GuardLens: Supporting Safer Online Browsing for People with Visual Impairments

Smirity Kaushik, Natã M. Barbosa, Yaman Yu, Tanusree Sharma, Zachary Kilhoffer, and JooYoung Seo, *University of Illinois at Urbana-Champaign;* Sauvik Das, *Carnegie Mellon University;* Yang Wang, *University of Illinois at Urbana-Champaign*

https://www.usenix.org/conference/soups2023/presentation/kaushik

This paper is included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

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

GuardLens: Supporting Safer Online Browsing for People with Visual Impairments

Smirity Kaushik[1], Natã M. Barbosa[1], Yaman Yu[1], Tanusree Sharma[1], Zachary Kilhoffer[1], JooYoung Seo[1], Sauvik Das[2], Yang Wang[1]
[1]University of Illinois at Urbana-Champaign [2]Carnegie Mellon University
{smirity2, natamb2, yamanyu2, tsharma6, dzk2, jseo1005, yvw}@illinois.edu, {sauvik}@cmu.edu

Abstract

Visual cues play a key role in how users assess the privacy/security of a website, but often remain inaccessible to people with visual impairments (PVIs), disproportionately exposing them to privacy and security risks. We employed an iterative, user-centered design process with 25 PVIs to design and evaluate GuardLens, a browser extension that improves the accessibility of privacy/security cues and helps PVIs assess a website's legitimacy (i.e., if it is a spoof/phish). We started with a formative study to understand what privacy/security cues PVIs find helpful, and then improved GuardLens based on the results. Next, we further refined Guardlens based on a pilot study, and lastly, conducted our main study to evaluate GuardLens' efficacy. The results suggest that GuardLens, by extracting and listing pertinent privacy/security cues in one place for faster and easier access, helps PVIs quickly and accurately determine if websites are legitimate or spoofs. PVIs found cues such as domain age, search result ranking, and the presence/absence of HTTPS encryption especially helpful. We conclude with design implications for tools to support PVIs with safe web browsing.

1 Introduction

Visual cues play a key role in how users assess the privacy/security posture of a website [17] but are often inaccessible to people with visual impairments (PVIs) [32, 33]. In turn, PVIs are disproportionately susceptible to a broad range of security risks, such as phishing threats [12, 17] and challenges with web authentication [18, 27] intertwined with privacy risks, such as shoulder surfing [4] and accidentally sharing personal information [6, 7, 42]. Prior research [1, 41] suggests that it is often difficult for PVIs to assess a website's credibility due to the poor accessibility of privacy/security cues, such as whether a website is HTTPS-enabled.

Our work explores ways to make website privacy/security cues more accessible to PVIs. We followed an iterative, user-centered design approach in designing and evaluating a browser extension, GuardLens, that collects and presents key privacy/security cues for a website, so users do not need to perform these checks manually. Based in part on prior work [1, 10, 32] as well as a formative study and pilot study that explored how PVIs assess the privacy/security posture of a website, GuardLens highlights key privacy/security cues. For instance, some security cues from GuardLens, like domain age registration and search result ranking, are relevant to phishing detection, while cues like HTTPS encryption and website owner are valuable general security cues. Guardlens also provides privacy cues, such as whether website images contain Not Safe For Work (NSFW) content to mitigate shoulder surfing and maintain social norms. Together, the privacy/security cues from GuardLens highlight many privacy and security-related threats to the PVIs online.

We aim to answer two main research questions:

- RQ1: How does GuardLens make privacy/security cues of a website more accessible to PVIs?
- RQ2: How does GuardLens help PVIs assess whether a website is legitimate or a spoof?

We conducted our research iteratively in three stages with 25 PVIs: a formative study (n=5), pilot study (n=3), and main study (n=19). The main study is an experiment (lab-based interview study) that builds on the field study and the pilots to directly answers the research questions. In the main study, participants evaluated the accessibility of privacy/security cues and website legitimacy with and without GuardLens.

Results. Our work has yielded novel and significant results.

First, in one easily accessible location, GuardLens presents important privacy/security cues about a website: e.g., whether it is HTTPS-enabled, its domain age, search result ranking. Without GuardLens, PVIs often miss these cues due to inaccessibility or inconvenience.

Second, GuardLens helps PVIs to determine the legitimacy of websites (spoof or not). Participants found privacy/security cues from GuardLens helpful in correctly determining that spoofs were spoofs and that legitimate, popular sites were

not spoofs. However, it also increased their concerns with unpopular sites that were not spoofed. We reflect on the ways future designs can improve the interpretability of these cues.

Third, we observed novel strategies participants used to assess a website's legitimacy without GuardLens. Strategies included externally verifying that a website's URL is highly ranked in a Google search of its title, checking for links related to copyright information and privacy policy in the footer, and reading URLs character-by-character with a screen-reader.

Contributions. This work makes three main contributions: we (1) designed a new tool, GuardLens, to make the **privacy/security cues of a website more accessible** to PVIs; (2) identified privacy/security cues that participants found useful to determine website's legitimacy while using GuardLens and observed **novel strategies** used by our PVI participants to assess website legitimacy while web browsing; and, (3) offer **recommendations to further improve the accessibility of privacy/security cues** for PVIs.

2 Related Work

Prior literature has studied the privacy and security concerns of PVIs extensively [2, 3, 5, 7, 9, 18, 25]. Researchers have highlighted various privacy concerns for PVIs, such as shoulder surfing [4] and accidentally sharing personal information [6, 7, 42] while browsing websites online. The privacy risks often intertwine with various security risks to PVIs, such as email and website phishing threats [12,50], challenges with web authentication [18,27], and the inaccessibility of security cues [10,32]. For instance, Barbosa et al. [10] highlights that although many websites offer visual cues to facilitate access to features, e.g., log-in, such visual shortcuts are not accessible to PVIs. Similarly, Napoli et al. [32,33] found usability and accessibility issues with online resources, e.g., insufficient web browser security indicators and poor accessibility of password managers. It results in poor access to privacy and security-related information online for PVIs, making them vulnerable to various privacy and security risks, such as unauthorized access to personal information and phishing threats.

2.1 Phishing Threats to PVIs

Phishing is a common problem. The Anti-Phishing Working Group (APWG) [8] detected 266,387 phishing websites in 2019, the highest number since 2016. A large body of work has explored *phishing websites* [15, 23, 28, 30, 34, 37, 38, 45, 47, 51, 52]. Xiang et al. [49] identified two major criteria of a phishing site: a) visual similarity to a legitimate site and b) at least one login form for users to input their credentials. Dhamija et al. [17] found that some phishing sites fooled 90% of participants, and existing anti-phishing browsing cues were ineffective. For instance, studies [19, 39] highlight that phishing websites are increasingly using HTTPS. Consequently, checking whether a website is HTTPS protected is no longer effective against phishing. A study on spear phishing emails found that older adults were more vulnerable to phishing attacks than younger adults [36].

Few studies have explored phishing threats specific to PVIs. Blythe et al. [12] investigated the response of blind users to phishing emails and found they used robust strategies for identifying phish based on a careful reading of emails. However, Abdolrahmani et al. [1] found that it is more challenging for PVIs to assess the credibility of phishing sites because of the inaccessibility of security indicators. Sonowal et al. [41] found similar accessibility issues while evaluating browser extensions designed to protect PVIs against phishing websites.

2.2 Website Privacy/Security Cues

Researchers have examined the effectiveness of privacy/security cues and often found them lacking [17, 29, 43]. Dhamija et al. [17] found that 23% of the participants did not look at browser-based cues such as the address bar, status bar, and security indicators, leading to incorrectly assuming phishing websites safe 40% of the time. Other studies have focused on accessibility issues of privacy/security cues for PVIs. Sonowal et al. [41] found a range of accessibility issues for PVIs, such as color-based privacy/security indications, missing instructions, and lack of shortcut keys. Napoli et al. [32] found that passive browser chrome indicators did not help PVIs browse websites securely because they can only see a small portion of a website when using a screen magnifier. The small field of view is more likely to focus on page content than other areas of the browser. Instead, to comprehend the page as a whole, they skimmed pages while completing tasks and skipped over large portions of content to find relevant information from a website. It is insufficient to provide alternative text to describe security cues like lock icons and SSL certificates because users may not actively seek out this information. As a result, the security information can potentially go unnoticed by users.

2.3 How PVIs Assess Site Credibility?

Researchers [24, 31, 32] have observed that blind and sighted users absorb information differently. Sighted users comprehend information from whole to part. They see the whole picture simultaneously and understand the different visual encodings in relation to each other (e.g., identifying a website as a shopping site upon visiting). In contrast, PVIs put together each piece of information to make sense of the picture as a whole (e.g., scrolling through the webpage to explore what the website is about). They often rely on text and use fast tab/scroll down the webpage as an exploration tactic to find relevant information. In this process, screen-reader users skip over large portions of the content to alleviate heavy cognitive loads associated with browsing websites audibly. However, studies suggest [1, 32] that this habit could increase the like-

lihood of missing vital privacy/security-related information, making it challenging for PVIs to assess webpage credibility [1].

Overall, prior work [10, 25, 41, 46] suggests PVIs are often exposed to privacy and security risks online, including phishing, due to poor accessibility of websites and insufficient privacy/security indicators. These insights informed GuardLens' design.

3 GuardLens System Design

We developed GuardLens with two design goals: (1) to *provide quick access to privacy/security information,* such as a website's domain name, and whether it is HTTPS enabled; and (2) *to equip users with information needed to protect them against privacy/security risks* such as phishing attacks. These goals correspond to helping PVIs overcome the *awareness* and *ability* barriers that can hinder users' acceptance of expert-recommended best practices for security and privacy [16]. Details of the design considerations are in the appendix 8.

3.1 System Overview

GuardLens JS was developed in ES6, compiled with BabelJS, and is executable and tested on Chrome, Firefox, Safari, Edge, and IE10+. We incorporated remote backend development used by the browser extension in response to any requests, local storage to handle data requested from API services, general helpers and algorithms to run required design features, and messages/prompts for users to make informed decisions. Requests to the backend were made over HTTPS, and the endpoints required no user data. For example, the endpoint to return TLS certificate information only requires a URL request parameter. The backend was hosted securely in our university servers with restricted access to our research team. (see Figure 2 in the Appendix). The workflow contains client requests sent to different services and a synchronous process of the data in server endpoint to present the results in the UI. We have open-sourced GuardLens [1]. GuardLens is an unlisted browser extension; only recruited participants received a download link.

The GuardLens web browser extension interacts with backend API endpoints, and the app engine creates queries from user requests (see Figure 2 in the Appendix). The app engine backend receives requests from a script embedded into the browser extension. These requests are sent automatically from the browser extension to the system's backend, where the system has endpoints to each of the cues supported by the browser extension. TensorFlow JS[2], Universal Sentence Encoder [14], and NSFW JS[3] are some of the notable helpers/algorithms used in the backend to build the privacy/security information features.

GuardLens also uses local storage to save users' preferences if they choose to opt out of (1) seeing a GuardLens pop-up for a particular website, or (2) seeing a particular type of information block for all sites in the future.

3.2 Interface Details

Guided by our design goals, we implemented GuardLens as a technology probe [26] that gives users easy access to privacy/security-related cues about a website upon request. GuardLens is a browser extension that consists of a collection of cues meant to surface pertinent privacy and security information about the website that one is currently browsing.

After installing GuardLens, participants read and reviewed the privacy policy for our study, and how data will be used for this research. Participants then chose whether they would consent to start using Guardlens or wish to uninstall it (see details in Figure 1 in Appendix). After users consented on this disclosure interface, they were prompted with a user input field to provide a participant ID. We used "Screen A" for the consent interface and the prompt message.

Once a participant entered their ID and clicked "OK", the GuardLens main interface ("Screen B" in Figure 1 in Appendix) appeared, displaying the privacy/security information of the website presently in focus in the form of information blocks (see "Screen B" in Figure 1 in Appendix). Each information block consists of an expandable drop-down with a ***"Tool Tip"*** and ***Actionable Suggestions***. Below we discuss each information block in the order presented in the GuardLens interface. We chose and ordered these seven S&P cues based on prior work [20, 32, 40] and findings from both our formative and pilot studies.

HTTPS Encryption: This information block highlights whether or not a site uses HTTPS. Prior work [32] suggests that the HTTPS lock icon and/or SSL certificates are often inaccessible to PVIs. To improve the accessibility of security information, the backend system of GuardLens parses TLS certification when a user visits the site. Users can find two additional messages by clicking the expandable drop-down: a) tool tip: *"Based on the actual information from the website's security certificate"*, and b) actionable suggestion: *"What you can do: You may choose not to send your information to this website such as payment or personal information"* if the site lacks HTTPS encryption.

Website Owner Identity: This information block identifies the entity that owns the website. We included this cue for reasons similar to adding the HTTPS information. Additionally, browsers share this information when displaying certificate information, and participants in the formative study found it useful. Clicking into the expandable drop-down, users can find two additional messages: a) tooltip: *"Based on this website's security certificate"*, and b) actionable suggestion:

[1] GuardLens source code: https://github.com/guardlens22/GuardLens
[2] https://www.tensorflow.org/js
[3] https://nsfwjs.com/

"What you can do: You may be more cautious about sending your information to this website not knowing who owns it.". The backend app engine parses the site's TLS certification to extract this information.

Domain Name: This information block states the domain name of the website word for word. We included this cue because some phishing URLs try to confuse users about the domain name, e.g. bestbuy.greatshops.com. Clicking into the expandable drop-down, user find two additional messages: a) tool tip:*"Based on this page's address"*, and b) actionable suggestion: *"What you can do: You may leave this website if it is not the intended website you wanted to access"*. The backend app engine parses the site's URL to extract this information.

Search Result Ranking: This information block presents a website's rank in Google search results. In the formative study and the pilots, participants evaluated the legitimacy of a site by manually checking if the site's domain appears in the top 5 of a Google search of its title, suggesting a need for the cue. Clicking into the expandable drop-down, user can find two additional messages: a) tool tip:*"Based on website title, search results are from Google search"*, and b) actionable suggestion: *"What you can do: If the website does not appear in the top 5 search result it is more likely to be a phish. If you are uncertain, do not enter any personal information."* The backend app engine submits a search with the website title as the query term via Google search APIs and determines whether the site is in the top 5 of the returned results. To the best of our knowledge this cue works with most top websites.

Domain Registration and Age: This information block shows *"The website domain was registered 27 years ago."* (see Screen B (Figure 1). We included this cue based on participants' suggestions from the formative study and the pilots. Clicking into the expandable drop-down, users can find two additional messages: a) tool tip:*"Based on website domain registration"*, and b) actionable suggestion: *"What you can do: Research suggests that younger websites are more likely to be phish. In particular, most phishing sites are less than 2 years old."* We added this actionable suggestion for domain age based on prior phishing studies [22,34,35,44]. The backend app engine parses the site's domain registration from the Prompt API [4] (Whois Lookup API that provides registration details) to extract this information.

External Links: This information block indicates how many external links point out of the website. We included this cue for two reasons. First, phishing sites often reuse the HTML code of the legitimate site they are attempting to spoof, change the part that launches the phishing attacks (e.g., login) and leave the rest intact, which means they often have many links pointing to the original site. Second, deceptive sites with click bait often have many external links [48]. Clicking into the expandable drop-down, user can find two additional messages: a) tool tip:*"Based on the destination address of all links"*, and b) actionable suggestion: *"What you can do: If this number is high, you may want to pay close attention to links before clicking them. You also leave the website if you think it is deceptive or masquerading as a real website, such as a fake website with links that point to the real website."* The backend app engine parses the site's HTML code to identify and count the external links to derive this information.

Image Description: This information block shares whether images on the screen show Not Safe For Work (NSFW) content. We included this cue because the unexpected inclusion of NSFW content can be a signal to help PVIs assess if they are browsing the website they intended to. Moreover, particularly in cases where the PVI may be near bystanders, they can use this information to assess whether or not they should leave the website up in keeping with the social norms of their situation. Clicking into the expandable drop-down, the user can find two additional messages: a) tool tip:*"Based on an automated standard detection of indecent or inappropriate images on the screen, which suggest images show content that may not be safe for work."* as a tool tip, and b) actionable suggestion: *"What you can do: You may want to leave this page if you are not comfortable with potential bystanders seeing your screen."* The backend uses existing trained machine learning models for detecting objects in images and image safety features (e.g., NSFW JS).

4 Methodology

We followed an iterative user-centered design process with a series of three studies: initial formative study, pilot of the main study, and the main study. This research is IRB approved. Our interdisciplinary team has expertise in privacy/security, human-computer interaction, and accessibility. One team member self-identifies as a person who is blind.

4.1 Main Study

We conducted lab-based interview experiment to explore the two main research questions stated in Section 1. These research questions were informed by the results from the formative study and the subsequent pilots. In the formative study, which included five participants, we deployed GuardLens as a technology probe [26] to field-test usefulness of privacy/security cues users while browsing websites. We then improved GuardLens design based on the results to better support PVIs needs. Next, we **piloted** the new design with three participants and made further improvements. Finally, our **main study** included 19 participants. Details of the formative study and the pilot study are included in the appendix 8.

4.1.1 Study Design

Due to the pandemic, we conducted the study remotely using Zoom. The one-hour session began with the study tasks

[4] https://www.crunchbase.com/organization/prompt-api

embedded within the interview questionnaire, followed by an exit interview. Participants received a $30 USD gift certificate upon completion of the session. The study tasks followed a within-subject design, where all participants browsed six websites. These websites were selected from three categories: popular, unpopular, and spoof across seven domains: finance, e-commerce, accessibility, news/media, education, healthcare, and productivity. ***Popular sites*** were chosen from sites in the top 1,000 Alexa ranking[5]. ***Unpopular sites*** were chosen from sites ranked 5,001+ in the Alexa ranking. The popular and unpopular sites are not spoofs. For ***spoof sites***, we developed spoofs of two popular sites for our target user population: amazon.com (Amazon) and nfb.org (National Federation of the Blind). We created these spoofs to be visually similar to their legitimate counterparts, similar to prior studies [33, 49]. The domain names of the spoof sites sounded identical to the original sites when read out aloud by a screen reader but were spelled differently: i.e. amaZaunn.com vs. amazon.com. Also, these spoof sites were safe to browse. Feedback from the formative study suggested GuardLens' usefulness depends on the popularity of and familiarity with the site. We thus explored these factors in the main study by having participants visit six websites that varied in familiarity and popularity, simulating real-world browsing. It helped us to test GuardLens' effectiveness at assessing site security, privacy features, and legitimacy across popular (often familiar), unpopular (often unfamiliar), and spoof (of popular) sites. Table 4 (Appendix) lists all the websites used in the main study.

For the study tasks, we emailed participants links to the websites we chose. We followed a scenario-based approach, commonly used in the prior work on phishing [17]. Our scenario stated, *'Imagine that you receive an email message that asks you to click on one of the following six website links. Imagine that you decide to click on the link to see if it is a legitimate website or a "spoof" (a fraudulent copy of that website). Please browse three websites using the GuardLens tool and the other three without the tool.'* We randomly selected two popular and two unpopular websites from a pool of four popular and four unpopular sites (see Appendix Table 4). The same two spoof sites were presented to all participants. Each participant browsed three sites (one popular, one unpopular, and one spoof) with GuardLens and another three sites without GuardLens without knowing the conditions (popular, unpopular, spoof sites). Note that, we counterbalanced the order of presentation of websites using Guardlens and without it. Some participants were first presented with GuardLens, followed by browsing websites without it and vice versa.

After browsing each website, participants were asked five 5-point Likert scale questions and three open-ended questions [6]. The Likert scale questions asked participants to rate legitimacy, familiarity, accessibility, ease of assessing privacy and security of the website, and whether they would recommend the site to their friends. They were also asked to provide reasoning for each rating. We also asked participants an open-ended question about the strategy they used to detect the privacy/security features of the website. If a participant read the URL of the website character by character, we asked open-ended questions about what prompted them, and how often they do so in daily life.

After participants completed browsing the six sites and answering the questions, which took about 45 minutes, we ended the study with a 15-minute exit interview. In the exit interview, we asked participants open-ended questions about their experiences of browsing the sites with and without GuardLens. Figure 5 (Appendix) illustrates the main study design.

4.2 Participants.

We recruited participants through the National Federation of Blind (NFB) mailing list and Reddit (r/Blind). Prospective participants took a screening survey with basic information on age group, occupation, self-reported visual abilities, and their regularly used email services, browsers, and screen readers. Eligible participants must (1) self-identify with visual impairments and (2) regularly use screen readers and the Chrome browser. The goal was to ensure that participants were familiar with the technical environment we provided. Then we identified 19 eligible participants (nine female, 10 male) to participate in our interview session (see appendix Table 3). 15 participants self-described as individuals who are blind and the other four self-described as individuals with low vision. All 19 participants used screen readers. Only P17 did the formative study and no participants did the pilot study.

We provided participants an online consent form within the screening survey, informing about our study procedure and data protection policy. We informed participants that this study was designed to improve the accessibility of privacy/security of browsing websites online.

4.3 Ethics

Our study was approved by our IRB. Prior to each of the three studies, participants signed a consent form, including an agreement to audio/video record. At the start of each session, we re-confirmed their consent and communicated our pseudonymization procedure. We also reminded them their participation was entirely voluntary.

4.4 Data Collection and Analysis

Upon receiving participant consent, we asked them to share their screen and began recording. We also took notes during the study. Our analysis was driven by our main research questions. To answer our questions on the ease of accessing

[5] Alexa Internet was a web traffic analysis company, owned by Amazon. It was discontinued on May 1, 2022. https://www.alexa.com/

[6] GuardLens study questions: https://github.com/guardlens22/GuardLens

privacy/security cues on a website, assessing a website's legitimacy, and security strategies participants employed, we first qualitatively analyzed participants' responses using thematic analysis [13]. Two co-authors (coders) manually and independently generated initial codes that capture meanings of the same subset of our interview data at a fine-grained level (usually at the sentence level). Then, the two coders discussed, and converged their codes into a code book of 50 unique codes ranging from easy access to GuardLens, trusted website footer links, and familiarity with site. We calculated the inter-coder reliability is 0.88 (Cohen's Kappa), which is considered good [21]. Next, the two coders used the agreed-upon code book [7] to code the rest of the responses. We followed an open coding method to explore how participants used GuardLens and why they found it helpful or not. We added new codes to the code-book when existing codes could not capture the data, until the code saturation was achieved. We then grouped all codes into higher-level themes, such as tool support, legitimacy assessment, and website content familiarity.

We next employed quantitative methods to assess if use of GuardLens resulted in statistically significant differences in: (1) participants' perceptions about the accessibility of privacy/security cues on a website; and, (2) participants' ability to differentiate between legitimate and spoofed websites. We also explored how independent factors — such as the accessibility of a website and participants' familiarity with the website — impacted users' ratings for assessing a website's privacy/security and legitimacy. To do so, we employed a mixed-effects regression analysis (R lme4 [11] package): we included participants' familiarity and perceived accessibility of a website as covariates, participants' use (or not) of GuardLens as the independent variable, and included a random-intercepts term for participant IDs since each participant browsed and rated multiple sites.

5 Results

We first examine participants' perceived ease of accessing privacy/security cues with or without using GuardLens for three types of websites: spoof, popular (legitimate), and unpopular (legitimate) (RQ1). Next, we evaluate whether participants correctly determine the website's legitimacy (i.e., spoof or not) with or without using GuardLens for each type of website (RQ2). We hypothesized that GuardLens should make privacy/security cues more accessible and help PVIs more easily assess website legitimacy.

5.1 Ease of Accessing Privacy/Security Cues

We asked participants to rate and provide reasoning for the ease of accessing the privacy/security cues of a website on a 5-point Likert scale (the "ease rating"). Ratings 4 and above mean participants found it easy to access the privacy/security cues; ratings 2 and below indicate that participants found it difficult, and a rating of 3 indicates neutrality. Figure 3 in appendix 8 shows the ratings for different types of websites with or without GuardLens. Table 1 in appendix 8 summarizes the most accessible privacy/security cues participants used with or without GuardLens.

5.1.1 Spoof Sites

We hypothesized that PVIs would access privacy/security cues on spoof websites more easily with GuardLens than without. Our results confirm the hypothesis.

Each participant visited a spoof of two sites, Amazon and the National Federation for Blind (NFB), which are well-known to our target user populations. If participants were asked to browse the spoof NFB site (eneffbee.org) using GuardLens, then they would browse the spoof Amazon (amazaunn.com) without using GuardLens and vice versa.

We used linear mixed-effect regression analysis to determine how GuardLens impacts participants' perceived ease of accessing privacy/security cues. The ease rating was the dependent variable, while using GuardLens or not was the independent variable. The familiarity rating and the accessibility rating of the site from the specific participant were covariates. We also included a random intercept term for each participant ID to account for repeated observations. The R lme4 model is: $ease = tool + familiarity + accessibility + (1|pid)$

Finally, we estimated the statistical significance (p-values) of the fixed effects with the R car::anova function (type III Wald Chi Square test). The evidence suggests that GuardLens made privacy/security assessments easier for PVIs as they browsed spoof websites. Participants gave significantly higher ease ratings when browsing spoof sites with GuardLens than without (estimate coefficient = 0.9152, $p<0.05^*$). Below, we present qualitative results providing additional context for why, and distill our findings into a key takeaway.

Without GuardLens, about 47% of participants gave a rating of 4 or above, while 53% gave a rating of 3 or below for ease of accessing privacy/security cues on spoof sites. It suggested that participants found it difficult to assess the privacy/security of spoof sites without GuardLens' cues.

Six participants (33%) checked the website's URL character by character using a screen reader, which helped them determine the site was a spoof. While three out of these six participants habitually checked for URLs character by character, the other three were primed by the URL's odd pronunciation.

Some participants checked a combination of specific privacy/security cues. For instance, those (16%) who searched the site for layout and footer information (e.g., contact us, privacy links, and copyright information) also checked for

[7] GuardLens study codebook: https://github.com/guardlens22/GuardLens

HTTPS. For instance, P11 gave an ease rating of 4 for the spoof NFB site because, *"It's a familiar website. I recognize the link, and there is https on the top"*. Note that participants gave an ease and legitimacy ratings independently; in this case, though the NFB site was spoofed, the participant still believed it was easy to access privacy/security cues without GuardLens, and ultimately made an incorrect determination.

With GuardLens, the majority (74%) of participants rated ease of accessing the privacy/security cues on spoof websites 4 and above. Participants stated GuardLens cues about a website's domain age and (lack of) appearance in the top five Google results raised suspicion, prompting them to manually check the URL character-by-character with their screen reader. For example, P8 rated ease of accessing privacy/security cues a 5 when visiting the spoof NFB site (eneffbee.org) based on the cues from GuardLens because, *"It was easy. It (website) was registered 10 months ago, 527 links go to other websites, and I spelled the URL—that's not them."*

Unlike P8, P13 ignored the GuardLens cues on the spoof amazaunn.com site. She checked all the cues, then stated *"I can't understand why GuardLens stated domain age as 11 months."*, as this information contradicted her expectation about Amazon's age. P13 assumed that Amazon's security certificate was renewed 11 months ago, then ignored Guardlens' domain age warning and assessed the site as credible based on the website footer links. This finding suggests that when GuardLens cues contrast with user expectations, some users may doubt the cue itself. We articulate relevant design implications for GuardLens in the discussion.

Observation 1: For spoof sites, GuardLens cues prompted many PVIs to check the URL character by character, making it significantly easier for them to assess the privacy/security of these websites.

5.1.2 Popular Sites

We hypothesized that people with visual impairments would rate ease of accessing the privacy/security cues on popular websites to be higher when using GuardLens than when not. Our results support this hypothesis. When using GuardLens, participants rated the ease of accessing privacy/security cues on popular websites significantly higher (estimate coefficient = 1.208, $p < 0.0005^{***}$). We highlight participants' reasoning for preferring GuardLens and provide a conclusion in observation 2.

Without GuardLens, approximately 47% of participants rated ease of accessing privacy/security cues of a popular website 4 and above. They often relied on checking the HTTPS encryption in the URL and the website footer information, such as the presence of copyright and privacy links. Those who gave ratings of 3 and below (53%) were unsure how to check a website's privacy/security cues.

With GuardLens, approximately 95% of participants rated ease of accessing privacy/security cues 4 and above for popular sites. Most relied on GuardLens because the tool consolidated website's security-related information in one place. For instance, P19 said*"Everything I needed to know about the website was in one place. I didn't have to look at all other places. It was a lot easier."* Participants further reported they found GuardLens' security information accurate and trustworthy. P7 said they browsed the website footer and found the *"Copyright info matched with GuardLens domain age."* Some of the security cues from GuardLens that participants found particularly helpful were domain age and HTTPS encryption information.

Observation 2: For popular (legitimate) sites, GuardLens significantly eases PVIs' access to a site's privacy/security cues by consolidating them in one place.

5.1.3 Unpopular Sites

We hypothesized that people with visual impairments would rate ease of accessing the privacy/security cues on unpopular websites to be higher when using GuardLens than when not. We did not observe strong evidence to support this hypothesis. While the descriptive statistics show that people gave higher ratings using GuardLens, using GuardLens was not a significant factor in the mixed-effect regression model ($p>0.05$). We further explore why by evaluating participants' reasoning and provide a conclusion in observation 3.

Without GuardLens, 36% of our participants gave ratings of 4 and above for ease of accessing the privacy/security cues of a website. Participants in this rating group often checked for three cues: HTTPS encryption in the URL; the presence of a privacy policy link in the website footer; and the general readability, accessibility, and layout of the website. For example, while browsing a productivity site (openoffice.org), P18 reasoned that it was easy for him to assess the privacy/security of the site because *"(The site was) built like other ones, and there's privacy policy link."* He was not familiar with the site so he browsed it thoroughly and found it accessible, similar to the other websites he often visits.

Some participants provided unique reasoning for their rating. While browsing a money-transferring site (zapsend.com), P4 reasoned that the website appeared in the top 5 Google search results, so it was easy to assess its privacy/security. Although he navigated through the website, he did not rely on the features within the site to assess its privacy/security. Rather, he verified whether it was a spoof or not by googling it and then matching the URL of the search result with the website we gave him to browse. Another participant (P11) visiting a shopping site (zolucky.com) accessed the website's SSL certificates by clicking on the lock icon near the address bar to check its domain registration date. Since he found that the website was registered and the security certificate was valid, he gave the rating 5 for ease of accessing privacy/security of

the site. Interestingly, P16 assessed the privacy/security of the same shopping site based on customer reviews for its products. *"It didn't take me a lot of time to realize there were no customer reviews. The cursor kept moving around."* She also found that the website had poor accessibility features, and the website footer did not include a privacy policy link. She concluded *"Even if it has https, I wouldn't trust it."* While we focused on assessing how well GuardLens helps participants identify phish, participants also assessed other types of threats. For example, here the site was not a spoof, but still seemed untrustworthy to this participant.

21% participants gave a rating of 3, and 47% participants gave a rating of 2 and below because they were unfamiliar with the website and uncertain of their assessment. For instance, P5 rated an unpopular audiobook site 3 *"because I am not familiar with the website. I am not very knowledgeable on website security and domain."* Similarly, P14 and P15 were uncertain because they were unaware of what type of data the sites collected from them. However, while browsing an online learning site from another country, P15 felt skeptical, *"I'm not certain of my assessment, it was much more difficult. I have my own biases because it's in Nigeria. I would be hesitant to buy something from a website in another country."* In the case of a financial money transfer website, P12 mentioned that *"I think with all these websites, it's very hard just by looking at it without entering personal information."* Participants also googled the websites; and checked for layout, content, and accessibility. P9 said, *"the score goes down because I couldn't find a Google result with website link. But the actual website looked legitimate."*

With GuardLens, more participants (42%) gave a rating of 4 and above for ease of accessing privacy/security cues of unpopular sites. It suggests that although we observed mixed results about the effectiveness of GuardLens on unpopular sites, the tool improves accessibility. Participants relied on GuardLens to access privacy/security cues about the website. However, even with GuardLens, they found it tougher to assess the privacy and security of unfamiliar websites. Those who gave ratings 3 (26%) or 2 and below (32%) found the information from GuardLens confusing, especially for unpopular sites hosting illegal content such as audiobook torrents. For example, while browsing an audiobook site (http://audiobookbay.ws/), P2 said *"It was difficult because the info in GuardLens was contradictory. It was in the top 5 search results and had low external links but it also had warnings. It was not clear to me. They might be illegally sharing audiobooks but not really trying to get my information."* According to P2, although GuardLens suggested two positive features for the site, it also gave warnings such as the site lacks HTTPS encryption, and the site has a younger domain, suggesting that it may not be safe. In such cases, even though GuardLens provided access to privacy/security information, it was insufficient. An important note: by "legitimate" websites, we mean sites that are not spoofs — not that the website is "secure" and harm-free. The audiobooks website in this example hosts torrents for audiobooks which is illegal in the US. However, the website is still safe to browse unless the user downloads anything from it. In that case, maybe they could download some potentially malicious files.

Observation 3: GuardLens privacy/security cues for unpopular (legitimate) sites are less helpful. Lack of familiarity with a site, and sometimes mixed (positive and negative) cues, seem to complicate user assessments.

5.2 RQ2: Assessing Website Legitimacy

We asked participants to rate the legitimacy of the websites on a 5-point Likert scale, where a high rating (>3) means that the user thinks the website is not a spoof or a phish. We also asked about their reasoning for the rating, and the security strategies used to assess legitimacy across the three website types (spoof, popular, and unpopular). We used the same spoof websites described in Section 5.1.1 for assessing site legitimacy. Figure 4 in appendix 8 shows ratings for different types of websites with and without GuardLens. Table 2 in appendix 8 summarizes the most popular strategies participants used to assess website legitimacy with and without GuardLens.

5.2.1 Spoof Sites

We hypothesized that PVIs would rate the legitimacy of spoof websites lower with GuardLens than without. Our results confirms this hypothesis. We performed a linear mixed-effect regression to determine Guardlens' impact on the perceived legitimacy of a site. The R model is:
$legitimacy = tool + familiarity + accessibility + (1|pid)$

We estimated the p-values of the fixed effects using the car::anova function (type III Wald chi-square test). We found statistically significant evidence suggesting that GuardLens impacted participants' legitimacy ratings for spoof websites (estimate coefficient = -0.8279, $p<0.05^{*}$). Participants gave a lower legitimacy rating for spoof sites when they had access to GuardLens than when they did not. We present their reasoning for the rating and provide a conclusion in observation 4.

Without GuardLens, participants tended to ignore the cues of spoof websites and assessed legitimacy based on their familiarity with the website. Only 45% of participants identified the spoof websites. Among these participants, 39% gave a rating of 2 and below and 6% gave rating of 3. The remaining 55% of participants failed to identify the spoof sites and gave legitimacy ratings of 4 and above.

Participants who successfully identified a spoof site without GuardLens often relied on manually reading the URL character by character using a screen reader. Participants also often checked whether the website was HTTPS-enabled. For example, P7 assessed the spoof website they encountered

without GuardLens as illegitimate: *"I don't think this is legitimate. The URL is very suspicious. But the homepage sounds like its clone."* But for the 55% of participants who failed to identify the spoof websites without GuardLens, they all mentioned familiarity with the site as the main reason for their high legitimacy ratings. P3 assessed the spoof NFB site as being legitimate with certainty, *"I am extremely sure the website is legitimate. I have been on the website (before)."*

With GuardLens, participants used cues which are otherwise inaccessible such as domain age of the website. Only 28% of participants failed to identify spoof websites. By contrast, the majority of participants (72%) successfully identified the spoof websites using GuardLens.

When participants used GuardLens, its cues were the most popular security strategy they used in making their legitimacy assessments. The most commonly cited GuardLens cue was the domain age of the website. Indeed, the domain age cue in GuardLens suggested that if the website was less than 2 years old, the site may be more likely to be a phish.

For instance, when visiting the spoof Amazon site, the tool surfaced that the domain age of the website was 9 months. This cue raised suspicion among participants since Amazon has been in the market for over 20 years. Similar observations were made for the spoof NFB site. For instance, P4 gave a low legitimacy rating (2) for the spoof Amazon site, explaining *"I am not sure at all (whether the website is legitimate). Because it seems to be a legitimate site, but GuardLens said it's a website from 10 months ago. So I'll give 2."*

Among participants who used GuardLens but failed to identify the spoof websites, the most common strategy employed was relying on their familiarity with the website content, layout, and accessibility. Even though they may have noticed suspicion-raising privacy/security cues of the spoof websites on GuardLens, they tended to make their assessments relying on familiarity. For example, in explaining why she gave a spoof site a legitimacy rating of 5, P2 said: *"I read the info provided by the tool which indicated that it was secure. I further confirmed by browsing that it is identical to one I browse."*

Observation 4: GuardLens significantly helped participants correctly identify spoof websites by providing privacy/security cues in one place.

5.2.2 Popular Sites

We hypothesized that PVIs would rate the legitimacy of popular websites to be higher when using GuardLens than when not. Our results confirm this hypothesis. We found significant evidence to suggest that GuardLens affected participants' legitimacy ratings for popular websites (estimate coefficient = 0.6405, $p<0.0005^{***}$). Unlike spoof websites, popular sites are most visited and are legitimate websites. Using GuardLens, participants gave higher legitimacy ratings for popular sites. Below we highlight their reasoning for the rating and provide a conclusion in observation 5.

Without GuardLens, 90% of participants gave legitimacy ratings of 4 and above, 10% of participants gave a neutral rating (of 3). The top three security strategies participants used were URL-related strategies (e.g., reading URL character by character using screen reader, checking for HTTPS encryption), browsing content of websites, and relying on familiarity with websites. For popular websites participants browsed daily, they tended to believe that the website was legitimate. Some of the participants (2 out of 19) did not check security cues but made decisions only based on familiarity. P2 and P3 gave high legitimacy ratings to popular websites. The reasons for their decision were, respectively: *"It's the NY times and it also seems consistent with what I know NYT should be."* and *"I visit it a lot (target.com)"*. In addition, other participants *"manually read URL character by character"* or attempted to *"check if the website uses https encryption"*. Since participants used these popular websites in their daily life, they remembered what the website URL should be. Thus, simple strategies such as comparing URLs could help facilitate participant assessment of site legitimacy.

With GuardLens, participants noticed more security cues instead of relying only on their familiarity with websites and checking URLs. 100% of participants gave legitimacy ratings 4 and above and successfully identified popular websites as legitimate. Participants preferred using GuardLens cues as the most popular security strategy to assess website legitimacy. They found three cues most useful: the website's domain age, Google search ranking, and the presence/absence of HTTPS encryption. For instance, P2 assessed a popular website as legitimate because *"GuardLens shows that it is a secure HTTPS website and has been around for 26 years; most phishing sites are not around that long."* Other than website's domain age and search ranking information, P2 also relied on the website's HTTPS encryption information, even though it is not a helpful cue to assess phishing websites.

P3 also noticed more cues, explaining their high legitimacy rating: *"very easy to navigate, headings were readable and in the right spot."* However, familiarity with websites is still a main factor influencing legitimacy perception. P5 explained *"Based on the content of the website and Guardlens information, I feel it is a real site. I don't know how you can copy an entire domain. But the content seemed familiar. I am familiar with NFB, so it is easy for me to recognize the content."* Interestingly, we found familiarity with websites both helped and hindered participants in correctly identifying legitimate websites.

Observation 5: GuardLens significantly helped participants correctly identify the legitimacy of popular sites. Participants leveraged their familiarity with the site, and GuardLens facilitated their assessment by providing cues (e.g. domain age of the site).

5.2.3 Unpopular Sites

We hypothesized that PVIs would rate legitimacy of unpopular (legitimate) websites higher with GuardLens than without. However, our results suggest the opposite. Using the same linear mixed effect model, GuardLens had a significant (negative) impact on participants' perception of unpopular websites' legitimacy (estimate coefficient = -0.6207, $p<0.005^{**}$). This suggests that GuardLens misleadingly increased participants' concern about the sites' legitimacy. Unlike popular websites, some unpopular websites focus less on privacy and security design. GuardLens helped participants identify security issues in unpopular websites, such as a lack of HTTPS encryption. Participants gave low legitimacy ratings based on security issues and unfamiliarity with unpopular sites. While these unpopular sites are not spoofed, their lack of security protection (e.g., HTTPS) is still worth noting to users. Thus, GuardLens can still be useful by presenting cues for multiple threats. Although the only security threat our study assessed was phishing, participants may have given lower legitimacy rating to certain unpopular sites based on poor security properties of those sites in general. We present participants' reasoning in detail below and conclude in observation 6.

Without GuardLens, 36% of participants gave a rating of 4 and above. 32% of participants gave a rating of 3, and 32% 2 and below. Being unfamiliar with these unpopular websites, participants most often used URL-related strategies to determine legitimacy. Since participants are not familiar with the URLs of these unpopular websites, most of them googled the URL. However, some participants did not realize that some of these websites do not use HTTPS. For instance, P14 gave a legitimacy rating of 5 to http://audiobookbay.ws/ and did not check the site for HTTPS. He stated *"I think this website is audiobook service provider."* In addition, P4, P10, P11, and P18 ignored the lack of HTTPS when they browsed unpopular websites without GuardLens.

With GuardLens, 20% of participants rated legitimacy 4 and above, 45% felt neutral (rating 3), and 35% rated 2 and below for unpopular websites that are not spoofs. GuardLens identified and presented some security issues of these websites, which made participants concerned about these sites' legitimacy. For example, GuardLens helped participants notice some unpopular websites not using HTTPS. P1 said *"(I knew) because the tool told me that it was not secure and warning about encryption."*

Observation 6: GuardLens highlighted security issues (e.g., no HTTPS) in some unpopular websites. These (negative) cues made PVIs significantly more concerned about the website's legitimacy. While these unpopular websites are not spoofs, these security issues still pose threats to users and deserve their attention.

6 Discussion

We employed a user-centered design process to design, implement, and evaluate GuardLens: a web browser extension that helps PVIs make informed privacy and security decisions about a website by surfacing a basket of privacy/security cues that would otherwise be inaccessible. Our results reveal the strengths and limitations of the current design and points to a rich area for future research and design.

Our results suggest that GuardLens improves the accessibility of privacy/security cues on websites and helps PVIs make informed decisions about website legitimacy, especially for spoofed and legitimate popular sites. Prior literature [2,32,41] has highlighted the accessibility issues of these cues. PVIs often miss these cues as they try to piece together and make sense of information on the website as a whole [24,31]. Our participants expressed appreciation that GuardLens, through its varied information blocks described in Section 3, provides a bird's eye view of the privacy/security information of a website in one, accessible location.

Prior studies [1,41] explored accessibility challenges faced by PVIs to identify the credibility of websites in general. Our study explores how this population interacts differently with websites to assess their credibility, depending on whether the website is popular, unpopular, or a spoof site. Our study asked participants to browse those three types of websites to mimic their real-world browsing experience.

GuardLens and Spoof Sites. Prior work [49] has identified two major criteria for phishing (spoof) sites: a) visual similarity to the legitimate site and b) at least one login page for users to input credentials. Our study's spoof sites are visually similar to the original sites for Amazon and the National Federation of the Blind. Using GuardLens, a significant majority of participants identified the spoof sites, relying on tool information such as domain age, search result ranking, and the domain name of the website. However, some participants still failed to identify the spoof sites. While they checked the information provided by the tool, they still relied on familiarity with the website's content and layout based on past browsing experiences with original sites. Two participants ignored the red flags about shorter domain age and website not appearing in the top five search results from GuardLens because they thought GuardLens had some glitches. We will revisit this challenge in the design implications section.

GuardLens and Popular Sites. GuardLens was also effective at helping users assess the legitimacy of popular sites. For example, by validating that the site is among the top Google search results for its title and by confirming that the site domain was registered when the user might have expected, participants could confidently recognize the website as legitimate. GuardLens provides an overview of these privacy/security cues in one location.

GuardLens and Unpopular Sites. Unlike the spoof and popular sites, we observed mixed results using GuardLens for

unpopular sites. Multiple participants stated that GuardLens reduced the effort to identify privacy/security information on a website, consolidating this information in one place. However, since our participants were unfamiliar with these sites, strategies such as checking domain age using GuardLens were not helpful in making legitimacy judgments, because participants did not have apriori expectations. Moreover, GuardLens elevates security cues not to be directly pertinent to whether or not a website is a phish, but nevertheless reveal poor security properties. It could cause confusion, as participants might conflate general security with legitimacy. For example, the presence or absence of HTTPS is not always relevant for assessing website phish [1]; yet, websites without HTTPS are less secure, leaving viewers more susceptible to man-in-the-middle attacks. Nevertheless, some participants relied on the HTTPS cue when making legitimacy assessments.

More generally, GuardLens cues correspond to different privacy/security threats without clear distinction. We will revisit this design challenge in the design implications section.

Security Assessment Strategies. Prior literature [33] touches on the security assessment strategies such as fast tab/scroll used by PVIs to determine a website's legitimacy and overall privacy/security posture. Our results confirm those accessibility-based strategies. However, unlike prior study [1], which claimed that PVIs may not rely on HTTPS or SSL/TLS dialogues to assess whether a website is legitimate or fraudulent, our participants considered the presence of HTTPS encryption in URL an important characteristic of a legitimate website. In addition, we also observed some novel strategies. Our participants relied on the website footer links, which included privacy policy, copyright information, 'Contact Us,' and 'About Us,' to determine website's legitimacy.

They also relied on their experience and familiarity with specific popular sites. They would often compare the content of the site they visited during the study with an impression of the site they had based on familiarity.

6.1 Design Implications

Privacy/security cue explanation. Participants found it challenging to interpret some GuardLens cues (e.g., *website's owner identity is unknown*). While GuardLens includes an expandable summary of what a cue means and what a user can do, our participants did not always check or understand those details. Future research should explore alternative ways to present such information: for instance, a chatbot allowing users to directly ask questions about those concepts.

Website accessibility and footer indicators. Screen reader users utilized a website's accessibility and footer information to assess a website's legitimacy. Browsers and security tools similar to GuardLens should consider adding a score to summarize websites' accessibility. An accessibility score could use factors like heading structure, inclusion of image description (alt-txt), and compatibility with various screen-readers such as JAWS, NVDA, or VoiceOver. Similarly, a footer score could highlight the presence of information such as privacy policy, copyright, and contact information.

Structuring privacy/security cues. GuardLens provides mixed signals for unpopular sites. For instance, for an unpopular audiobooks site, GuardLens warned that the site lacks HTTPS encryption and has a younger domain age, suggesting it may not be safe. However, GuardLens also mentioned that the site appeared in the top five search results and had few external links, suggesting the site is safe. Different GuardLens cues tend to correspond to different threats and might sometimes confuse users. Future designs can more explicitly distinguish the underlying threats (e.g., man-in-the-middle attacks, phishing) and structure the cues accordingly.

Providing a blanket privacy/security statement? Some participants desired a simple blanket statement about whether they should visit a site or not. We believe that tools could provide a strong warning for sites that are clearly problematic (e.g., spoof sites). However, as for the long tail of unpopular sites that often have mixed privacy/security cues, providing such a blanket statement is risky because it does not convey the nuance of privacy/security. In those cases, providing detailed but structured (based on underlying threats) cues might be more appropriate.

Engendering user trust with privacy/security tools. Sometimes participants suspected GuardLens has glitches because the cues conflict with expectations. For instance, when Guardlens suggested that the domain age of a spoofed Amazon site was 11 months. P13 nevertheless fell for the spoof because they thought that GuardLens was wrong, mistakenly showing the age of the site's current SSL certificate. Exploring ways to increase users' trust in assessment tools like GuardLens is another design challenge for future work. One strategy could be to more explicitly state where and how the tool creates a security cue (e.g., domain age). Another strategy is the web browser directly incorporating such features rather than having them in a third-party tool.

6.2 Limitations

6.2.1 Limitations of the Current GuardLens Design

Sound Alerts. Participants suggested that GuardLens should have a sound alert when it pops up on the screen with a warning about website. It would nudge users to check the security cues of a website.

Reading Website Domain Names Character by Character. In the current version of GuardLens, the domain name information block states the website domain name as words (e.g., Amazon). Participants must manually read the name by character using a screen-reader (e.g., A-m-a-z-o-n) to verify the spelling of the domain name. Participants suggested that if GuardLens could read out the domain name of the website character by character, it would help PVIs to more easily no-

tice whether they are visiting a phishing website that uses a domain name similar to a legitimate website. Future design could incorporate an option to automatically pronounce the website domain name character by character.

Activating GuardLens. Several participants preferred GuardLens to pop up only when visiting a new site because they are already certain about sites they frequently visit. In the current version, GuardLens does not filter whether the user has previously visited a site. Future design could explore an option where users can define different policies for enacting GuardLens. For instance, GuardLens could ignore a whitelist of sites that a user visited more than twice in the past month.

Catering to Different Levels of Technical Expertise. Participants exhibited multiple levels of technical expertise in the study. While GuardLens provides privacy/security cues for a website, it does not adjust itself for an individual user's technical expertise. Future iterations of GuardLens could be improved to better cater to individual differences in technical expertise, which could be voluntarily provided by a user at the first time of usage by answering a short set of questions.

6.2.2 Limitations of Our User Study

Sample Size. 25 participants finished our study. While it would be desirable to have more participants with different backgrounds, our sample size is on par with the other privacy/security user studies focusing on PVIs [12, 32].

Study Design. Though atypical, we first conducted the formative field study, followed by the summative lab study. In the formative field study, participants used GuardLens as part of their regular browsing experience. The field study strengthened the system's ecological validity and improved its design. The main study yielded many insights, but we could not test GuardLens in real-world context. Participants in the lab-based interview study were aware of being observed and could have been primed to look for privacy/security cues both with and without GuardLens. Nevertheless, the comparison results remain valid. Future work could conduct another summative field study to observe participants' use of GuardLens in situ. We could only test a few websites and website genres to conduct the study within a reasonable duration, especially because these tasks could be taxing for our participants. Future work could explore additional sites, along with GuardLens's usability, factors influencing its adoption/abandonment, and inclusion of other security and privacy features.

7 Conclusion

To address the accessibility barriers that PVIs face in assessing the privacy/security posture of a website, we conducted an iterative, user-centered design process with 25 PVIs. First, we explored what privacy/security cues PVIs find helpful in assessing the legitimacy of websites. Using this knowledge, we designed and implemented GuardLens, a web browser extension that automates and aggregates these cues for PVIs. We then evaluated if and how GuardLens helps PVIs assess the legitimacy of three types of websites, i.e. spoof, popular, and unpopular. We found that while PVIs had difficulty interpreting GuardLens cues for legitimate, unpopular websites with otherwise poor security properties, it effectively increased the accessibility of privacy/security cues, and was helpful for PVIs in assessing the legitimacy of spoof and popular sites.

8 Acknowledgements

We thank our participants for their contributions and sharing their insights. This research was in part supported by the National Science Foundation (NSF) grants #2126314 and #2028387 and #2126058.

References

[1] Ali Abdolrahmani and Ravi Kuber. Should i trust it when i cannot see it? credibility assessment for blind web users. In *Proceedings of the 18th international acm sigaccess conference on computers and accessibility*, 2016.

[2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

[3] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Understanding the physical safety, security, and privacy concerns of people with visual impairments. *IEEE Internet Computing*, 21(3):56–63, 2017.

[4] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. Up to a limit? privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–27, 2018.

[5] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016.

[6] Taslima Akter, Tousif Ahmed, Apu Kapadia, and Swami Manohar Swaminathan. Privacy considerations of the visually impaired with camera based assistive technologies: Misrepresentation, impropriety, and fairness. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, 2020.

[7] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. " i am uncomfortable sharing what i can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[8] APWG APWG. Phishing activity trends report: 3rd quarter 2019. *Anti-Phishing Working Group. Retrieved April*, 2019.

[9] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. Passchords: secure multi-touch authentication for blind people. In *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*, 2012.

[10] Natã M Barbosa, Jordan Hayes, Smirity Kaushik, and Yang Wang. "every website is a puzzle!": Facilitating access to common website features for people with visual impairments. *ACM Transactions on Accessible Computing (TACCESS)*, 2022.

[11] Douglas Bates, Martin Mächler, Ben Bolker, and Steve Walker. Fitting linear mixed-effects models using lme4. *arXiv preprint arXiv:1406.5823*, 2014.

[12] Mark Blythe, Helen Petrie, and John A. Clark. F for fake: Four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011.

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

[14] Daniel Cer, Yinfei Yang, Sheng-yi Kong, Nan Hua, Nicole Limtiaco, Rhomni St John, Noah Constant, Mario Guajardo-Cespedes, Steve Yuan, Chris Tar, et al. Universal sentence encoder. *arXiv preprint arXiv:1803.11175*, 2018.

[15] Qian Cui, Guy-Vincent Jourdan, Gregor V. Bochmann, Russell Couturier, and Iosif-Viorel Onut. Tracking phishing attacks over time. In *Proc. of WWW*, 2017.

[16] Sauvik Das, Cori Faklaris, Jason I Hong, Laura A Dabbish, et al. The security & privacy acceptance framework (spaf). *Foundations and Trends® in Privacy and Security*, 5(1-2):1–143, 2022.

[17] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006.

[18] Bryan Dosono, Jordan Hayes, and Yang Wang. " i'm stuck!": A contextual inquiry of people with visual impairments in authentication. In *SOUPS*, pages 151–168, 2015.

[19] Vincent Drury and Ulrike Meyer. Certified phishing: taking a look at public key certificates of phishing websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 211–223, 2019.

[20] Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, 2016.

[21] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. *Statistical methods for rates and proportions*. john wiley & sons, 2013.

[22] Dan Geer. For good measure. *USENIX PATRONS*, page 72, 2020.

[23] Xiao Han, Nizar Kheir, and Davide Balzarotti. Phisheye: Live monitoring of sandboxed phishing kits. In *Proc. of CCS*, 2016.

[24] L. Hasty. Teaching tactile graphics, perkins school for the blind. https://www.perkinselearning.org/videos/webcast/teaching-tactile-graphics.

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

[26] Hilary Hutchinson, Wendy Mackay, Bo Westerlund, Benjamin B Bederson, Allison Druin, Catherine Plaisant, Michel Beaudouin-Lafon, Stéphane Conversy, Helen Evans, Heiko Hansen, et al. Technology probes: inspiring design for and with families. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2003.

[27] Ravi Kuber and Shiva Sharma. Toward tactile authentication for blind users. In *Proceedings of the 12th international ACM SIGACCESS conference on Computers and accessibility*, 2010.

[28] Victor Le Pochat, Tom Van Goethem, and Wouter Joosen. Funny accents: Exploring genuine interest in internationalized domain names. In *Proc. of PAM*, 2019.

[29] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. Does domain highlighting help people identify phishing sites? In *Proc. of CHI*, 2011.

[30] Baojun Liu, Chaoyi Lu, Zhou Li, Ying Liu, Hai-Xin Duan, Shuang Hao, and Zaifeng Zhang. A reexamination of internationalized domain names: The good, the bad and the ugly. In *Proc. of DSN*, 2018.

[31] Alan Lundgard, Crystal Lee, and Arvind Satyanarayan. Sociotechnical considerations for accessible visualization design. In *2019 IEEE Visualization Conference (VIS)*, pages 16–20. IEEE, 2019.

[32] Daniela Napoli. Accessible and usable security: Exploring visually impaired users' online security and privacy strategies. 2018.

[33] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. "i'm literally just hoping this will Work:'' obstacles blocking the online security and privacy of users with visual disabilities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021.

[34] Adam Oest, Yenganeh Safaei, Penghui Zhang, Brad Wardman, Kevin Tyers, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. Phishtime: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. In *Proc. of USENIX Security*, 2020.

[35] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*, 2020.

[36] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 chi conference on human factors in computing systems*, pages 6412–6424, 2017.

[37] Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, and Gang Wang. What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proc. of Asia CCS*, 2019.

[38] Peng Peng, Limin Yang, Linhai Song, and Gang Wang. Opening the blackbox of virustotal: Analyzing online phishing scan engines. In *Proc. of IMC*, 2019.

[39] Yuji Sakurai, Takuya Watanabe, Tetsuya Okuda, Mitsuaki Akiyama, and Tatsuya Mori. Discovering httpsified phishing websites using the tls certificates footprints. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 522–531. IEEE, 2020.

[40] Pan Shi, Heng Xu, and Xiaolong Zhang. Informing security indicator design in web browsers. In *Proceedings of the 2011 iConference*, pages 569–575. 2011.

[41] Gunikhan Sonowal, KS Kuppusamy, and Ajit Kumar. Usability evaluation of active anti-phishing browser extensions for persons with visual impairments. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017.

[42] Abigale Stangl, Kristina Shiroma, Bo Xie, Kenneth R Fleischmann, and Danna Gurari. Visual content considered private by people who are blind. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility*, 2020.

[43] Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt. The web's identity crisis: Understanding the effectiveness of website identity indicators. In *Proc. of USENIX Security*, 2019.

[44] Ke Tian, Steve TK Jan, Hang Hu, Danfeng Yao, and Gang Wang. Needle in a haystack: Tracking down elite phishing domains in the wild. In *Proceedings of the Internet Measurement Conference 2018*, pages 429–442, 2018.

[45] Javier Vargas, Alejandro Correa Bahnsen, Sergio Villegas, and Daniel Ingevaldson. Knowing your enemies: leveraging data analysis to expose phishing patterns against a major us financial institution. In *Proc. of eCrime*, 2016.

[46] Yang Wang. Inclusive security and privacy. *IEEE Security & Privacy*, 16(4):82–87, 2018.

[47] Colin Whittaker, Brian Ryner, and Marria Nazif. Large-scale automatic classification of phishing pages. In *Proc. of NDSS*, 2010.

[48] Colin Whittaker, Brian Ryner, and Marria Nazif. Large-scale automatic classification of phishing pages. 2010.

[49] Guang Xiang, Jason Hong, Carolyn P Rose, and Lorrie Cranor. Cantina+ a feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security (TISSEC)*, 14(2):1–28, 2011.

[50] Yaman Yu, Saidivya Ashok, Smirity Kaushi, Yang Wang, and Gang Wang. Design and evaluation of inclusive email security indicators for people with visual impairments. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1202–1219. IEEE Computer Society, 2022.

[51] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong. Phinding Phish: Evaluating Anti-Phishing Tools. In *Proc. of NDSS*, 2007.

[52] Yue Zhang, Jason I Hong, and Lorrie F Cranor. Cantina: a content-based approach to detecting phishing web sites. In *Proc. of WWW*, 2007.

A Design Considerations

We designed a tool, GuardLens, to improve the accessibility of privacy/security cues of websites and help PVIs make more informed decisions while browsing websites online.

First, GuardLens provides easy access to privacy/security cues about a website (RQ1). This information is often inaccessible to PVIs but accessible to others almost instantly through a quick visual scan of a page (e.g., HTTPS lock icon, website search result ranking). The information otherwise readily provided by GuardLens is traditionally cumbersome to obtain or even inaccessible for PVIs, such as security certificate information [32, 33]. Motivated by prior work [10] and RQ1, one of our design goals was to *give users the ability to quickly obtain privacy/security information*.

Second, GuardLens hopes to help users with visual impairments protect against insecure websites (RQ2). Sighted users can rely on readily obtained privacy/security cues by simply glancing at a rendered page, enabling them to quickly take action to act on their privacy and security. For example, a quick glance may provide cues on whether a web page shows inappropriate images, what topic/genre the website or page is about (e.g., finance, news, shopping) and whether the page is out of context or is a click bait. In addition, with little additional effort, sighted users can also verify if links work or point to other website domains (e.g., via mouse-over), which can be helpful cues to detect phishing websites.

However, this is often not the case for PVIs. They use screen readers to navigate website content and often skip over large portions of text to prevent cognitive overload of information. However, doing so increases their likelihood of missing vital privacy/security related information [1]. Thus, obtaining privacy/security information about a website requires disproportionate effort on the part of PVIs. To this end and conforming with RQ2, our second design goal was to *provide equitable access to privacy/security-related information*, equipping users with useful information that could help protect them against privacy/security risks such as phishing websites. For instance, an attacker creates phishing (visually similar spoof) websites with a goal to trick users into entering personal information (e.g., account credentials, financial information). We assume that the attacker cannot alter information from trusted sources such as security certificates, domain registrations and Google search results.

Note that we conducted the formative study after developing GuardLens' initial version. We updated GuardLens tool design iteratively based on participant feedback from the formative study and the pilots.

B Formative Study

First, we conducted a formative study with five PVIs. Our **formative study** was motivated by prior work [10, 25, 41, 46] highlighting PVIs' needs for more accessible privacy/security

cues. The goal of this exploratory study was to understand the usage of GuardLens, as a technology probe, through 2-week field deployment. Each participant who completed the study for the full two weeks received a $70 gift card. We hypothesized that presenting a website's privacy/security cues in a non-visual format would help PVIs better assess the website. In particular, we explored two research questions: (1) what are the pros and cons in making website privacy/security-related information more salient to PVIs? (2) under what circumstances are privacy/security cues useful for PVIs?

To initiate the field study, we conducted a session with each participant to help them install the GuardLens browser extension. Due to the COVID-19-related social distancing guidelines, we conducted the study remotely via Zoom. After the initial session, participants used the system for two weeks as part of their regular browsing experience. Participants were asked to visit a minimum number of unique websites based on the screening survey. For example, if they claimed to visit 10-15 websites in the week prior to answering the screening survey, they were asked to visit at least 10 unique websites per week and half of the sites using GuardLens. After the 2-week period, we conducted 45 minute semi-structured exit interviews with participants. These interviews focused on the pros and cons of increased accessibility of privacy/security cues and whether the information provided by GuardLens was helpful. During the interview, we encouraged participants to share their experiences with GuardLens.

Participants found it difficult to access the security certificate of a website by clicking the padlock icon on the address bar. Therefore, GuardLens providing the security certificate information was useful. In addition, participants found three types of information from GuardLens most helpful: HTTPS encryption, external links pointing out of the website, and website owner. However, they also found the tool annoying because it would pop-up too frequently and it presented too much information. We used this feedback to improve the tool, for instance, by only showing the GuardLens pop-up when it detects important security issues (e.g., lack of HTTPS). We also added an option that allows users to choose specific privacy/security cues they want to see for a website. In addition, we made GuardLens more accessible, e.g., we improved the accessibility of the prompt dialog box (see Screen A in Figure 1) using an ARIA label.

C Pilot of Main Study

We pilot tested the main study with three PVIs, who self-identified as male, blind screen reader users. One of them did the earlier formative study. We followed the main study protocol and each pilot took about 1 hour. Each participant received a $30 gift card for completing the study.

Bird's eye view. Participants commended GuardLens' overview of privacy/security information of a website at one location. They said it saved them time compared to manually checking that information themselves. For instance, a participant said, *'When I am navigating without GuardLens, I don't have tool that tell me info about related links on the website and links to external websites. It gives me a quick bird-eye view of the website.'* Pilot participants found the following information from GuardLens most useful: website encryption (HTTPS), owner identity, and external links pointing out of the website. Participants assumed that if more links point out of the website, it may not be secure.

Feedback to improve GuardLens. Pilot participants reported that it was difficult to interpret the warning about 'owner identity unknown' because it only provided descriptive information but no actionable suggestions. We also observed that without GuardLens, participants applied strategies such as reading a website's URL character by character using their screen reader, and Googling unfamiliar websites to determine whether they are legitimate by checking their position in the Google search results.

Based on the findings from these pilots, we made several changes to GuardLens. We added two new information features to the system, namely, *domain age of website*, and *Google search results of a website*. The details about these cues were discussed in Section 3.2. We also added actionable suggestions for some of the cues, e.g., checking the website URL character by character as an actionable suggestion for the *'owner identity unknown'* cue.

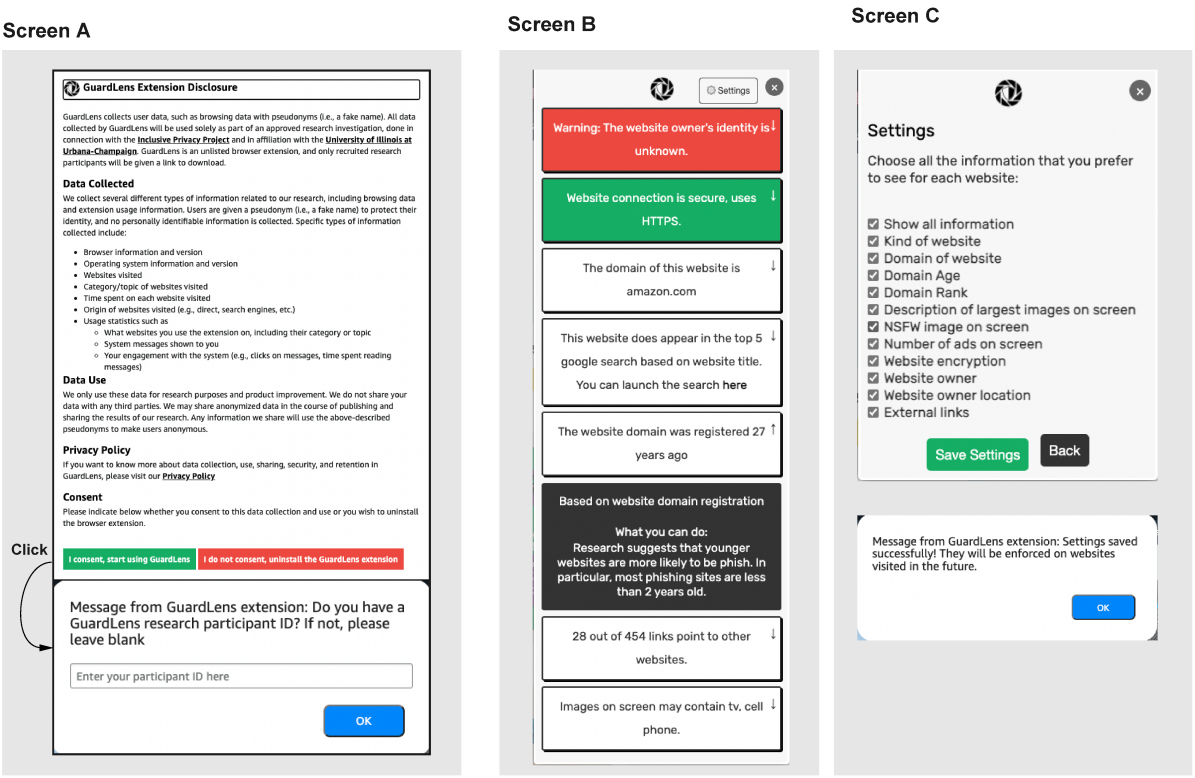

Figure 1: GuardLens UIs: (a) Screen A includes privacy disclosure and purpose of the study, (b) Screen B includes the main screen with privacy/security information blocks for a site being visited by a user and clicking into the arrow key of an information block will show tooltips and actionable suggestions, and (c) Screen C includes settings for the user to choose which information blocks to appear on GuardLens main screen as well as a confirmation page for saved settings. All the screens are marked up with the adapted information hierarchy and touch targets for screen reader accessibility.

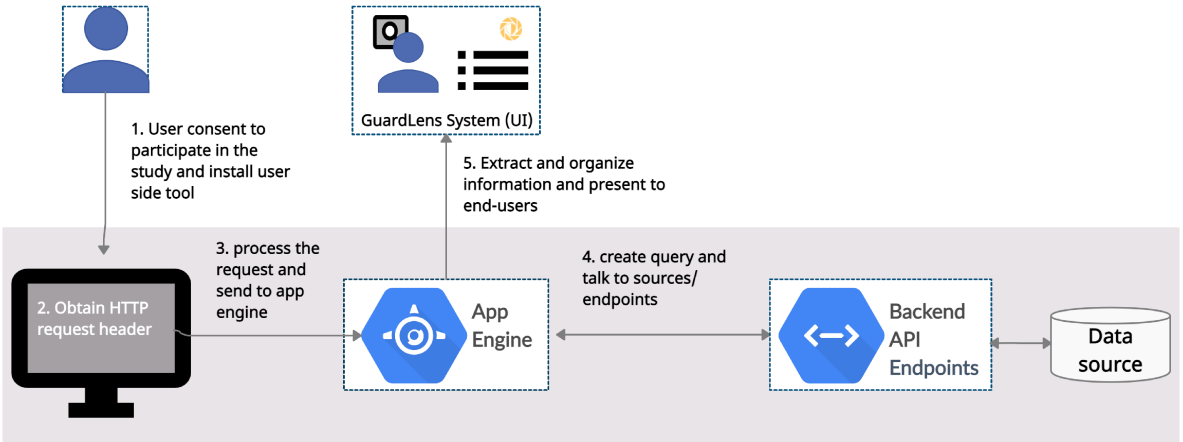

Figure 2: Workflow of GuardLens: upon user consent, GuardLens is triggered to send requests and build a channel between app engines (helpers) and external Backend API endpoints. App engines create queries, talk to data sources/endpoints, and present the structured information in the GuardLens UI for end users.

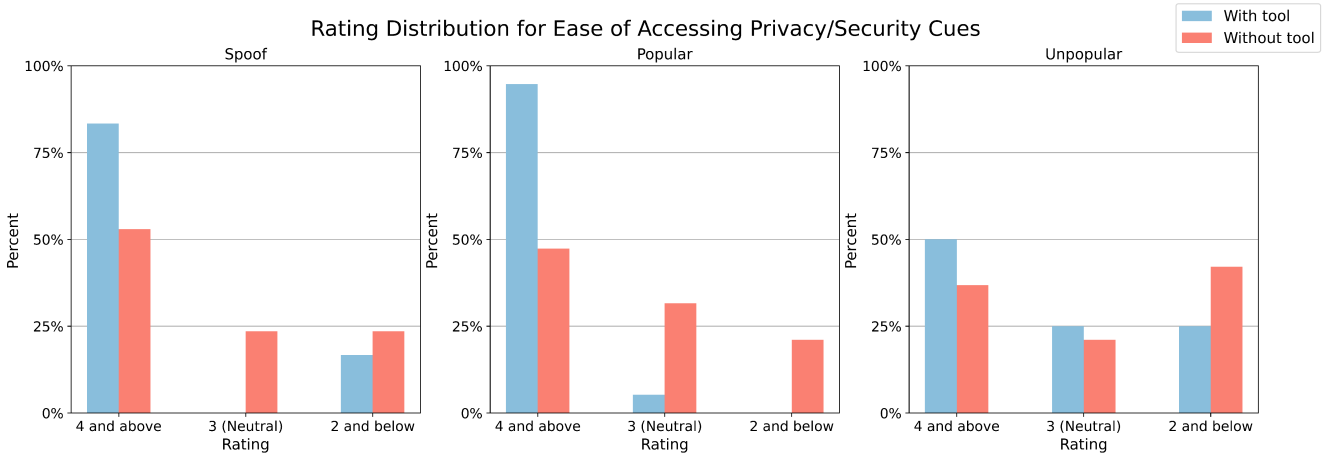

Figure 3: Participant ratings for ease of accessing privacy/security cues across three types of websites, spoof, popular, and unpopular websites, with and without GuardLens.

Table 1: The table shows most accessible privacy/security cues (in decreasing order) used by participants for three website types, i.e., spoof, popular, and unpopular, while browsing websites without and with GuardLens tool.

With/out Tool	**Spoof**	**Popular**	**Unpopular**
Without Tool	Read URL char by char Website footer Links HTTPS encryption in URL	HTTPS encryption in URL Website footer Links	HTTPS encryption in URL Website footer Links Website Accessibility
With Tool	Domain Age Domain Name	Domain Age HTTPS encryption (from tool)	HTTPS encryption (from tool) Domain Age Search Result Ranking

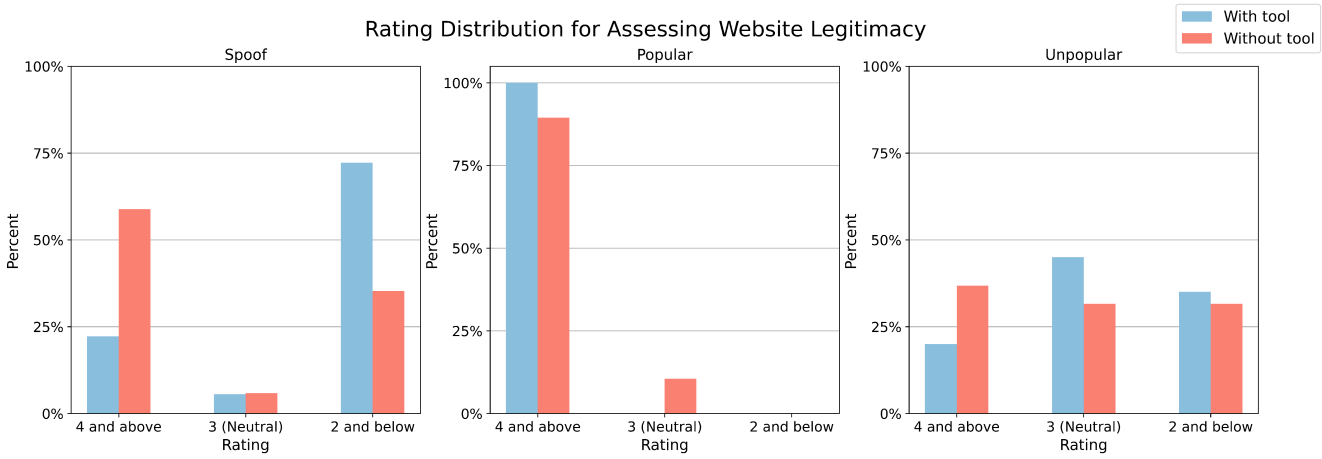

Figure 4: Participant ratings for website legitimacy across three types of websites (Spoof, Popular, and Unpopular) with and without the GuardLens tool.

Table 2: The table shows the most popular privacy/security strategies (in decreasing order) used by participants to assess the website legitimacy for three website types, i.e., spoof, popular, and unpopular, with or without GuardLens.

With/out Tool	**Spoof**	**Popular**	**Unpopular**
Without Tool	Familiarity with site Read URL character by character HTTPS encryption in URL	HTTPS encryption in URL Browsing content Familiarity with site	Google search by website title HTTPS encryption in URL
With Tool	Domain Age	Domain Age Google search result ranking (from tool) HTTPS encryption (from tool)	HTTPS encryption (from tool)

Table 3: Participant demographics (main study)

Participant ID	Order of Condition	Age Group	Gender	Self-Described Visual Ability	Assistive Technology Use	Education
P1	GuardLens First	45-54	Female	Blind	JAWS on laptop, VoiceOver on iPhone with Safari	Associate Degree
P2	Without tool First	55-64	Female	Blind Loss of Hearing	JAWS, VoiceOver, Refreshable Braille Display	Master's degree
P3	GuardLens First	25-34	Female	I can see lights, shadows, and objects very close to my face	JAWS, VoiceOver, ZoomText, Refreshable Braille Display	Master's degree
P4	Without tool First	25-34	Female	Blind	JAWS,Narrator, VoiceOver	Master's degree
P5	GuardLens First	35-44	Female	Blind	JAWS,NVDA, VoiceOver	Master's degree
P6	GuardLens First	18-24	Male	Blind	NVDA	Bachelor's degree
P7	GuardLens First	25-34	Male	Blind	NVDA,VoiceOver, Refreshable Braille Display	Bachelor's degree
P8	Without tool First	35-44	Female	Blind	JAWS,NVDA,VoiceOver, Refreshable Braille Display	Trade/technical /vocational training
P9	GuardLens First	18-24	Male	Blind	JAWS,NVDA,VoiceOver, Seeing AI, AIRA, Envision AI, ABB YY Fine Reader	Master's degree
P10	Without tool First	25-34	Male	Blind	JAWS,NVDA	Bachelor's degree
P11	GuardLens First	35-44	Male	I have retinal detachment	NVDA	No diploma
P12	Without tool First	35-44	Female	Blind	JAWS,NVDA,Narrator,VoiceOver, Refreshable Braille Display	Bachelor's degree
P13	GuardLens First	35-44	Female	Blind	JAWS	Master's degree
P14	Without tool First	25-34	Male	I'm diagnosed with RP (Retinitis Pigmentosa) with Maculer Degeneration and 100% blind	JAWS,NVDA,ORCA	Bachelor's degree
P15	GuardLens First	35-44	Male	Blind	JAWS	Master's degree
P16	Without tool First	18-24	Female	Totally blind except for light perception	JAWS, VoiceOver	High school graduate
P17	GuardLens First	25-34	Male	Retinopathy of prematurity, rop5; no light perception.	JAWS, VoiceOver, ABBYY	Professional degree
P18	Without tool First	65-74	Male	Blind	JAWS, Refreshable Braille Display	Professional degree
P19	GuardLens First	65-74	Male	Blind	JAWS, NVDA, Narrator, VoiceOver	Master's degree

Table 4: Websites from seven categories: finance, e-commerce, accessibility, news/media, education, healthcare, and productivity.

Website	Type	Genre
https://nfb.org/	Popular	Accessibility-related
https://aira.io	Popular	Accessibility-related
https://nytimes.com	Popular	News/Media
https://www.webmd.com	Popular	Health
https://www.target.com/	Popular	E-commerce
https://www.zapsend.co/index.php?//	Unpopular	Finance
https://yourcodercamp.com	Unpopular	Education
http://zolucky.com/	Unpopular	E-commerce
http://www.openoffice.org/	Unpopular	Productivity
http://audiobookbay.ws/	Unpopular	Audiobooks
https://www.amaZAUNN.com	Spoofed Amazon	E-commerce
https://www.enеffbee.org	Spoofed NFB	Accessibility-related

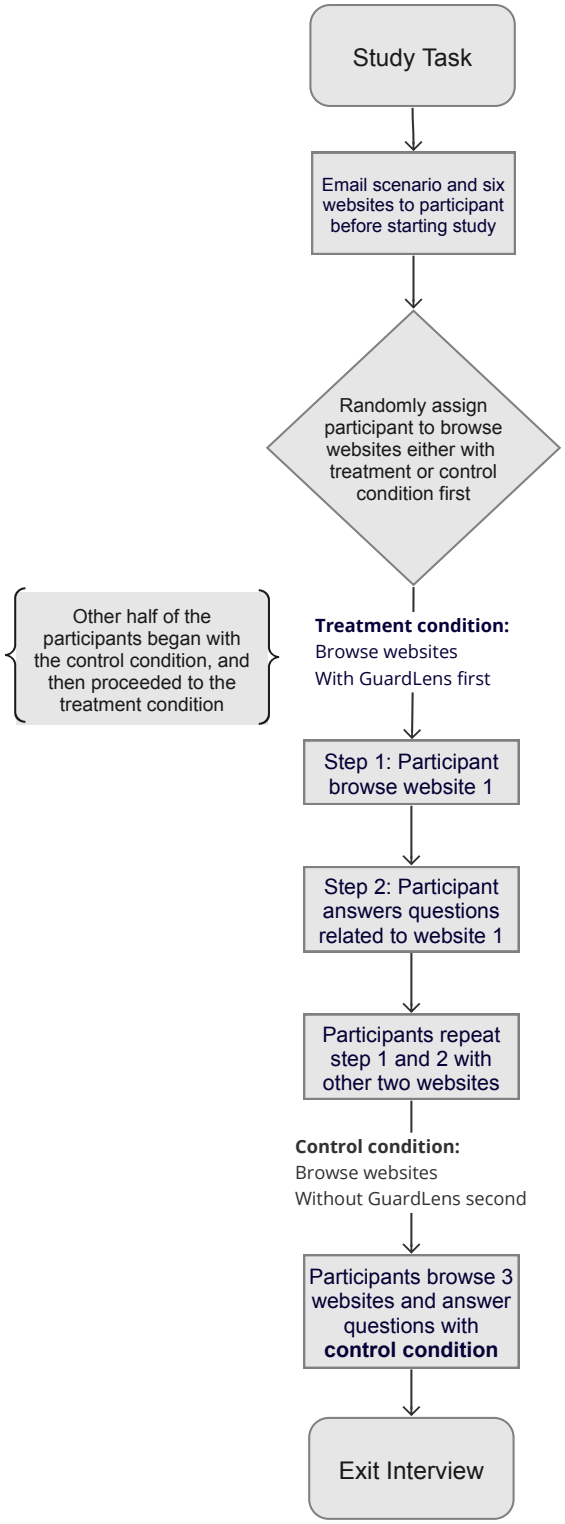

Figure 5: The main study design included the study task and the exit interview. In the study task, we emailed participants links to the websites along with a scenario. They visited various sites with and without GuardLens, unaware of site conditions, in a counterbalanced order.