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

Elaine Lau
Cal Poly, San Luis Obispo

Zachary Peterson
Cal Poly, San Luis Obispo

Abstract

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 the placement and size 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. We attribute this not 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 their choices, exacerbated by a deficit of clear methodologies for conducting studies with this population. Indeed, the challenges are manifold. In this paper, we analyze and address the methodological challenges of conducting security and privacy research with a visually impaired population, and contribute a new set of methodological best practices when conducting a study of this kind. Using our methodology, we conduct a preliminary study analyzing the experiences of the visually impaired with browser security warnings, perform a thematic analysis identifying common challenges visually impaired users experience, and present some initial solutions that could improve security for this population.

1 Introduction

The increasing prevalence of web-based malware and phishing attempts [4, 32] 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 recommend a course of action [45]. 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 [16]. 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 [53]. Similarly, Bauer *et al.* suggest a common layout for structuring warning information, including a single icon that conveys the severity level of a message [5]. In a study of Google Chrome's SSL warnings, 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 [19].

While the efficacy of visual techniques has promoted safety for sighted users, these techniques are 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 [28]. 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 [6]. Indeed, the challenge of communicating security cues to this population is not unique to web browser warnings [28]. Hochheiser *et al.* note that graphical passwords, icons, images, and pop-up dialogs are often not interpreted by screen reader software [27, 28]. Further, screen readers cannot read image-based CAPTCHAs, which the W3C has identified as a major problem for blind and visually impaired users [37].

The 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 [45] with accessibility as a top concern. Zurko and Johar discuss possible additions to WSC recommendations, including the use of aural interfaces in warning design [55].

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 [42]. 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 its usefulness 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 [44]. 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 regard to how users with visual disabilities experience web browser security warnings, generally. Our work aims to fill this gap.

The contributions of this work are threefold: (1) we identify and address 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; (2) through a preliminary study, we investigate how visually impaired individuals 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; and (3) we draw upon our 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 work is to contribute toward conceptualizing and designing inclusive security research methodologies and mechanisms with the needs and concerns of at-risk populations in mind.

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. 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.

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. 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 unobtrusively collect pseudonymous data from users. 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 led to a lower click-through rate. In our study, we focused on the same three types of browser security warnings. While we did not test adherence rates, we examined the factors influencing visually impaired users to bypass a warning, and the steps they would take to do so.

There have also been studies examining phishing warning effectiveness as the design evolved. 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 [18]. 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 visually impaired users about their interaction with a phishing warning example. It is unclear whether phishing warnings meet these recommendations when they are accessed via screen readers.

Browser security warning effectiveness is also affected by a user's trust in whether a warning is genuine. Bravo *et al.* interview 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 findings that the look and feel of a website is often the most significant factor in gaining user trust [21, 54]. 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 a warning, for example, if and how they determine its authenticity or trustworthiness.

Sotirakopoulos *et al.* use an experimental study design to investigate SSL warning effectiveness and learn about participants' reactions to SSL warnings in general [46]. 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.

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 [34]. Screen reader users develop their favorite strategies for web browsing, based on their individual preferences or on the task they are trying to accomplish [7]. 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 [52]. 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 [49]. These strategies are known as *previewing* or *probing* a web page [52]. 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 [12]. Blind users will often employ *gambling scanning* in this fashion until they encounter desired content, and thereafter will navigate sequentially [52].

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 [48]. 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 [7]. 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 [52].

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 [22]. 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 [49]. This information overload often ends up being very time consuming, and in the context of browser security warnings, it could im-

[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.

pact warning compliance. 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 such situations, screen reader users employ navigation tactics to escape from the situation, rather than pursue their goal. For example, screen reader users were found to employ navigation 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 [51]. Encountering browser security warnings could involve the use of some of these tactics, since browser security warnings cause problematic situations such as confusion and stopping the user from their original task. In our study, we leverage Vigo and Harper's work to understand visually impaired users' experiences.

2.3 Web Security and Privacy Research with Visually Impaired Users

There have been few studies investigating the security and privacy experiences of visually impaired users. Of those studies that have been conducted, most document the most common concerns and challenges that visually impaired users encounter on the web [1, 28, 29, 40], while others evaluate specific security mechanisms or behaviors for users with visual disabilities, such as audio-based CAPTCHAs and other authentication experiences [17, 35]. Particularly, Napoli *et al.* conducted a comprehensive investigation of visually impaired users' online security and privacy concerns, including the accessibility of web security cues and perception of web-based security threats [40]. Through task-based interviews that instructed participants to complete common tasks such as e-commerce shopping and e-mail login, researchers discovered inaccessible web security indicators, including phishing indicators that were interpreted misleadingly by assistive technology, leading to risky behavior and complex security management methods. In contrast, we document visually impaired users' experiences specifically with interstitial browser security warnings, of which there are currently no studies. Browser security warnings research with sighted users reveals that visual design elements often impact adherence rates, as discussed in 2.1. For that reason, we assert that there must be considerations into the effectiveness of warning pages when visited by users who have visual disabilities and do not perceive the visual warnings used on warning pages. These visual indicators on interstitial warning pages differ from other security indicators on the web, as they are standalone web pages that block potentially significant security threats. To inform our approach, we have gleaned methodological approaches from prior studies in this domain, especially the work documenting visually impaired users' experiences of interacting with a specific security mechanism.

Contextual Inquiry. Dosono *et al.* examine visually impaired users' experiences with authentication mechanisms using a contextual inquiry approach, asking participants to think aloud while performing a set of five common authentication scenarios [17]. Contextual inquiry features three main facets: (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 [43]. 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. In our study, we adopt contextual inquiry as a methodology accomplished through task-based semi-structured interviews, asking participants to think aloud while navigating examples of browser security warnings and allowing room for further conversation.

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 [40]. An initial questionnaire or interview at the beginning of the study helps to inform the subsequent parts of the research protocol, as it can be used to explore issues and concerns for further investigation, and to prepare for the technology setup, including assistive technology preferences. Hayes *et al.* study how visually impaired users 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 [25]. 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 [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 [23]. In our study questionnaire, we include questions regarding these three variables.

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

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 users' privacy while recording video by turning the camera away when credentials were being entered [17]. 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 [40]. 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, resulting in less accurate results. 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 [26]. 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).

Previous studies that focus on *visual* elements in warnings have maintained ecological validity through the use of a visual representation of a user interface. For example, Sunshine *et al.* include screenshots in an online survey to examine users' perceptions of SSL warnings [47] and Almuhidemi *et al.* display screenshots in an online survey with Amazon Mechanical Turk to investigate why users ignore malware warnings [3]. This approach 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, we met subjects in person in order to observe how a warning page, as rendered 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.

The vast variability in browser security warnings also presents a challenge. Warnings differ across browsers and their versions, and warning page layouts vary. For example, the page hierarchy of the malware warning differs 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; each browser has their own Accessibility API that is queried by screen readers [36]. Internet Explorer 9+ includes a feature called SmartScreen Filter that must be activated for certain warnings to be available. We developed a research protocol that anticipates and accounts for the variability of warnings across browsers and technological setups.

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

Table 1: Website sources that represent an example of each warning type, by browser.

3 Methodology

To understand visually impaired users' experiences of interacting with web browser security warnings, we adopt a generic qualitative approach. We focus on three types of warnings as Akhawe and Felt: 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 list of reported phishing or malware sites, or when there may be a problem with a website's security certificate. 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 1 for a list of source URLs that were used for each type of warning and browser.

3.1 Participant Recruitment

Our participant criteria aligns with Gerber's three recommended screening variables for research with blind and visually impaired users [23]. 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 [13]. 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.

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 (See Appendix A). 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 (to which we offered to travel). We did not provide monetary incentives.

3.2 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, 17, 40], our data collection consisted of two 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. The questionnaire prepared us with the knowledge of the applicable computer setup and warning types, as well as any concerns of interest to the participant. The full research protocol and artifacts can be found in Appendices A, B.

3.2.1 Phase 1: Questionnaire

The questionnaire was hosted on the Section 508-compliant website SurveyMonkey, ensuring 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 approved our informed consent form. In accordance with non-deceptive user research [14], the informed consent document on the first page discloses the purpose and procedure of the study, reports minimal risk to the participant, cites potential benefits, and provides the option to exit the questionnaire or continue to the questions. We note in the informed consent form, as well as the in-person interview, the potential benefits for participants, including an increased understanding of browser security warnings' accessibility via screen reader, which can lead to potential improvements in the future. The questionnaire inquires about the browser, operating system, and screen reader respondents typically use, as well as screen reader proficiency and customization, and perceptions of web security questions. The questions and options were drawn from the WebAIM Screen Reader User Survey [30]. Lastly, there was a field for the preferred method of contact for the respondent to indicate whether they would agree to an in-person interview.

3.2.2 Phase 2: Contextual Inquiry

To recreate the user's working conditions, we adopted a contextual inquiry approach to qualitative research, commonly used to learn what is important to users in the context of their own environment [43]. The interviews were conducted in a natural setting in order to focus on users' experiences in their typical work or home settings where they regularly use their devices [15]. For each of the three warning types, we leverage existing websites that serve to represent an example of the warning in a specific browser. This way, the user navigates and interacts with a warning without any risk.

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 unread e-mail. The contents of the email were sourced from Cornell University's Phish Bowl website, a repository of common phishing emails targeting Cornell University students and staff [50]. 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. This scenario was not conducted for Internet Explorer users as the warning is a duplicate of the the malware warning at the time of this study (See Section 4.1).

Malware and SSL Warning Scenario To minimize task duration, we instructed participants to navigate directly to the example of a malware or SSL warning by reading the source URL aloud while the participant typed into the address bar. Internet Explorer displayed an SSL warning webpage, while for Safari users, navigating to the same page triggered an SSL warning popup to appear.

We set appointments with each participant and traveled to their home. We began the interview by disclosing the purpose of the study, and reminded them 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 warning types available from the browser without posing any safety risk. A full chronological description of events is included in Appendix B.2.

Our semi-structured interview approach leveraged a series of open-ended questions to ask about the participant's re-

action, whether they have encountered the warning before, the steps that are necessary to bypass a warning or return to the previous page, and whether they had suggestions for improving these interactions or the available information on the warning page. All questions are listed in Appendix B.5. We took observational notes labeled with a unique ID number assigned to the participant. 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 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 [31, 41]. Minimizing the potential for harm is pertinent in studies involving this population within security and privacy contexts. To this end, we made the deliberate choice to instruct participants to visit benign examples of warning websites that displayed warning content, instead of "live" vulnerable sites. By visiting websites that served only as examples of warning pages, participants were under no real threat of safety. Participants were informed of this at the start of their task-based interview. The advantage of disclosing the purpose of the study and instructing participants to proceed through the warning example "as they normally would" led to meaningful discussions with the participant about their typical behavior when faced with warnings, while posing no safety risk to the user.

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. We also 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 [26]. We also alerted the participant to any unusual noises from our activities, including starting, pausing, or stopping a video recording. Interactions with service animals in the vicinity were avoided, as suggested by Henry [26].

3.4 Thematic Analysis

We chose a thematic analysis process for our analysis method, which Boyatzis recommends as the normative approach for analyzing qualitative information [8]. Only one researcher was involved in the analysis procedure, including code and theme development. Following each interview session, video recordings were manually transcribed and carefully reviewed for accuracy. The coding procedure of interview data and observational notes involved a five-step procedure based on the foundational work of Braun and Clarke [9], which includes: (1) becoming familiar with the dataset, accomplished through manual transcriptions and multiple reviews of the transcripts, (2) generating initial codes for the entire dataset, accomplished through three rounds of labeling participant quotes that capture their decision making process or pain points, (3) examination of the codes to search for potential themes through organization of participant quotes into broader patterns, (4) developing and reviewing the candidate themes, (5) refining, defining, and naming the themes. Boyatzis also guided our code and theme generation process, stating that a "good code" is one that captures the qualitative richness of a phenomenon, and defining a theme as "a pattern in the information that at minimum describes and organises the possible observations and at maximum interprets aspects of the phenomenon" [8]. As such, themes emerged by organizing codes into broader patterns of meaning across the entire dataset among all participants. Based on Fereday and Muir-Cochrane's work on demonstrating rigor using thematic analysis [20], credibility and trustworthiness were established through the use of raw interview data, including direct participant quotes, throughout the process of identifying themes.

4 Results

Of the sixteen subjects who responded to our questionnaire, eight individuals agreed to an in-person interview. All respondents self-identified to have a level of visual impairment. The small sample size comes close to that of similar studies investigating visually impaired users' security experiences that involved 10-15 participants [17, 39]. Our study sample size was limited due to the inherent difficulty of recruiting users of this population who are available for an interview at their home or workplace. This paper acknowledges that the small sample size may not result in generalizability in the traditional sense. This concern is exacerbated by the difficulty of replicating a methodology that varies depending on participants' preferred browsers and computer setups, given the

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 2: 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.

changing landscape of popular technologies. However, Myers asserts that a major strength of the qualitative approach is that it allows for deeper explorations that result in providing sufficient details for capturing the idiosyncrasies of situations [38]. According to Myers, an in-depth, detailed, and more personal level of understanding often results from qualitative studies confined to a small number of subjects. In our study, the sample of eight individuals produced a large volume of data in the form of interview transcripts and observational notes.

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. In future studies, 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) [30]. 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.

ID	Browser	Phishing	Malware	SSL
U07	Safari	✓	Offline	✓
U08	Safari	Incomplete	✓	✓
ID	**Browser**	**Phishing/Malware**		**SSL**
U01	IE 9+	✓		✓
U04	IE 8	Offline		✓
U09	IE 9+	Offline		✓
U10	IE 9+	✓		✓
U11	IE 9+	✓		✓
U12	IE 9+	✓		✓

Table 3: Warning scenarios that were successfully completed marked with a check mark (✓), and issues preventing participants from completing a scenario are described.

4.1 Warning Scenarios

Out of the eight total participants, 50% of the users successfully completed all of the scenarios, 25% completed 2/3 of the scenarios, while the remaining 25% completed half of the scenarios. The incomplete scenarios were not due to participant errors, but rather, unexpected issues or inconsistencies with the warning example websites that arose during interviews, despite the interviewer having tested the web pages prior to the interview. Table 3 displays the completed warning scenarios, as well as a summary of the issues that prevented participants from completing them. At the time this study was conducted, Internet Explorer 9+ did not have a phishing-specific warning and displayed a malware warning for both the phishing and malware scenarios, resulting in only one scenario for both warning types for the six individuals using this browser.

Other reasons that warning scenarios were not completed were either researcher error in instruction, or because a warning website could not be accessed at the time. 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 these obstacles, 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.

4.2 Common Themes

Website Familiarity. 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 (mistaking the malware warning for an SSL warning) 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.*"

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 do so.

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 sce-

nario U12 was presented with the options "Click here to close the web page," "Continue to this website (not recommended)," and "More information." U12 inquired aloud about whether the link to close the web page 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 web page 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 web page, 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'.*"

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.*"

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.*"

Checking the Browser Toolbar. Two of the participants that used Internet Explorer recalled encountering warnings in the browser's toolbar. Upon encountering the SSL warning example, U09 noted that he would immediately consult the toolbar 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 homepage, 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.*"

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.*"

4.3 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. 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.*" 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.*" 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.

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 "Reported unsafe website, navigation blocked" 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.

We observed different speeds of screen reader narration, due to participants' chosen screen reader settings (none of the participants changed their settings for the purpose of the interviews). 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 "*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."*

5 Reflections on 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.

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 Section 4.1). 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 and security mechanisms. 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 external websites that are meant to serve this purpose, but may not always be reliable.

Phishing Warning Scenario Privacy Concerns. The phishing warning scenario highlights another challenge of creating an authentic scenario, without creating other issues. As described in Section 3.2.2, when U07 was tasked with signing into a new Gmail account (for the purpose of viewing a typical phishing email, leading to a phishing warning example page), his existing, yet empty, email inbox was displayed. While we intended to minimize task duration and unnecessary steps,

U07 spent a few minutes to figure out how to sign out of their Gmail account. One potential solution is to ask participants to use an incognito window, which provides a blank slate for the user, solving the potential privacy issue and prevents similar inconveniences. 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.

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 skill 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.

6 Key Findings

Findings Consistent with Sighted Users. We found common themes across findings from our pilot study with visually impaired users and those from prior work involving sighted users. In a study of the correlations between website reputation and warning adherence for Google Chrome users, Almuhimedi *et al.* reported several observations consistent with our 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, as did one participant in our study.

As was suggested by Almuhimedi *et al.*, the wording and phrasing in warnings can be modified to provide education to users and prevent the common misconceptions that lead to web safety risks. 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 warnings could be preventing an attack that the operating system's antivirus software may not protect them from, could also be necessary. Having 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 browser security warnings research 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 Section 4.2.

The prevalence of these themes in both sighted and non-sighted users indicates that these modifications 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 examine the design decisions that are to the most benefit.

Browser Security Warnings Interface Standards. Our findings suggest a number of potential improvements. There may be a need for more uniformity of warning language that conveys the meaning of available actions. Standards of phrasing that provide clear indication as to the destination that a button or link would lead the user to often results in uncertainty, and is worth considering. In addition, standards of page structure and hierarchy of page elements could be of benefit, at least for warnings within the same browser. A normative user interface that standardizes the placement of available options would help screen reader users have a more consistent, useful, and therefore effective, experience when they encounter the warning. It may 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, 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 the case with U01 interacting with a malware warning), there could instead be a disabled button or clear, consistent 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. Browser security warning language is paramount when visual indicators such as graphical elements may be missed, ignored, or not interpreted

in the same manner 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" [24]. 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.

Implications of Screen Reader Interactions. Our findings reveal new insights and confirm previous work on how visually impaired users interact with websites. As discussed in Section 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 [12, 48, 52]. Our findings confirm these 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 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. Screen readers were also observed to narrate multiple blank lines at a time, which users spent time skipping past. 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.

7 Conclusion

Understanding the experience of visually impaired user with browser security warnings is a subtle and poorly understood problem. To bridge this knowledge gap, we propose a research methodology that considers and merges the best practices of conducting browser security warning research with human subjects with those of working with the visually impaired.

Using specially developed 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 an inconsistent experience across warning types, receiving no benefit from 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.

Acknowledgments

An early version of this work appeared in the 2015 Workshop on Inclusive Privacy and Security (WIPS), a workshop held in conjunction with the USENIX Symposium On Usable Privacy and Security (SOUPS) [33].

References

[1] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2015.

[2] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proceedings of the USENIX Security Symposium*, 2013.

[3] Hazim Almuhimedi, Adrienne Porter Felt, Robert W Reeder, and Sunny Consolvo. Your reputation precedes you: History, reputation, and the chrome malware warning. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2014.

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

[5] Ljudevit Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. Warning Design Guidelines (CMU-CyLab-13-002). Technical report, CMU CyLab, 2013.

[6] Yevgen Borodin, Jeffrey P. Bigham, Glenn Dausch, and I. V. Ramakrishnan. More than meets the eye: A survey of screen-reader browsing strategies. In *Proceedings of the International Cross Disciplinary Conference on Web Accessibility (W4A)*, 2010.

[7] Yevgen Borodin, Jeffrey P Bigham, Glenn Dausch, and IV Ramakrishnan. More than meets the eye: a survey of screen-reader browsing strategies. In *Proceedings of the International Cross Disciplinary Conference on Web Accessibility (W4A)*, pages 1–10, 2010.

[8] Richard E Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[9] Virginia Braun and Victoria Clarke. *Thematic analysis*. American Psychological Association, 2012.

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

[11] José Carlos Brustoloni and Ricardo Villamarín-Salomón. Improving security decisions with polymorphic and audited dialogs. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2007.

[12] Maria Claudia Buzzi, Marina Buzzi, Barbara Leporini, and Fahim Akhter. User trust in ecommerce services: Perception via screen reader. In *Proceedings of the International Conference on New Trends in Information and Service Science*, 2009.

[13] Disability Rights Commission. *The Web: Access and Inclusion for Disabled People; a Formal Investigation*. The Stationery Office, 2004.

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

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

[16] Giuseppe Desolda, Francesco Di Nocera, Lauren Ferro, Rosa Lanzilotti, Piero Maggi, and Andrea Marrella. Alerting users about phishing attacks. In *Proceedings of the International Conference on Human-Computer Interaction*, 2019.

[17] Bryan Dosono, Jordan Hayes, and Yang Wang. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[18] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 2008.

[19] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving SSL warnings: Comprehension and adherence. In *Proceedings of the Conference on Human Factors and Computing Systems*, 2015.

[20] Jennifer Fereday and Eimear Muir-Cochrane. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods*, 5(1):80–92, 2006.

[21] B. J. Fogg, Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, John Shon, Preeti Swani, and Marissa Treinen. What makes web sites credible? a report on a large quantitative study. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 2001.

[22] Ombretta Gaggi, Giacomo Quadrio, and Armir Bujari. Accessibility for the visually impaired: State of the art and open issues. In *Proceedings of the IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2019.

[23] Elaine Gerber. Surfing by ear: Usability concerns of computer users who are blind or visually impaired. In *Proceedings of the International Conference of California State University Northridge Technology and Persons with Disabilities*, 2002.

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

[25] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. *Proceedings of the Symposium of Usable Privacy and Security (SOUPS)*, 2019.

[26] Shawn Lawton Henry. *Just ask: integrating accessibility throughout design*. http://www.uiaccess.com/accessucd, 2007.

[27] Harry Hochheiser, Jinjuan Feng, and Jonathan Lazar. Challenges in universally usable privacy and security. In *Proceedings of Symposium On Usable Privacy and Security (SOUPS)*, 2008.

[28] J Holman, J Lazar, and J Feng. Investigating the security-related challenges of blind users on the web. In *Designing inclusive futures*. Springer, 2008.

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

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

[31] Helen Keller and AFB Connects You. Conducting usability research with computer users who are blind or visually impaired. In *Proceedings of the International Conference of California State University Northridge Technology and Persons with Disabilities*, 2002.

[32] Neil Kumaran and Sam 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.

[33] Elaine Lau and Zachary 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.

[34] Jonathan Lazar, Aaron Allen, Jason Kleinman, and Chris Malarkey. What frustrates screen reader users on the web: A study of 100 blind users. *International Journal of HumanComputer Interaction*, 2007.

[35] Jonathan Lazar, Jinjuan Feng, Tim Brooks, Genna Melamed, Brian Wentz, Jon Holman, Abiodun Olalere, and Nnanna Ekedebe. The soundsright CAPTCHA: An improved approach to audio human interaction proofs for blind users. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 2012.

[36] 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.

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

[38] Margaret Myers. Qualitative research and the generalizability question: Standing firm with proteus. *The qualitative report*, 4(3):9, 2000.

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

[40] Daniela Napoli, Khadija Baig, and Sonia Chiasson. "I'm Literally Just Hoping This Will Work:" Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2021.

[41] 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.

[42] Helen Petrie and Omar Kheir. The relationship between accessibility and usability of websites. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 2007.

[43] Mary Elizabeth Raven and Alicia Flanders. Using contextual inquiry to learn about your audiences. *ACM SIGDOC Asterisk Journal of Computer Documentation*, 20(1), feb 1996.

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

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

[46] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2011.

[47] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the USENIX Security Symposium*, 2009.

[48] Hironobu Takagi, Shin Saito, Kentarou Fukuda, and Chieko Asakawa. Analysis of navigability of web applications for improving blind usability. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 14(3):13–es, 2007.

[49] Mary Frances Theofanos and Janice (Ginny) Redish. Bridging the gap: Between accessibility and usability. *Interactions*, 10(6):36–51, November 2003.

[50] Cornell University. Phish bowl | it@cornell. https://it.cornell.edu/phishbowl.

[51] Markel Vigo and Simon Harper. Challenging information foraging theory: Screen reader users are not always driven by information scent. In *Proceedings of the ACM Conference on Hypertext and Social Media*, 2013.

[52] Markel Vigo and Simon Harper. Coping tactics employed by visually disabled users on the web. *International Journal of Human-Computer Studies*, 71(11), 2013.

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

[54] Min Wu, Robert C Miller, and Simson L Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems*, 2006.

[55] Mary Ellen Zurko and Kenny Johar. Standards, usable security, and accessibility: can we constrain the problem any further. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, 2008.

A Questionnaire

A.1 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)

A.2 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:

A.3 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.

B Contextual Inquiry

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

B.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.

B.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.

B.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.

B.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 B.5 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 B.5 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 B.5 for subsequent questions.*

B.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?

B.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.