an expired certificate, it doesn't worry me when I'm trying to go to some place I know.*"

Six out of eight interviewees were able to complete two warning scenarios. All but one user who participated in two warning scenarios reacted differently to each scenario. In both the malware and SSL warning examples, U12 expressed the inclination to heed both warnings and return to safety.

In reaction to both the malware warning and SSL warning scenario, U01 stated that she would typically bypass the warning. Although the first warning scenario that U01 completed was a malware warning, and not an SSL warning, she mentioned that she would "*get a lot of certificate errors and things like that*" and chose to bypass the malware warning for that reason. When she encountered the SSL warning, she stated, "*Again I'd look for some way to skip past this, I've noticed a lot of smaller websites have trouble keeping up with this...I'm arrowing down to look for some way to bypass it.*"

U07 was the only participant to complete the phishing warning scenario. He completed the SSL warning scenario as well, and reacted differently to each. He expressed that the SSL warning example was a non-concern, especially in the case of visiting a website that he was familiar with. In contrast, he stated that he would heed a phishing warning, and avoid interacting with the page for safety reasons: "*When it says suspected phishing site, I probably would just close it, just so I don't have to deal with it...I wouldn't wanna click on the link that says learn more, because the more you click, the more you take a chance of infecting your computer.*"

U08 reacted differently to the malware and SSL warning scenario. While he stated that he would ignore the malware warning if he was visiting a website he was familiar with, the text content of the SSL warning page was found to more likely promote compliance: "*The wording is more compelling, it makes the website sound more harmful, makes the website sound more malicious.*"

In reaction to both the malware and SSL warning scenarios, U10 expressed an inclination to heed the warning. In reaction to the malware warning example, he quickly stated that "*My first reaction is I should probably leave the website*". However, in the SSL warning scenario, he elaborated that he would ignore the warning in certain cases, "*It's probably not safe to go to this website, but if I really need to slash want to, I'd probably go to it anyways...if I was doing research or something like that, I think I would*". Depending on the task that he was trying to complete, he felt that he would bypass a warning, despite his first reaction to heed the warning.

In reaction to the malware warning example, U11 described the keyboard action that he would take to return to safety: "*First reaction would be hit the ALT HOME and go back to the Google search.*" In response to the SSL warning scenario, U11 recalled a time that he had seen the warning before and had the ability to bypass the warning: "*Sometimes I've been able to go through it, I don't remember how I did it...I somehow*

managed to get to and I can't remember how, it's been a long time." He proceeded to use the arrow keys to search for the link to bypass the warning: "*OK, so I'm gonna first go over to the page and gonna just ARROW down. I'm looking for links...and then I would hit the space bar, and then I would get to where I was trying to get to.*"

4.3.2 Phrasing and Terminology in Warnings

The phrasing and terminology used in the textual elements in warnings are a common theme among participants; half of the participants commented, or made a suggestion, on how a warning message or call to action could be conveyed. During the malware warning scenario, U01 noted that the warnings that she had encountered in the past have had alternate terminology to describe actions for bypassing or ignoring a warning, and suggested more uniformity: "*Sometimes it's skip, sometimes it's don't warn me about this in the future. There should be some kind of uniform message...phrasing should be similar.*" This uniformity in phrasing may help screen reader users quickly locate the button or link to bypass a warning: "*I think at least something specific to look for, hey, if I come across this kind of security warning, how do I get past it. What's the phrasing I'm looking for. Because this kind of stuff really does kinda frustrate people...they don't know how to get past it.*" The idea that a warning should contain phrasing that users can become familiar with and search for was also suggested during her SSL warning scenario: "*I mean continue to website is fine, but then they have to know with all of these pages to look for that language. So if I know every time to 'continue on to website'...great.*" Because screen reader users often navigate a page by iterating through heading levels and links and listening to the start of each line, a standard set of phrases to indicate the available courses of action may help to identify them more efficiently.

The phrasing of the bypass option could contain clarification of the destination that the button or link would lead the user to. During the phishing warning scenario in Apple Safari, the options available on the phishing warning example page were to "Learn more," "Ignore Warning," "Go Back," and "Report an error." U07 suggested that the "Ignore Warning" button could further specify the result of clicking the button with the words, "Ignore warning and proceed to page." He also wondered about the effect of the "Report an error" button, and the entity that was producing the warning message that would receive the error report: "*I am trying to think of what 'report error' would mean. The more things you click, the more trouble you may get into. Report an error to whom? Where is this error coming from?*" His comments reveal a sense of caution when faced with the phishing warning message, and suggest that buttons and links that contain specific words indicating what the result of clicking on them would be, would provide more confidence for the user to click on them.

U07's suggestion for more specific phrasing of where a button or link would take the user to coincides with the confusion that several participants using Internet Explorer experienced in the SSL warning scenario. During the SSL warning scenario U12 was presented with the options "Click here to close the webpage," "Continue to this website (not recommended)," and "More information." U12 inquired aloud about whether the link to close the webpage would lead her to her browser's home page or her previously visited page: "*The only thing that I would wonder is where am I gonna go, like am I gonna go back to my blank screen, where I start from, my home page, or am I gonna go back to where I came from, in other words, if I had been surfing around Google, and got here, would I go back to Google, would I go back to my home page, where would I go?*" Similarly, when U10 and U11 navigated to the option to close the webpage in the same SSL warning scenario, they were uncertain of what the result would be. When prompted to "do what he would normally do" when he encountered

the warning, U10 said: "*I'm just gonna close it down and see what happens.*" U11 also voiced the same sense of discovery when considering what the effect would be of clicking on the option: "*Click here to close this webpage, I'm not sure what it'll do, let's find out!*" Among several participants using Internet Explorer to navigate the SSL warning example, there was a theme of uncertainty of where the option would lead the user to.

In the malware warning scenario, U08 had the same idea that U07 had in the phishing warning scenario, of using the word "proceed" to indicate that bypassing a warning would lead a user to the page that they were trying to visit: "*Something that bothers me, is what it says on the buttons, it says ignore warning or go back. How would I rephrase that, I would probably just use different wording, like proceed.*" Similarly, in the SSL warning scenario, U01 suggested using language that provides direction to the user: "*Continue on to website, bypass this message, ignore this message. Something that very clearly gives the next step as to where to go from here.*"

Several users commented on the phrasing in a warning message being an indicator of the severity of danger. U08, who used Apple Safari, felt that the SSL warning message indicated more danger than the malware warning message: "*This warning message is more compelling to, make it sound more harmful...the wording of the message is more compelling, it makes it sound more malicious, as opposed to the previous message. I'd be more likely to follow its advice.*" U07, on the other hand, who also used Apple Safari, felt the opposite way about the same SSL warning: "*If it was an expired security SSL certificate, that's not as ominous sounding as a phishing scam or some other message. It doesn't sound like it's gonna screw up my computer.*" Similarly, U10, who used Internet Explorer, pointed out that the SSL warning message used words that were less definitive than the malware warning message, and therefore yielded less caution. U10 noticed that the malware warning declared that the website

that he would be trying to visit "is unsafe," while the SSL warning stated that the website "could be unsafe": "*I guess the keyword for me on this one is that it says 'unsafe', the other one says 'could be unsafe,' so I'm more willing to push the envelope on 'could be unsafe' than 'is unsafe.'*"

4.3.3 Common Screen Reader Shortcuts

During the interviews, we asked participants to demonstrate how they would return to the previous page or continue to the next page, if their initial reaction to the warning did not consist of those interactions. Several of the participants used the same method to return to the previous page. Windows users U04, U09, U11, and U12 all reported that they would use the JAWS hotkeys ALT+LEFT ARROW in order to return to the website that they came from. Two participants mentioned using their screen reader's shortcut for accessing buttons or links on a web page in order to locate the bypass option. After discovering that the option to bypass the malware warning was not available, U01 suggested adding a button to the warning that would allow users to bypass the warning that would be accessed through the screen reader using the "B" key: "*I would put a button. With JAWS at least, pressing B for button will take you to every single button on the page.*" When U11 was asked during the malware warning scenario what he would do to bypass the warning, U11 mentioned an alternative JAWS screen reader shortcut that accesses the links on the page, instead of the buttons: "*I'm going to Insert F7 to get to the links.*"

4.3.4 Seeking More Information

Several of the participants commented aloud on whether or not they would read the additional information provided by the "More information" or "Learn more" option

(depending on the warning type). All warning scenarios but one, the SSL warning on Apple Safari, displayed this option on the web page rather than a dialogue box. When prompted to "do what you would normally do" when encountering the SSL warning, U04, U08, and U09 opted to read the additional information about the SSL warning, by choosing the option on the web page. U12, on the other hand, distinctly expressed that she was not interested in the option: "*The chances of me choosing more information are slim, because I don't really care.*" The only participant who completed a phishing warning scenario, U07, also reported that he would not click on the "Learn More" option, "*because the more you click, the more you take a chance of infecting your computer.*"

4.3.5 Checking the Browser Toolbar

Two of the participants, who both used Internet Explorer, reported recollection of encountering warnings in the browser's toolbar. Upon encountering the SSL warning example, U09 noted that he would immediately consult the notification bar in the browser for options: "*First of all I would see if there's anything in the notification bar that I need to be aware of, and I'm looking to see if there's any buttons that I need to be aware of. There have been some instances where I've seen the action to be taken on the notification bar.*" U09 proceeded to navigate to the browser's toolbar using his keyboard, and listened to the screen reader announce the contents of the elements, including the address bar as well as the browser icons for accessing home-page, favorites, and settings. Upon encountering the malware warning example, U12 also recalled warnings that she had encountered previously with options in Internet Explorer's information bar: "*Most of the warnings that I have seen have come through the information bar, where you have to...go up to the information bar and it gives you choices like open this site, or don't, or whatever.*"

4.3.6 Trust in Antivirus Software

For two participants who used Internet Explorer, their trust in their antivirus software helped them feel safe in ignoring the SSL warning. When asked to "do what he would normally do" if he encountered the warning, U04 communicated his trust in the Microsoft Windows antivirus software: "*I'm going on to the website because I trust Microsoft Security Essentials and...whatever the anti-malware stuff is in Windows 8.*" U09 expressed a similar sentiment: "*Trusting that I have my malware and antivirus stuff up-to-date, then I'll just continue on to the site...usually you trust your antivirus software will detect anything malicious.*"

4.4 Screen Reader Interactions

While most participants listened to the screen reader narrate the contents of the entire warning page upon encountering the warning, others (U01 and U11) stopped the screen reader narration at the start of the web page. U01 employed a *probing* browsing strategy to quickly navigate through the page to search for a method to bypass the warning, skipping blank lines and headings when the first few words did not match what she was looking for. U11, on the other hand, immediately used ALT+HOME keyboard shortcut to return to his homepage.

For two participants using Internet Explorer, U11 and U12, the screen reader narrated a warning message that was not displayed on the warning web page contents: "*Reported unsafe website, navigation blocked.*" U12 reported that she had never heard this warning message from the browser before. The screen reader repeated this message three times in succession without any keyboard actions from the user, and then reported the number of headings and links on the web page: "*Page has six headings*

and three links." We later discovered that this was the title of the web page. U11 opted not to listen to the actual contents of the web page, while U12 listened to the screen reader narrate the entirety of the contents.

Five out of the seven participants who used a screen reader to navigate the warnings, used either the DOWN arrow or TAB key on their keyboard to iterate through each of the available options on the page before deciding their action. Two participants did not iterate through the options, and instead opted to return to their previous page using a keyboard shortcut.

We also observed different speeds of screen reader narration. U10's Windows-Eyes screen reader narrated the contents of the warnings at a significantly more rapid rate than the other participants' screen readers, while U12's JAWS screen reader narrated at a slower rate than the average.

In contrast to Apple Safari warnings which did not display any iconography, Internet Explorer warnings included an icon alongside both warnings' main heading, in addition to each of the available options, which were narrated by the screen reader. For example, the screen reader narrates aloud, "*Graphic recommended icon*" followed by the recommended option. When encountering this, U12 thought aloud, *"I guess it's just a graphic with alt text, nothing to activate."*

Chapter 5

DISCUSSION

5.1 Reflection of Methodology

As is common with human subjects research, a number of unforeseen circumstances arose during our pilot study that can be addressed in future work. In this section, we examine methodological choices that we made and the resulting trade-offs and obstacles or unexpected scenarios that occurred.

5.1.1 Reliability of Warning Example Pages

One methodological challenge inherent in this type of research is creating warning scenarios that accurately and reliably display the correct browser security warning page to participants, according to the version of browser that they use. While we were able to identify websites that serve this purpose, it forced us to be reliant on external websites being available at the time of the interview. In some instances, the example warning websites were not reliable, and for one of them we were able to identify an alternative mid-study (See Chapter 4.2.1). While reliance on external websites to provide example warnings caused site reliability issues that we needed to work around, these warning websites proved to be authentic and reflected exactly what the participant would have encountered. In future work, researchers can consider hosting their own warning websites or backups on a reliable server; however while this solves the availability issue, this approach gives rise to the challenge of creating example websites that continuously support ever-changing browsers. There is not a simple solution to striking the right balance between creating an authentic warning

scenario for the participant to interact with, without leveraging the external websites that are meant to serve this purpose, but may not always be reliable for an in-person interview.

5.1.2 Phishing Warning Scenario Privacy Concerns

The phishing warning scenario highlights another challenge of creating an authentic scenario, without creating other risks. As described in Chapter 3.3.2, we tasked the participant with navigating to Gmail to sign in to a provided email account with given credentials, in order to demonstrate to the participant a typical phishing email, which would lead to an example of a phishing warning. We did not consider that the participant may already be signed into an existing Gmail account, as U07 was, potentially revealing private email to the researcher. In addition to privacy, there are also time, convenience, and complexity considerations (*e.g.* will the subject want to sign out, will they be able to sign in again, *etc.*). When U07 navigated to Gmail by our instruction, an existing, yet empty, email inbox was displayed. U07 proceeded to search for options on the web page for signing out. While we intended to design the website tasks to minimize task duration and unnecessary frustrations, U07 ended up spending a few minutes to figure out how to sign out of their Gmail account.

One potential solution is to ask participants to perform these tasks in an incognito window, which provides a blank slate for the user, solving the privacy issue and prevents the inconvenience of needing to sign out of their account and sign back in. However, asking the user to use an incognito window may be inconsistent with users' typical working environment and may have the potential of providing the participant with a greater sense of security and influencing their authentic reaction to the warnings, in a scenario that has ecological validity already compromised by having users

navigate directly to the warning. Here again, researchers must be cognizant of the trade-offs inherent in studies of this kind.

5.1.3 Minimum Allowable Sized Window

It is common for blind or visually impaired users to navigate websites solely through their keyboard. However, we did not expect that U01's browser window would be sized to the minimum as allowed by the operating system, occluding nearly all visual content. As a result, we were not able to view what was being navigated on the web page during the interview, nor were we able to record on video what was occurring on the page. However, this did not interfere with the interview tasks. In order to avoid additional tasks for the participant, we did not instruct the participant to expand their browser window size. We were able to collect data and have a discussion with the participant regarding all of the interview tasks involved, and deemed that it was not necessary to modify the users' original browser window size setting.

From this one unexpected occurrence, we found that the video recording was helpful insofar as playing back the audio for transcribing conversations with the participant and hearing the screen reader. It was not particularly useful for us to view what was being shown on the participant's computer screen. In fact, this one circumstance proved the benefit of relying solely on audio to understand the user's experience in this research. Capturing only the audio reflects exactly what is experienced by the user, and nothing more.

5.1.4 Ongoing Modifications to Methodology

This study benefited from slight modifications to the task-based interviews while the interviews were being conducted on a rolling basis. For instance, the example malware

warning page source URL was changed to one hosted by Mozilla upon discovery that the original example page hosted by Google was no longer available mid-study, allowing for subsequent Apple Safari interview participants to navigate to a warning page that was available.

Another example of a mid-study modification to our task-based interviews was a slight change in the instruction to participants to proceed with "what they would normally do" if they encountered the warning while browsing the Web. For the purpose of minimizing duration of tasks, but at the expense of ecological validity, we asked participants to navigate directly to the examples of warning pages. This artificial environment in which users navigate directly to a warning, instead of being interrupted with a warning while browsing, often led to confusion and hesitation to proceed with their natural action.

For example, during the SSL warning scenario, U01 was instructed to "do what she would normally do" in the case that she encountered the SSL warning, and used the ARROW key to locate the option on the page. She then inquired aloud: "*That's what I'd normally do, is continue to this website. So, do you want me to continue, or do you want me just to...?*" U01 was uncertain of whether to continue to the next page, or stay on the current page after locating the option. We responded that she did not need to proceed, as we were able to collect data on the steps she needed to take to find the option to proceed.

Similarly, during the phishing warning scenario, U07 iterated through the available options with his keyboard when asked to "do what he would normally do" upon encountering the warning. When he concluded that his natural action would be to return to the previous page, he indicated hesitation to do so: "*I'd probably just click go back. Do you want me to do that or click on the other buttons?*" The hesitation to either return to the previous page, or continue to the next page, seemed to be due to

the artificial nature of the study environment. After noticing this hesitation from U01 and U07, we mitigated this in subsequent interviews by providing clear instructions to the user to "do what she would normally do", while specifying to do so without actually clicking on the button. This instruction to refrain from following through with their decided action allowed for continued discussion while the user remained on the warning example page, without burdening the user with any extra steps.

5.1.5 Analysis of Screen Reader Interactions

Conducting interviews and analyzing participants' screen reader interactions requires that the researcher possesses at least a basic competency with screen readers and their output. This is an important skill for researchers throughout all stages in a study of this nature. For example, basic competency prepares the researcher to assist participants when needed, such as when locating the option to sign out of a participant's email account via the screen reader. It also allows researchers to examine, in real time during the interview, the browsing strategies through the keystrokes. In our study, we used a combination of the interview questions and the video recording to interpret browsing strategies and keystrokes. These proved to be helpful, and in future work, other methods can be explored for capturing participants' experiences of interacting with their screen reader. For example, recording only audio and analyzing the data aurally is worth consideration. Researchers can practice listening to screen readers at different speeds, and potentially test these screen reader settings' impact on warning perception and effectiveness.

5.2 Key Findings

5.2.1 Findings Consistent with Sighted Users

Common themes that were revealed in our pilot study involving visually impaired users have been found in previous browser security warning research involving sighted users. For example, in a study of the correlations between website reputation and warning adherence for Google Chrome users, Almuhimedi *et al.* reported several observations that were consistent with our pilot study findings [3]. First, their study revealed that users are more likely to heed warnings from websites that they are not familiar with. In our analysis with visually impaired users, familiarity with a website was the most common reason to ignore a warning. Almuhimedi *et al.* also found a dangerous user misconception that users' antivirus software installed in their operating system protected them from malware, providing users a false sense of security and causing them to be less likely to adhere to the Google Chrome malware warning. Our findings revealed a similar sentiment among visually impaired Internet Explorer users who trusted that the Windows security software protected them from Internet malware. Lastly, Almuhimedi *et al.* discovered that the Google Chrome participants confused malware warnings with SSL warnings. Similarly, one participant in our study reacted to a malware warning based on her experience with SSL warnings.

As was suggested by Almuhimedi *et al.*, the wording and phrasing in warnings can be tweaked in order to provide education to users and prevent the common misconceptions that would expose them to security threats. For example, using special language to warn users when visiting websites that they have visited before, or have a high reputation generally, can increase warning adherence. Providing education to users that the browser warning could be preventing a malicious attack that the operating system's antivirus software may not protect them from, could also be necessary. Hav-

ing better distinctions between warning types could also provide further clarity to users.

Warning language impacting participant reactions to a warning was also consistent with prior research on browser security warnings with sighted users. Akhawe and Felt observed that the use of the word "untrusted" in the title of a warning contributed to greater rates of warning adherence, while not being the sole factor [2]. Similarly, our participants were influenced by warning content that conveyed severity of danger, as discussed in Chapter 4.3.2.

The prevalence of these themes in both sighted and non-sighted users indicates that these tweaks to warning design can increase warning adherence universally, whether they are consumed via visual means or screen reader. As it is important to address the themes that are found across both populations, future research can deeply examine the design decisions that are to the most benefit.

5.2.2 Browser Security Warnings Interface Standards

Our findings suggest a number of potential improvements to the user experience of browser security warnings for the visually impaired. There may be a need for more uniformity and standardization of language for consistency and to better convey the meaning of available actions. It is worth consideration to create standards of phrasing in browser security warnings that provide clear indication as to the destination that a button or link would lead the user to, as current phrasing has resulted in uncertainty for visually impaired users.

In addition, standards of page structure and hierarchy of page elements across browser security warnings could be of benefit, at least within the same browser, and ideally across all browsers. A normative user interface for warnings that includes a standard

for the placement of available options would help screen reader users have a more consistent, useful, and therefore effective, experience when they encounter a browser security warning. This would allow visually impaired users to more quickly navigate to the option they are expecting to find, with fewer keystrokes required. When participants decided on their action upon encountering a warning, the common inclination was to use the DOWN arrow key to iterate through headings and links in order to find the options available to them according to their mental model developed from encountering prior warnings. If an expected option is unavailable, such as the option to proceed to the next page (as was not found to be an option in the malware warning scenario with U01), there could instead be a disabled button or clear language indicating the lack of that expected option, so that screen reader users are not spending time trying to hunt for an option that is not there. Having clear and consistent language in browser warnings is most important to the population of users with visual disabilities, as these users do not benefit from the context of visual indicators such as graphical elements. These graphics may be missed, ignored, or not interpreted in the same way when navigating via the screen reader or other assistive technology. Researchers can consider testing and setting guidelines for more consistent, yet effective warning language and element placement in future work.

It could be argued that uniformity in language and placement of options could instead endanger users through habituation, which is defined as the "decreased response to repeated stimulation" [31]. For example, previous work has shown that randomized placement of option buttons has resulted in users being less likely to ignore the safe option [11]. However, our review of the literature regarding habituation to security warnings reveals an examination of the issue only in the context of *sighted* users, where a lack of visual consistency assists with users' security awareness. In a more inclusive warning design, it is important to weigh the benefits of reduced warning habituation against the benefit of a design that visually impaired users can navigate in a manner

that is more predictable, informative, and less time-consuming. Further research is required to create warning designs that strike this balance of creating inconsistency for the purpose of safety, yet avoiding confusion for users with disabilities.

5.2.3 Other Ecological Validity Challenges

Other concerns of ecological validity arose. As discussed in Chapter 4.3.5, some of the participants checked their browser's notification bar for information or errors upon encountering a warning, and did not find any additional information or options. It is unclear whether in a real world context, the participants would have discovered other indicators in their browser's toolbar, or if they were referring to older or different versions of Internet Explorer. In either case, the experience may not be matching exactly what would have occurred if they encountered a real warning. For example, Chrome displays a security indicator in the address bar when encountering an SSL warning. However, none of the participants in this study used Google Chrome. Further research is required to understand visually impaired users' interaction with these browser warning elements and their efficacy, by ensuring that the browser will display the toolbar or address bar elements that would reflect reality.

5.2.4 Implications of Screen Reader Interactions

Our findings reveal new insights and confirm previous work documenting how visually impaired users interact with websites. As discussed in Chapter 2.2, blind users have been observed to employ a variety of techniques to "scan" a web page using their screen reader in the context of online shopping [13, 71, 76]. Our findings confirm these browsing strategies in the context of browser security warnings; we observe both *previewing* or *probing*, as well as *gambling* techniques to navigate the warnings.

Through our observations of what the participants hear when consuming the browser security warnings via screen reader, we found that the screen reader narration often includes content that is unexpected or unnecessary. For example, some participants listened to the screen reader narrate the website title, "*Reported unsafe, navigation blocked*" multiple times prior to narrating the page body. The screen reader also frequently narrates blank lines, which results in users needing to spend time skipping past several of them at a time. Lastly, graphical elements are narrated as "*Graphic recommended icon*" or "*Graphic unrecommended icon*" in Internet Explorer, which does not provide any additional safety measures to the user. It is unclear whether the screen reader, the website source code, or the browser is primarily responsible for these issues. Nonetheless, the experience is problematic, and highlights the incongruities visually impaired users suffer due, in large part, to a lack of standards and coordination between these entities.

These findings have implications on the effectiveness of warnings for this population. We speculate that the screen reader narrating extra content in a warning could diminish the important messages that are found alongside it, and could contribute to "warning fatigue," described by Akhawe and Felt as a situation in which users may pay less attention to subsequent warnings they encounter [2]. There exists an open challenge of creating warnings that are hard to ignore, while being accessible and usable to people with disabilities. Again, we have not found any studies that examine warning habituation and warning fatigue in the context of navigating browser warnings via screen reader or other assistive technology, and thus remains an unexplored research area.

Chapter 6

CONCLUSION

In this paper we attempt to more deeply understand the experience of visually impaired users with the security warnings presented by web browsers. We have developed a research methodology that considers and merges the best practices of conducting human subject research and browser security warnings with those of working with the visually impaired—a combination previously unexplored in the research literature.

Using this methodology, we conducted a pilot study that observed a group of visually impaired users employing their own computers, browsers, and assistive software in an authentic setting. Our investigation reveals that while the use of screen readers for aiding the visually impaired to interpret the web is prevalent, it is highly incongruous with a usable and secure experience. We find that visually impaired users' experience is consistent with sighted users with respect to misunderstandings of, and frustrations with, security warnings, but whose experience is further confounded by a more inconsistent experience across warning types, and receive no benefit from the normative security indicators, such as color and iconography.

We propose a set of initial suggestions to better align visually impaired users' experiences with those of sighted users, perhaps improving all users' security in the process, but ultimately conclude that there is a rich body of unexplored research topics and necessary experimentation to be conducted in the space of usable security and privacy for the visually impaired, particularly with web browsers. We believe our initial results elucidate some of the compelling issues suffered by this population, and that

our methodology (and reflections there upon) lays a helpful groundwork for those looking to repeat or extend this line of inquiry.

BIBLIOGRAPHY

[1] 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*, 2015.

[2] D. Akhawe and A. P. Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *USENIX Security Symposium*, pages 257–272, Washington, D.C., Aug. 2013. USENIX Association.

[3] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[4] APWG. Phishing activity trends report 2nd quarter, 2021.

[5] A. P. Association et al. Guidelines for assessment of and intervention with persons with disabilities. *The American psychologist*, 67(1):43, 2012.

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

[7] L. Bauer, C. Bravo-Lillo, L. Cranor, and E. Fragkaki. Warning Design Guidelines (CMU-CyLab-13-002). Technical report, CMU CyLab, 2013.

[8] Y. Borodin, J. P. 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)*, pages 1–10, 2010.

[9] Y. Borodin, J. P. Bigham, G. Dausch, and I. V. 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)*, W4A '10, pages 13:1–13:10, New York, NY, USA, 2010. ACM.

[10] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):0018–26, 2011.

[11] J. C. Brustoloni and R. Villamarín-Salomón. Improving security decisions with polymorphic and audited dialogs. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 76–85, 2007.

[12] E. Buchanan, J. Aycock, S. Dexter, D. Dittrich, and E. Hvizdak. Computer science security research and human subjects: Emerging considerations for research ethics boards. *Journal of Empirical Research on Human Research Ethics*, 6(2):71–83, 2011.

[13] M. C. Buzzi, M. Buzzi, B. Leporini, and F. Akhter. User trust in ecommerce services: Perception via screen reader. In *International Conference on New Trends in Information and Service Science*, pages 1166–1171, 2009.

[14] V. J. Caracelli and J. C. Greene. Crafting mixed-method evaluation designs. *New directions for evaluation*, 1997(74):19–32, 1997.

[15] M. C. N. Carvalho, F. S. Dias, A. G. S. Reis, and A. P. Freire. Accessibility and usability problems encountered on websites and applications in mobile devices by blind and normal-vision users. In *Proceedings of the 33rd Annual ACM symposium on applied computing*, pages 2022–2029, 2018.

[16] V. L. P. Clark and J. W. Creswell. Designing and conducting mixed methods research, 2011.

[17] D. R. Commission. *The Web: Access and Inclusion for Disabled People; a Formal Investigation*. The Stationery Office, 2004.

[18] J. W. Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications, 2013.

[19] J. W. Creswell and D. J. Creswell. *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications, 2018.

[20] G. Desolda, F. D. Nocera, L. Ferro, R. Lanzilotti, P. Maggi, and A. Marrella. Alerting users about phishing attacks. *International Conference on Human-Computer Interaction*, 2019.

[21] B. Dosono, J. Hayes, and Y. Wang. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Symposium On Usable Privacy and Security (SOUPS)*. USENIX Association, 2015.

[22] S. Egelman, L. F. 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.

[23] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. Improving SSL warnings: Comprehension and adherence. In *Proceedings of the Conference on Human Factors and Computing Systems*, 2015.

[24] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the 32nd annual*

ACM conference on Human factors in computing systems, pages 2667–2670. ACM, 2014.

[25] B. J. Fogg, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, J. Shon, P. Swani, and M. Treinen. What makes web sites credible? a report on a large quantitative study. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, page 61–68. Association for Computing Machinery, 2001.

[26] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' conceptions of web security: A comparative study. In *CHI'02 extended abstracts on Human factors in computing systems*, pages 746–747. ACM, 2002.

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

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

[29] E. Gerber. Surfing by ear: Usability concerns of computer users who are blind or visually impaired. In *The 17th Annual International Conference of California State University Northridge (CSUN) "Technology and Persons with Disabilities*, 2002.

[30] C. Goble, S. Harper, and R. Stevens. The travails of visually impaired web travellers. In *Proceedings of the Eleventh ACM on Hypertext and*

Hypermedia, HYPERTEXT '00, page 1–10, New York, NY, USA, 2000. Association for Computing Machinery.

[31] P. M. Groves and R. F. Thompson. Habituation: a dual-process theory. *Psychological review*, 77(5):419, 1970.

[32] B. Hagler, C. Ice, L. Johannesen, S. Keates, E. Kunzinger, B. Lovelacer, J. Sacco, and S. Trewin. Conducting user evaluations with people with disabilities. White paper, IBM Research, 2005.

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

[34] S. L. Henry. *Just ask: integrating accessibility throughout design.* http://www.uiaccess.com/accessucd, 2007.

[35] H. Hochheiser, J. Feng, and J. Lazar. Challenges in universally usable privacy and security. In *Symposium On Usable Privacy and Security (SOUPS)*, 2008.

[36] S. E. Hollier. *The Disability Divide: A Study into the Impact of Computing and Internet-related Technologies on People.* PhD thesis, Curtin University of Technology, 2007.

[37] 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.

[38] J. Hong. Usable privacy and security: A grand challenge for HCI, 2009.

[39] F. A. Inan, A. S. Namin, R. L. Pogrund, and K. S. Jones. Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1):28–40, 2016.

[40] Institute for Disability Research, Policy, and Practice. Webaim screen reader user survey #6 results.

[41] M. L. Johnson, S. M. Bellovin, and A. D. Keromytis. Computer security research with human subjects: risks, benefits and informed consent. In *Financial Cryptography and Data Security*, pages 131–137. Springer, 2012.

[42] 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 *Symposium On Usable Privacy and Security (SOUPS)*, pages 39–52, Ottawa, 2015. USENIX Association.

[43] H. Karen and J. Sandra. Contextual inquiry: A participatory technique for system design. In *Participatory design*, pages 177–210. CRC Press, 2017.

[44] H. Keller and A. C. You. Conducting usability research with computer users who are blind or visually impaired. In *Paper presented at the 17th Annual International Conference of California State University Northridge (CSUN)" Technology and Persons with Disabilities*, 2002.

[45] N. Kumaran and S. Lugani. Protecting businesses against cyber threats during COVID-19 and beyond. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond, 2021.

[46] S. Kvale. Dominance through interviews and dialogues. *Qualitative inquiry*, 12(3):480–500, 2006.

[47] E. Lau and Z. Peterson. A research framework and initial study of browser security for the visually impaired. In *Workshop on Inclusive Privacy and Security (WIPS): Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[48] 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 HumanComputer Interaction*, pages 247–269, 2007.

[49] 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*, CHI '12, page 2267–2276, New York, NY, USA, 2012. Association for Computing Machinery.

[50] J. Lazar, J. H. Feng, and H. Hochheiser. *Research methods in human-computer interaction*. John Wiley & Sons, 2010.

[51] LEVEL Access. How browsers interact with screen readers and where ARIA fits in the mix. http://www.ssbbartgroup.com/blog/how-browsers-interact-with-screen-readers-and-where-aria-fits-in-the-mix/. Accessed: 2016-01-12.

[52] M. May. Inaccessibility of CAPTCHA. *Alternatives to Visual Turing Tests on the Web. I: W3C (red.), W3C Working Group Note, work in progress*, 2005.

[53] D. M. Mertens. *Transformative research and evaluation*. Guilford press, 2009.

[54] D. M. Mertens. Transformative mixed methods research. *Qualitative inquiry*, 2010.

[55] D. Napoli. *Accessible and Usable Security: Exploring Visually Impaired Users' Online Security and Privacy Strategies*. PhD thesis, Carleton University, 2018.

[56] D. Napoli, K. Baig, and S. Chiasson. ï'm literally just hoping this will work:ˊ obstacles blocking the online security and privacy of users with visual disabilities. In *Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[57] J. Nielsen and T. K. Landauer. A mathematical model of the finding of usability problems. In *Proceedings of the INTERACT '93 and CHI '93 Conference on Human Factors in Computing Systems*, CHI '93, pages 206–213, New York, NY, USA, 1993. ACM.

[58] Nielsen Norman Group. Beyond accessibility: Treating users with disabilities as people. https://www.nngroup.com/articles/beyond-accessibility-treating-users-with-disabilities-as-people/. Accessed: 2016-01-12.

[59] Nielsen Norman Group. The use and misuse of focus groups. https://www.nngroup.com/articles/focus-groups/. Accessed: 2010-01-28.

[60] W. H. Percy, K. Kostere, and S. Kostere. Generic qualitative research in psychology. *The Qualitative Report*, 2015.

[61] H. Petrie and O. Kheir. The relationship between accessibility and usability of websites. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 397–406. ACM, 2007.

[62] 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, 2012.

[63] M. E. Raven and A. Flanders. Using contextual inquiry to learn about your audiences. *SIGDOC Asterisk J. Comput. Doc.*, 20(1):1–13, feb 1996.

[64] M. E. Raven and A. Flanders. Using contextual inquiry to learn about your audiences. *SIGDOC Asterisk J. Comput. Doc.*, 20(1):1–13, Feb. 1996.

[65] 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.

[66] A. Saldhana and T. Roessler. Web security context: User interface guidelines. *World Wide Web Consortium LastCall WD-wsc-ui-20100309*, 2010.

[67] J. Saltzer and M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[68] M. Scanlan. Reassessing the disability divide: unequal access as the world is pushed online. *Universal Access in the Information Society*, 2021.

[69] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 1–18, 2011.

[70] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *USENIX Security Symposium*, pages 399–416, 2009.

[71] H. Takagi, S. Saito, K. Fukuda, and C. Asakawa. Analysis of navigability of web applications for improving blind usability. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 14(3):13–es, 2007.

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

[73] H. Tonn-Eichstädt. Measuring website usability for visually impaired people-a modified goms analysis. In *Proceedings of the 8th international ACM SIGACCESS conference on Computers and accessibility*, pages 55–62, 2006.

[74] C. University. Phish bowl — it@cornell. https://it.cornell.edu/phish-bowl.

[75] M. Vigo and S. Harper. Challenging information foraging theory: Screen reader users are not always driven by information scent. In *Proceedings of the 24th ACM Conference on Hypertext and Social Media*, HT '13, page 60–68, New York, NY, USA, 2013. Association for Computing Machinery.

[76] M. Vigo and S. Harper. Coping tactics employed by visually disabled users on the web. *Int. J. Hum.-Comput. Stud.*, 71(11):1013–1025, Nov. 2013.

[77] Y. Wang. The third wave? inclusive privacy and security. *New Security Paradigms Workshop*, 2017.

[78] T. Whalen and K. M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005*, GI '05, pages 137–144, School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 2005. Canadian Human-Computer Communications Society.

[79] T. Whalen and K. M. 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.

[80] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson. Research-based guidelines for warning design and evaluation. *Applied ergonomics*, 33(3):219–230, 2002.

[81] M. S. Wogalter, D. DeJoy, and K. R. Laughery. *Warnings and risk communication*. CRC Press, 1999.

[82] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 601–610. ACM, 2006.

[83] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, page 601–610, 2006.

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

[85] S. L. Young and D. R. Lovvoll. Intermediate processing stages: Methodological considerations for research on warnings. *Warnings and risk communication*, pages 27–52, 1999.

[86] M. E. Zurko and K. Johar. Standards, usable security, and accessibility: can we constrain the problem any further. In *Symposium On Usable Privacy and Security (SOUPS)*, 2008.

APPENDICES

Appendix A

PARTICIPANT RECRUITMENT E-MAIL

My name is Elaine Lau and I am a computer science graduate student at Cal Poly, San Luis Obispo. I am conducting a research project whose goal is to learn how visually impaired people using a screen reader experience web browser security warnings. For example, when a web browser displays a warning if the connection to a destination website is untrusted. Through your participation, we hope this research can directly contribute to the improvement of accessibility of these warnings in the future.

If you are blind or visually impaired,use a screen reader to access the web, and are willing to participate please visit this online questionnaire at SurveyMonkey at this link: [URL]. It will take approximately 10 minutes of your time, is anonymous, and is intended to learn more about computer usage and perceptions about web security. The questionnaire will ask if you would be interested in participating in an in-person interview at a later date.

Thank you for your time and consideration. If you have any questions, please feel free to contact me by e-mail at [E-MAIL] or phone at [PHONE NUMBER].

Appendix B

QUESTIONNAIRE

B.1 Informed Consent Form

INFORMED CONSENT TO PARTICIPATE IN A RESEARCH PROJECT, "A Research Framework and Initial Study of Browser Security for the Visually Impaired."

A research project on the accessibility of browser security warnings is being conducted by Elaine Lau, a graduate student in the Department of Computer Science at Cal Poly, San Luis Obispo under the supervision of Dr. Zachary Peterson. The purpose of the study is to learn how visually impaired people using a screen reader experience security warnings in a web browser.

You are being asked to take part in this study by answering an initial questionnaire and participating in a video recorded in-person interview at a later date. The questionnaire will ask about your typical computer usage and perceptions about website security. You may choose to answer the initial questionnaire, but not volunteer for the in-person interview. If you volunteer to participate in the interview, you will be asked to navigate to three web pages, each showing an example of a different type of web browser security warning. There is no real security risk involved. For each warning, you will be asked about your experience and to think aloud. You will be asked for permission regarding the placement of the video recorder, which will be used to capture the screen and use of the keyboard. Your participation will take approximately ten to fifteen minutes for the questionnaire, and one hour for the interview. Please be aware that you are not required to participate in this research and you may

discontinue your participation at any time without penalty. You may omit any items you prefer not to answer in the questionnaire or the interview.

There are no risks anticipated with participation in this study. If you should experience emotional distress or confusion, please be aware that you may contact the project advisor, Dr. Zachary N.J. Peterson at (805) 756-2088 for assistance. Please be aware that you may take a short break or period of rest at any point during the study.

Your confidentiality will be protected by codifying your name in the analysis of the data and discussion of results so that personally identifiable information will not be associated with the data, and will not be revealed to others in any form. Potential benefits associated with the study include an increased and more in-depth understanding of how accessible and usable browser security warnings are for people with visual impairments, as well as recommendations for making them easier to navigate via a screen reader.

If you have questions regarding this study or would like to be informed of the results when the study is completed, please feel free to contact Elaine Lau or Zachary N. J. Peterson at (805) 756-2088. If you have concerns regarding the manner in which the study is conducted, you may contact Dr. Steve Davis, Chair of the Cal Poly Human Subjects Committee, at (805) 756-2754, sdavis@calpoly.edu, or Dr. Dean Wendt, Dean of Research, at (805) 756-1508, dwendt@calpoly.edu.

If you agree to voluntarily participate in this research project as described, please indicate your agreement by completing the following questionnaire. Please save an electronic copy of this form now for your reference, and thank you for your participation in this research.

B.2 Demographics

This questionnaire is intended to learn about your computer usage and perceptions about internet security. Thank you for taking this time to complete this questionnaire!

1. What is your gender? (Female, Male)
2. What is your age? (18 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64, 65 to 74, 75 or older)

B.2.1 Your Computer Profile

If you use more than one computer, please answer the following questions to describe the one you use for web browsing the most.

3. Which operating system do you use when using your primary screen reader? (Microsoft Windows, Apple Mac OS X, Linux, Other (please specify)
4. Which of the following is your primary desktop/laptop screen reader? (JAWS, Windows-Eyes, VoiceOver, NVDA, System Access or System Access To Go, ZoomText, ChromeVox, Other (please specify))
5. How customized are your screen reader settings? (e.g. changed verbosity, installed scripts, etc.) (A lot of customization, Somewhat customized, Slightly customized, Not at all)
6. If possible, please specify the screen reader customizations you have.
7. Which browser do you use when using your primary screen reader? (Internet Explorer 9+, Firefox, Internet Explorer 8, Safari, Internet Explorer 6, Internet Explorer 7, Chrome, Other (please specify))

8. Please rate your proficiency level for browsing the web using a screen reader: (Expert, Advanced, Intermediate, Beginner)

9. Do you use other assistive technologies besides a screen reader for browsing the web? (Yes, No)

10. If yes, please specify the other assistive technologies you use to browse the web:

B.2.2 Security Perceptions

11. How confident are you that your browser is protecting you from danger on the internet? (Extremely confident, Very confident, Moderately confident, Slightly confident, Not at all confident)

12. If possible, please explain:

13. Have you ever encountered a security warning while browsing the web? (Yes, No)

14. If possible, please explain what occurred:

15. Do you have any questions or concerns about web browser security warnings that you would like to discuss?

16. We would like to conduct an in-person interview to learn about your experience with web browser security warnings. Please provide your e-mail address and/or phone number if you would be available in the summer of 2015 and are willing to participate in an interview.

Appendix C

CONTEXTUAL INQUIRY

The following interview procedure was submitted to and approved by our University IRB.

C.1 Special Considerations for Blind and Visually Impaired Participants

- The researcher will not move anything at the interview site without asking first. Nothing should be moved to a different place than the participant is used to because the participant cannot see where things are moved.
- The researcher will explain any unusual noises from her activities, such as beginning to record, pausing or stopping the recording.
- If any guide dogs or service animals are present, the researcher will not interact with them to avoid distracting them.
- For all paperwork, the researcher will provide documents in the participant's preferred format.
- The researcher strives to minimize the steps necessary to complete a task since it can be exhausting to listen to a screen reader while using busy interfaces.
- The researcher will also strive to communicate that the participants are in no way being "tested" or evaluated for their ability to navigate the warnings.
- The researcher will take steps to minimize capturing any identifying information using the video recorder.

C.2 Chronological Description of Events

1. The researcher will brief the participant by introducing herself, and by reading the informed consent form to the participant. The researcher will ask the participant if they have any questions, and clarify any questions regarding the reason for conducting the study, procedures involved, potential risks, and how they can get more information about the study. The researcher will also provide an electronic copy of the informed consent form using the participant's e-mail address.

2. The researcher will request the participant's signature on the printed informed consent form. The printed form will have a signature guide, a small piece of plastic with a window in the middle, to indicate where the signature should be. If the participant agrees, the researcher will provide a pen and show the location of the signature guide.

3. The researcher will ask the participant for permission to set up the video recorder in that location. Upon consent, the researcher will place the video recorder in a location so that it will aim to capture only the participant's computer screen and keyboard, maintaining anonymity, and minimizing all other distractions. With subject's permission, the researcher may set up an extra lamp in the room to have adequate lighting for the video recording.

4. The researcher will ask the participant for permission to record audio with the video recorder. Upon consent, the researcher will ask the participant to use the computer's speakers for audio instead of headphones.

5. The researcher will describe the setting displayed in the video recording including the relative position of the participant in the video recording, the screen display, and keyboard.

6. The researcher will ask the participant to turn on their computer and open the web browser that they are most comfortable with.

7. The researcher will ask the participant to sign in to gmail.com using a fake username and password provided. The researcher will read aloud the username and password to be entered.

8. The researcher will ask the participant to open a single, unread e-mail that has been specially crafted to simulate a phishing attempt. The e-mail will contain a link to a canonical but benign example of a phishing warning page.

9. The researcher will ask the participant to navigate the resulting web page as they normally would and talk through their experience. The researcher will ask a series of open-ended questions to learn more. The researcher will communicate her understanding, and ask the participant to expand or correct her understanding of the responses. After the participant has finished with the page, or about 10 minutes has passed, the researcher will ask the participant if they would like to add anything else. The researcher will then move on to the next warning type.

10. The researcher will then ask the participant if to navigate to a canonical example of a second warning type (malware warnings) and repeat step 7.

11. The researcher will then ask the participant to navigate to a canonical example of a third warning type (SSL warnings) and repeat step 7.

12. The researcher will ask the participant if they would like to add anything else. The participant will be thanked for their time.

13. The researcher will stop the video recording and then remove any extra lighting and video recording equipment from the room.

14. The researcher will thank the participant for their time and provide the researcher's contact information.

C.3 Interview Scripts

Hello! As you know, my name is Elaine Lau, and I'm a computer science graduate student at Cal Poly San Luis Obispo. My advisor is Dr. Zachary Peterson but I'm alone here today.

Today we'll be doing a contextual interview, meaning you'll navigate two different types of web browser security warnings. I'll ask you to think aloud while you navigate the warnings, about what you're doing and why you're doing it. You are essentially the master, and I'm the apprentice; so I'd like to observe and learn from you about what works and what doesn't.

If you ever have any questions about the purpose of the study, procedures, risks, or anything at all, please let me know and I'll be happy to answer.

Before you took the survey, you read and agreed to an informed consent form that included participation in this interview. Please remember that you are not required to participate in this research, you may discontinue your participation at any time, and you do not have to answer any questions you choose not to answer. Shall we begin the interview?

Now there are a couple things to set up first: the video recorder, the lighting, and audio.

I have a video recorder to capture the computer screen and keyboard. Is it okay if I place the video recorder here? The video only captures the computer screen and keyboard, and does not show your face.

[OPTIONAL] Now, is it okay if I place an extra lamp here so that there is better lighting in the video?

The next thing is audio. Is it okay if we turn up the audio on the computer, and (if the participant is using headphones) use speaker instead of headphones?

I'm going to turn on the video recorder now. The video shows the back of your head, the screen display, and the keyboard. I'm now done setting up and we can start!

(See Warning Scenario Scripts.)

I think it's time to wrap up this warning. Is there anything else you would like to mention about this warning page that we haven't talked about?

Is there anything else you would like to add or do you have any questions? (Wait for user to respond.)

I appreciate you taking this time out of your day! I'm now going to stop the video recording. I hope to continue communication with you afterwards while I am writing up the results so that I have a correct understanding of what I have learned from you and interpreted from the interview. I may be in contact with you through e-mail if I have any questions or clarifications, if that's all right.

C.4 Warning Scenario Scripts

I will ask you to think aloud while navigating the warnings, about what you are doing and why you are doing it. You are essentially the master, and I am the apprentice, so I would like to observe and learn from you about what works and what doesn't. I will be taking notes at the same time. If you ever have any questions about the purpose of the study, and the procedures, or the risks, please don't hesitate to ask. I have a video recorder that is capturing the computer screen and the keyboard.

Before you took the survey, you read and agreed to an informed consent form that included participation in the interview, so please remember that you are not required to participate in this research, and you may discontinue your participation at any time. You do not need to answer any questions that you choose not to answer.

Browser: Internet Explorer, Warning Type: Malware

(If the user is using Internet Explorer) First, I want to mention that Internet Explorer 9 has a feature called SmartScreen Filter that blocks phishing and malware websites. We should make sure Internet Explorer 9 has SmartScreen Filter turned on so that we can see the browser security warnings. If you agree, could we make sure it is turned on?

1. Please open Internet Explorer. 2. On top menu, select Tools (ALT+X) (IE 9). Please look for the Safety menu (4th down from list) 3. Select SmartScreen Filter from the drop-down list and click on Turn on SmartScreen Filter.

When you're ready, could you please open Internet Explorer?

The first security warning I would like to learn about your experience with is the malware warning. Internet Explorer checks the sites you visit against a list of reported phishing and malware sites. If it matches, then the browser will show a warning page. The first website I would like you to visit is a demo page created by Microsoft that triggers the warning. Visiting the page will not cause you any harm. When you are ready, please navigate to the URL https://malvertising.info. *See Appendix C.4 Interview Prompts for subsequent questions.*

Browser: Internet Explorer, Warning Type: SSL

The second warning I would like to learn about is the SSL warning. Internet Explorer displays an SSL warning when there is a problem with the website's security certificate. The website I would like you to visit has an expired certificate. It is an example page that also does not cause any harm, but it will trigger an SSL warning in the browser. When you are ready, please type into the address bar https://expired.badssl.com. *See Appendix C.4 Interview Prompts for subsequent questions.*

Browser: Safari, Warning Type: Phishing

When you are ready, please open the Safari browser. The first security warning that I would like to learn about your experience with is the phishing warning. Safari checks the websites you visit against a list of recorded phishing and malware sites. If it matches, then the browser will show a warning page. I would like you to first sign

into a fake Gmail account with a provided username and password to see an example of this. When you are ready, please visit gmail.com and I will provide the credentials.

The username is [USERNAME] and the password is [PASSWORD]. When you are ready, please sign in.

When you are ready, please read the single unread email. It is an example of a typical phishing email. The email contains a link to a web page that will trigger a phishing warning in the browser, and this is only a demo page that Google has provided, so that we can visit the warning without causing any harm. When you are ready, please visit the website at the link in the phishing email. *See Appendix C.4 Interview Prompts for subsequent questions.*

C.5 Interview Prompts

The following description of the contextual inquiry was submitted to and approved by our University IRB.

Interviews will be conducted at the user's home, work place, or other preferred natural setting. The researcher will collaborate with the participant to understand how they experience the warnings and why. The researcher will share their interpretations and insights with the participant during the interview. The researcher will ask the participant to expand or correct her understanding of the responses.

For each warning type, the following prompts and questions will be asked.

1. What is your first reaction when encountering this warning?

2. Have you encountered a warning like this before?

3. Please do what you would normally do if you encountered this warning, and think aloud about the steps you are taking if possible.

   If the participant has not already tried to proceed through the warning:

4. If you wanted to proceed through the warning and continue to the next page, please show me how you would do that. If possible, think aloud about the steps you would take.

5. Why did you do that? How can the interaction be improved?

   If the participant has not already tried to go back to the previous page:

6. Please show me how you would go back to the previous page, and think aloud if possible.

7. Why did you do that? How can the interaction be improved?

8. Is there any information about this page that could be useful, but is not available?

C.6 Phishing Email

The phishing email contents were drawn from a common phishing email at Cornell University. Cornell University provides examples of phishing emails on their Phish Bowl webpage at https://it.cornell.edu/phish-bowl.

Subject Line: Email Account Security info replacement

Body: Someone started a process to replace all of the security info for your Email Account.

If this was you, you can safely ignore this email. Your security info will be replaced with 15623535981 when the 5-day waiting period is up.

If this wasn't you, someone else might be trying to take over your email account. [Click here to fill in details] and verify your current information in our servers and we'll help you protect this account.

Appendix D

PARTICIPANT RESPONSE DATA

Table D.1: Questionnaire response data, "Your Computer Profile" Part 1

ID	Which browser do you use when using your primary screen reader?	Please rate your proficiency level for browsing the web using a screen reader:	Do you use other assistive technologies besides a screen reader for browsing the web?	If yes, please specify the other assistive technologies you use to browse the web:
U01	Internet Explorer 9+	Advanced	No	(Blank)
U04	Internet Explorer 9+	Advanced	No	(Blank)
U07	Safari	Expert	Yes	iPhone, Windows browsers with JAWS and NVDA.
U08	Safari	Beginner	No	(Blank)
U09	Internet Explorer 9+	Expert	No	(Blank)
U10	Internet Explorer 9+	Advanced	Yes	android
U11	Firefox	Advanced	Yes	Magic magnification
U12	Internet Explorer 9+	Advanced	No	(blank)

Table D.2: Questionnaire response data, "Your Computer Profile" Part 2

ID	Which operating system do you use when using your primary screen reader?	Which of the following is your primary desktop/laptop screen reader?	How customized are your screen reader settings? (e.g. changed verbosity, installed scripts, etc.)	If possible, please specify the screen reader customizations you have.
U01	Microsoft Windows	JAWS	Not at all	(Blank)
U04	Microsoft Windows	Windows-Eyes	Slightly customized	AI Squared's IE Enhance
U07	Apple Mac OS X	VoiceOver	Somewhat customized	I cut down on the verbosity a lot.
U08	Apple Mac OS X	Natural Reader and Adobe	Somewhat customized	Voice, Speed, and hot keys
U09	Microsoft Windows	JAWS	A lot of customization	(Blank)
U10	Microsoft Windows	Windows-Eyes	Slightly customized	(Blank)
U11	Microsoft Windows	JAWS	Not at all	(blank)
U12	Microsoft Windows	JAWS	Slightly customized	Mostly, they are changes to voice rate and some visual tracking to support accessibility-related presentations. One thing that may be important is my "forms mode" setting. I tend to set it for manual, rather than auto.

Table D.3: Questionnaire response data, "Security Perceptions"

ID	How confident are you that your browser is protecting you from danger on the internet?	If possible, please explain:	Have you ever encountered a security warning while browsing the web?	If possible, please explain what occurred:
U01	Moderately confident	(Blank)	Yes	Sometimes, a message about a certificate error pops up.
U04	Slightly confident	(Blank)	Yes	(Blank)
U07	Slightly confident	The Mac is less problematic than Windows.	Yes	The warning declared that my computer had a virus.
U08	Very confident	I feel I have the discernment to securely operate the internet	Yes	warnings for downloads and websites, unless I am familiar and confident with the website or software I follow the wariness advice
U09	Very confident	(Blank)	Yes	Most often, I get warnings that the sites are untrusted and I get an option to look at the certificate warnings.
U10	Moderately confident	(Blank)	Yes	(Blank)
U11	Not at all confdient	So much malware keeps getting loaded onto my system that it slows it way way down.	Yes	I get contact has been blocked warning. The we have
U12	Slightly confident	I try to read about security and look at my browser settings, but I'm probably someone who knows enough to know what she does not know.	Yes	IE gives warnings about whether or not to "show all content." And I've also seen warnings about certificates that weren't up-to-date.

Appendix E

WARNING EXAMPLE SCREENSHOTS

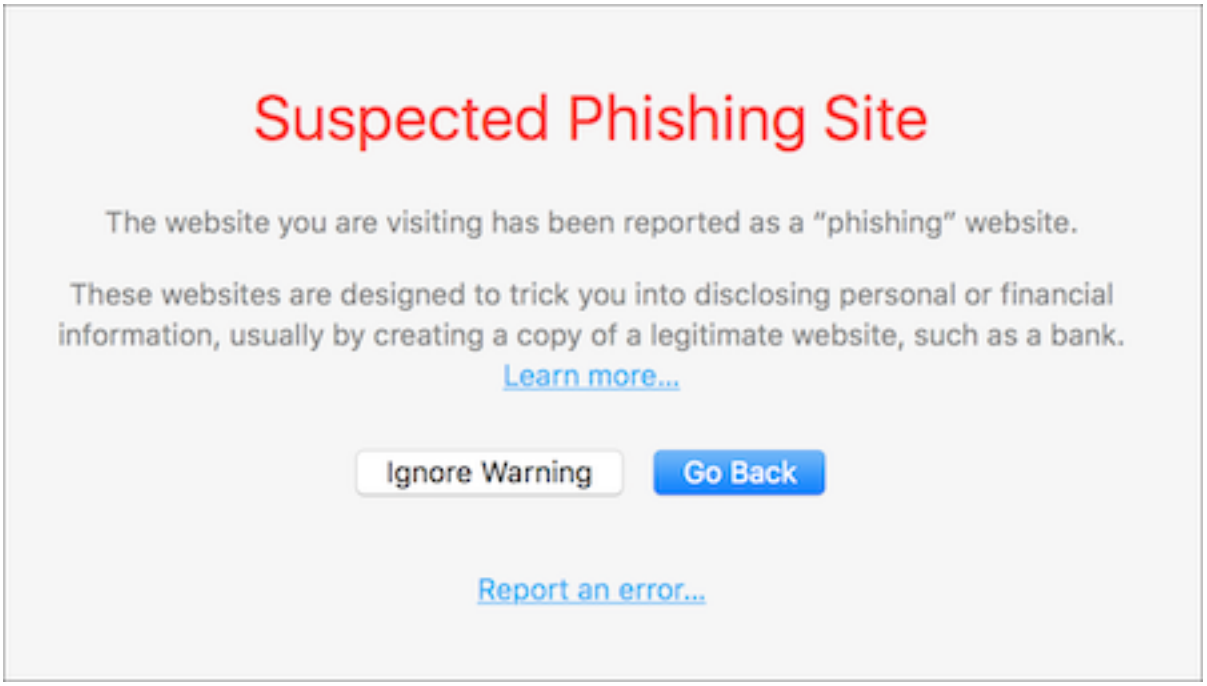

Figure E.1: Example of a phishing warning page in Safari.

Figure E.2: Example of an SSL warning popup in Safari.

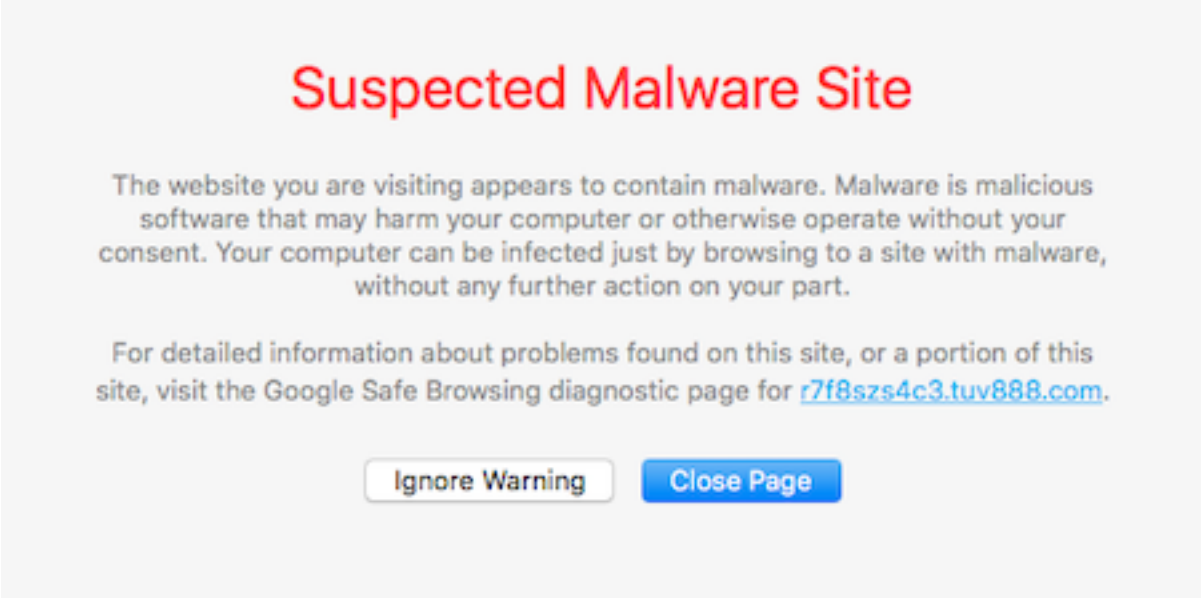

Figure E.3: Example of a malware warning page in Safari.

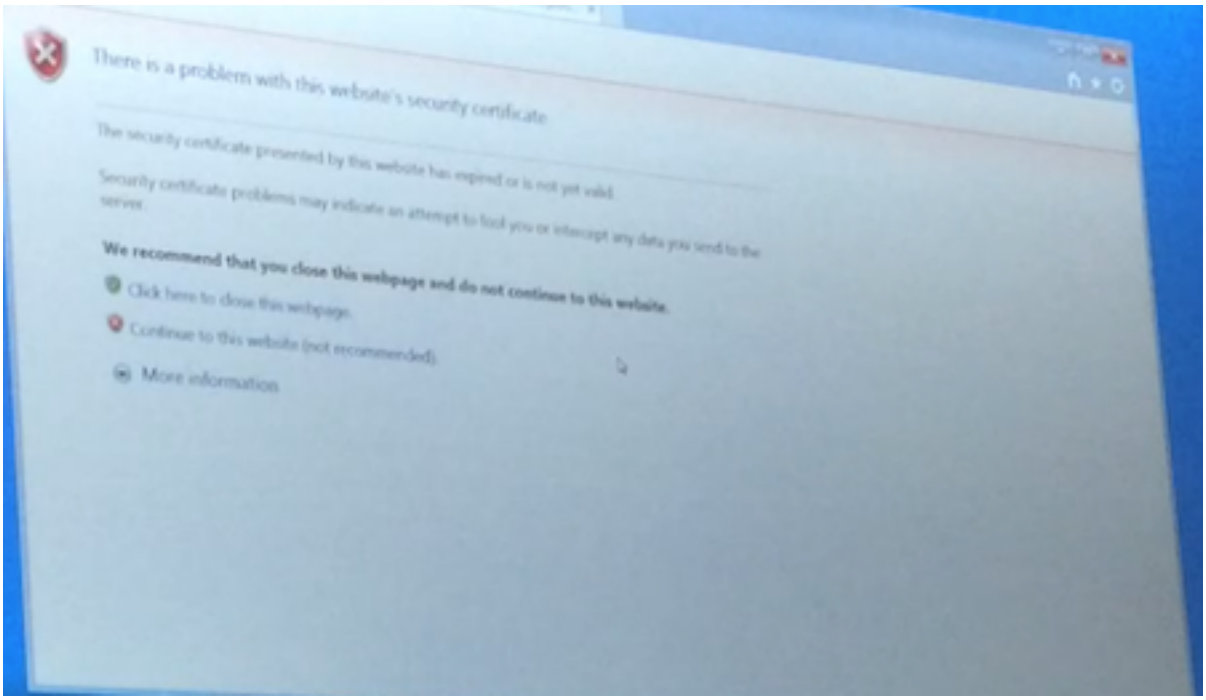

Figure E.4: Example of an SSL warning page in Internet Explorer.

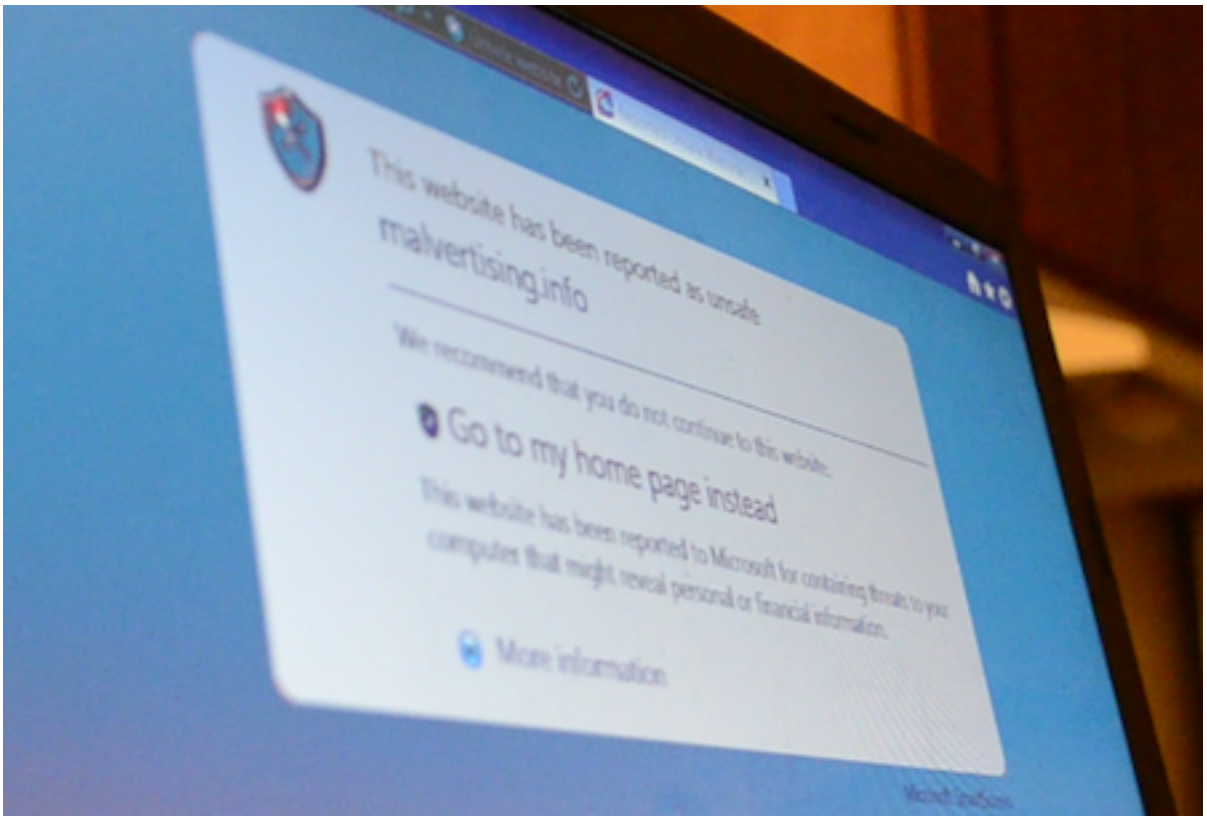

Figure E.5: Example of a malware warning page in Internet Explorer.