The Lack of Accessibility for Visually Impaired People to Prevent Phishing Attacks

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree Bachelor of Science, School of Engineering

Alan Sameth

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisors

William J Davis, Department of Engineering and Society

Introduction

According to the FBI Internet Crime Complaint Center (IC3), over $12.5 billion was lost to cybercrimes in 2023, representing a 22% increase in financial losses from 2022, while the number of reported cybercrimes rose by 10% (FBI, 2023, p. 3). Among the growing number of cybercrimes, the most common form we see in our day-to-day lives is phishing attacks. Phishing attacks are emails, texts, or websites that malicious internet users send to victims to steal money or sensitive data by impersonating legitimate or trusted individuals or entities, whether it be a friend, a coworker, the Internal Revenue Service, or Amazon. Everyone in the world has encountered phishing, from simple text from a stranger to a "Google" pop-up saying you're a "winner" of a free prize by being the 38th trillionth search. Phishing has become such a common occurrence that people do not recognize it as a threat to their data and money, but it is not true, especially for the visually impaired.

As the reliance on the Internet grows with more websites and applications published daily and the rapid development of new technologies such as artificial intelligence, phishing attacks are becoming increasingly sophisticated and harder to detect. The surge in online activity leads to the proliferation of unstandardized, novel website and app designs and nearly identical phishing websites and emails. Anti-phishing software has been developed to combat phishing schemes, but it often relies on visual cues that would otherwise be inaccessible to the visually impaired.

This lack of accessibility in anti-phishing technology, combined with the poor current web design and assistive text-to-speech tools, leaves visually impaired people disproportionately vulnerable to phishing attacks. Despite efforts to make the web more inclusive, there remains a critical gap in cybersecurity measures for this population, exposing them to greater financial

risks and personal data breaches. Data from a UK study suggests that even though websites boast greater accessibility, researchers found a large percentage of violations of the Web Content Accessibility Guidelines in many features, including even labeling for text fields and checkboxes, at an average violation rate of 75% (Hanson & Richards, 2013, p. 16). This is expressed in the disabled community as they found frustration when encountering unlabeled text fields and missing alternative text (Lazar et al., 2007, p. 260). The danger posed by phishing attacks strips away their independence, as they often need the assistance of a second party, which they may not have all the time (Janiero et al., 2024, p. 68).

Additionally, this extends beyond personal use and into the jobs of visually impaired people. In many companies, employees are required to be trained against phishing attacks by regularly sending phishing emails and having them mark suspicious messages. Visually impaired people are put at a significant disadvantage since they often rely on assistive technologies, like screen readers, that may not properly interpret or highlight phishing indicators. As a result, these individuals may be more susceptible to falling for phishing attacks, which could compromise not only their personal security but also the integrity of their workplace.

In this paper, I argue that current anti-phishing software, web design standards, and assistive technologies do not adequately protect visually impaired users. By analyzing the barriers to accessibility of phishing attacks, websites, apps, and the visually impaired through the lens of human-computer interaction (HCI) and applying Actor-Network Theory to emphasize key sources of the systemic problems in software engineering, this research aims to highlight the shortcomings in existing software and propose strategies to improve phishing detection accessibility for the visually impaired.

Background

In a 2020 study conducted by the Vision Loss Expert Group, over 43.3 million people were reported as blind, and 295 million had moderate to severe visual impairments, meaning they cannot see even with corrective lenses (VLEG, 2020). Given the global scale of visual impairments, a significant portion of the online population may face unique challenges in identifying and avoiding digital threats. This vulnerability is especially urgent considering phishing accounted for more than half of all reported cybercrimes in 2023, contributing to $12.5 billion in financial losses in the U.S. alone (FBI, 2023, p. 16).

Although innovations in accessibility, such as screen readers, braille displays, and speech input, have improved digital experiences for many users, most websites and applications still lack comprehensive accessibility (Barbosa et al., 2022; Hanson & Richards, 2013). These platforms are often cluttered with visual and informational bloat that text-to-speech software cannot effectively convey. As noted by Lazar et al. (2007), screen reader users frequently encounter unlabeled buttons, poor layout navigation, and inconsistent alternative text. This results in a confusing user experience that not only impedes productivity but also creates ground for phishing attacks to go unnoticed. Rapid developments in AI-generated content and the professional polish of phishing campaigns further blur the lines between legitimate and fraudulent interactions (Baker, 2024).

A 2016 study by Inan et al. found that visually impaired users expressed greater concern over cybersecurity threats than their sighted peers, largely because assistive technologies often fail to present security cues clearly. Participants reported difficulties with forms, confusing layouts, and missing alt text, all of which hindered their ability to safely navigate the web (Inan et al., 2016,

p. 29). More alarmingly, the study discovered a negative correlation between cybersecurity awareness and internet use, meaning the more informed these users were about risks, the more they limited their online activity as a self-protective measure.

These fears are justified by findings from *Understanding phishing experiences of screen reader users* (2024), who studied how screen reader users responded to suspicious emails. Visually impaired participants were more likely to trust emails based on familiar names or emotionally resonant subjects, tactics frequently used in phishing. Compounding the issue, screen reader errors and vague security alerts, like mispronunciations or unreadable CAPTCHA warnings, made it even harder to spot deception (Janeiro et al., 2024, p. 67).

Efforts to improve defenses through anti-phishing software and browser extensions have yielded limited success for this demographic. *Usability evaluation of active anti-phishing browser extensions for persons with visual impairments*. (2017) demonstrated that most anti-phishing tools rely heavily on visual cues like pop-ups and color-coded warnings, which are inherently inaccessible to screen reader users. Of the extensions evaluated, few offered keyboard shortcuts, alternative text, or audio-based alerts tailored for blind users (Sonowal et al., 2017, p. 5). Similarly, Aljallad and Capra (2023) critiqued email clients for failing to design inclusive security indicators, often ignoring user testing with visually impaired individuals altogether.

The accessibility shortcomings found in both mainstream websites and cybersecurity tools not only restrict internet access for visually impaired people but also deepen the digital divide and foster environments where phishing can thrive.

Literature Review

All of these researchers agree that there are accessibility issues for visually impaired individuals when it comes to preventing phishing attacks from websites and software. Developers are often caught up in building applications and websites for sighted people, leaving visually impaired users as an afterthought. They correctly diagnose this disparity by surveying visually impaired individuals and examining the issues they face through the Human-Computer Interaction (HCI) perspective.

Despite the acknowledgment of accessibility challenges, there has been no unifying framework that addresses the systemic issues in cybersecurity design related to visually impaired users. Most studies, such as *Understanding Phishing Experiences of Screen Reader Users,* focus on specific aspects of the problem, whether it is user behavior or technological limitations of assistive devices. While these individual studies highlight critical vulnerabilities, they do not suggest a comprehensive strategy for making cybersecurity more inclusive.

Similarly, the *Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments* study sheds light on the anxiety and heightened risk perceptions among visually impaired users but stops short of linking these concerns to systemic design flaws in cybersecurity tools.

This fragmented approach in the literature underscores a significant gap: while individual studies recognize various accessibility challenges, there is little emphasis on addressing these issues culture of cybersecurity and software development as a whole. The prevailing focus remains on repurposing existing tools rather than rethinking the foundational principles of secure web design from an accessibility-first perspective. This oversight perpetuates a cycle where visually impaired users must adapt to insecure systems rather than systems being designed to

accommodate their needs from the outset.

This paper seeks to bridge that gap by analyzing not only the shortcomings of current anti-phishing tools and web design practices but also the systemic issues in the development processes that exclude visually impaired users. By applying an HCI lens, this research aims to synthesize existing findings into an argument for a more inclusive approach to cybersecurity design. This will involve examining how assistive technologies interact with phishing indicators, the limitations of current design standards, and the broader implications of these gaps on user safety.

In doing so, this research moves beyond identifying isolated issues to propose a universal understanding of how cybersecurity systems can be fundamentally restructured to better protect visually impaired individuals.

Methodology

This paper will employ a combination of literature review, an analysis of contemporary websites and app design through the HCI lens, and the motivations in the greater software development industry to examine the vectors of vulnerability and blind spots that increase phishing risks for visually impaired users. Actor-Network Theory (ANT) will serve as the framework, linking user interactions, developers, and software features. ANT is particularly useful as it highlights the relationships between human and non-human actors, illustrating how they influence and interact with one another (Latour, 1987).

The key aspect Latour introduces as a part of ANT is non-human actors, allowing them to shape and influence relationships within a network just as much as human actors. This

perspective is crucial in understanding how technology, infrastructure, and design decisions actively guide interactions, rather than being passive tools. In the context of software feature accessibility, ANT aligns well with HCI analysis by emphasizing how assistive technologies such as screen readers or braille keyboards affect user experiences, particularly for visually impaired individuals. Since ANT views both people and technological systems as agents that shape outcomes, it provides a structured way to analyze how accessibility features either support or hinder effective interaction. By examining how these non-human elements mediate access to critical information, we can better understand the vulnerabilities that arise when phishing exploits gaps in accessibility tools, ultimately reinforcing the importance of designing security-conscious and inclusive digital environments.

This paper draws inspiration from previous uses of ANT in analyzing software development processes. Specifically, Ahmedshareef, Hughes, and Petridis (2014) applied ANT to uncover the complex factors behind software project delays by mapping both human and non-human actors in development environments. Their work demonstrated how ANT could reveal hidden dynamics and systemic issues, which informed this paper's approach to examining how accessibility gaps and phishing vulnerabilities are shaped by interconnected design and development decisions.

The actors and non-actors that will be used to create the actor-network will be formed by the literature review, an analysis of popular website and app design, and the people who create these apps. From the literature review, which synthesizes accumulated studies on visually impaired individuals and their interactions with software, the paper will extract aspects that either assist or hinder their ability to identify phishing attacks as non-human actors. These may include factors such as software malfunctions that misinterpret or obscure critical security cues,

reliance on assistive technologies that may not convey urgency effectively, or the need to seek a second perspective from a sighted individual to verify suspicious content. By incorporating these insights, the actor network will reflect the complex interplay between accessibility features, user behavior, and security risks.

As for the analysis of popular website and app design, independent research through the HCI lens will focus on identifying confusing design practices that contribute to the vulnerability of visually impaired users to phishing attacks. Elements such as misleading button placements, ambiguous alt text, inconsistent screen reader compatibility, and deceptive visual hierarchies that obscure security warnings will be analyzed, as they often obscure the legitimacy of the website. These design choices function as non-human actors within the actor-network, actively shaping user interactions and influencing everyday decision-making and phishing identification. By assessing how these elements disrupt accessibility and hinder security awareness, the analysis will highlight the role of graphical user interface design (GUI) in either mitigating or exacerbating phishing risks, emphasizing the need for inclusive, simpler, and standardized software design.

As an extension of the previous analysis, the broader tech industry plays a crucial role in shaping the accessibility of software features, influencing how visually impaired users interact with applications. The design choices present in widely used platforms are not accidental as they result from decisions made by human actors within the industry, including developers, designers, product managers, and executives. These actors prioritize certain features based on business goals, regulatory requirements, and user demand, often placing security and accessibility in conflict with other concerns such as efficiency, aesthetics, or profitability. When accessibility is deprioritized or overlooked, critical features may be misaligned with the needs of visually

impaired users. The absence or misplacement of motives to create accessible security features results in a system where usability gaps persist, making it easier for phishing attacks to exploit these vulnerabilities. By examining how these decisions are shaped by the tech industry's priorities, the analysis will illustrate how both human and non-human actors interact to create an environment where accessibility and security are not always considered, reinforcing the need for a shift in industry standards toward more inclusive design practices.

Analysis

Revisiting the Literature Through an ANT and HCI Lens

Among the few studies that analyze the struggles that visually impaired people face when trying to identify phishing attacks, the most common problems stem from three main aspects of the software: accessibility, software issues, and poor design. These three factors are not only recurring themes in the literature but also serve as structural barriers that disproportionately expose visually impaired users to phishing threats.

Building on the prior research, it becomes clear that a lack of accessibility is not simply a matter of missing features or poor design, but rather it reflects a deeper issue of exclusion in the design and development process. This is evident in the HCI analysis in *Usability evaluation of active anti-phishing browser extensions for persons with visual impairments,* as shortsighted developers frequently fail to create cybersecurity tools with accessibility taken into consideration. Many of the browser extensions were reliant on color-based cues and pop-ups that would appear on the screen, which are otherwise inaccessible to the visually impaired. Additionally, one of the key ways visually impaired people navigate websites is through keyboard navigation and shortcuts with a computer mouse, since it typically requires a high

degree of visual and spatial awareness to locate and interact with on-screen elements accurately. However, the add-ons lacked support for keyboard shortcuts, making it nearly impossible for visually impaired users to interact with the extensions at all. This is further exacerbated by the fact that most of the extensions provide no instructions or usage guidelines for users (Sonowal et al., 2017, p. 5). Inaccessibility also extends far beyond the cybersecurity software into applications they use daily, such as Gmail. Another study found that when users were asked to identify phishing emails, the warnings provided were vague, and key images lacked alt-text, descriptive text that appears when an image fails to load, making them inaccessible to screen reader users. In fact, the Gmail spam filter worsened the inaccessibility by hiding images that image-recognition software would be able to access normally (Janiero et al., 2024, p. 68). Such limitations hinder a visually impaired person's ability to navigate the web securely and independently.

In tandem with these accessibility issues, software malfunctions and incompatibility exacerbate the problem. These can range from bugs in assistive technologies to compatibility problems between screen readers and website scripts, which disrupt or entirely prevent the transmission of key information. In some cases, screen readers contribute to the confusion by mislabeling or mispronouncing words or links or skipping over alerts that warn users about phishing attempts (Janiero, 2024, p. 68). Even when security features are technically present, they may not render correctly or may be inaccessible through keyboard navigation, which is an essential component for blind users. For instance, in a study that tested Gmail’s email alert feature and its interaction with visually impaired individuals and screen readers, when converted from the standard view to HTML, a user-interface (UI) with only hierarchies and none of the graphic design, the HTML view would lose Gmail warnings from the standard view or reword

warnings to be labeled as spam even when in a regular inbox (Aljallad & Capra, 2023, p. 2887-2888). Inconsistencies in how software implements interactive elements can lead to false confidence or overlooked threats.

Visually impaired people are also disproportionately affected by the broader trends in modern web design, which often prioritize aesthetic appeal and brand identity over functional accessibility. These trends introduce serious usability issues for screen reader users and others who rely on non-visual navigation. Features such as dynamic content loading, minimal contrast, icon-only interfaces, and JavaScript-heavy layouts frequently interfere with assistive technologies, making phishing indicators like suspicious URLs, email headers, or browser warnings less visible or even entirely inaccessible. This is especially problematic when approaching new websites or encountering new features, as there is a lack of standardization even among common elements like “log-in” or “sign-up” (Barbosa et al., 2022, p. 2).

When examining Amazon’s front page, there is a distinct hierarchy and blocks for featured products and settings. However, positional and organizational information is not available to the visually impaired, making it harder for them to find features, especially if they are hidden behind dropdown menus. A screen reader would also have to read through all the different modules and links, turning an ordinarily quick transaction into a time-consuming process. These design choices benefit phishing attacks by obscuring essential details in a digital mess, making it easier to replicate convincing illegitimate websites. Poor design also leads to potentially dangerous behaviors, such as skipping over unverified links (Janiero, 2024, p. 70).

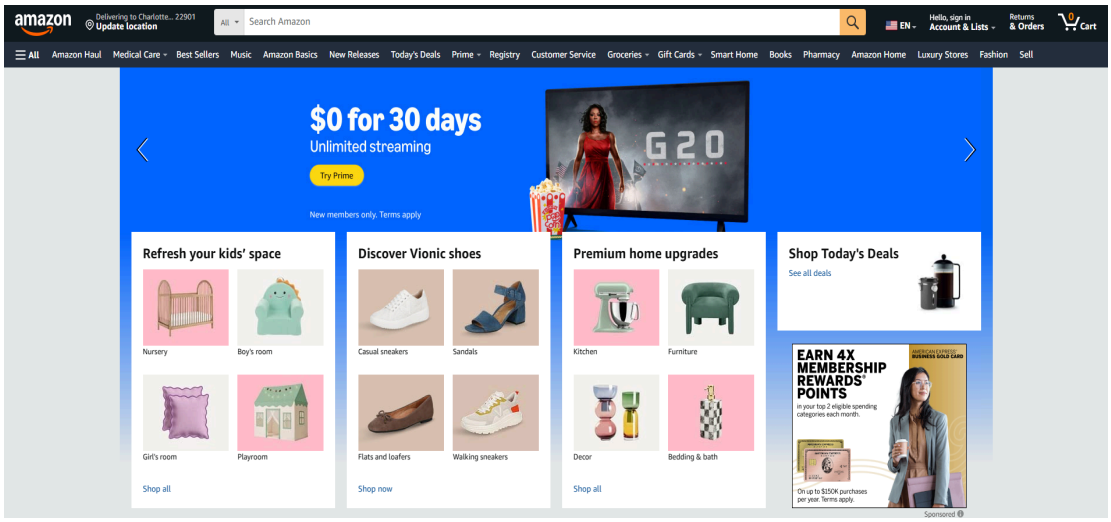

Figure 1: Amazon front page

One such behavior is bypassing the header and UI elements like “reply” and “forward,” which users may find tedious, in order to reach the body of the email, where the content is displayed. In the case of the Gmail warning study, this habit led visually impaired participants to completely skip the automated Gmail warning (Aljallad & Capra, 2023, p. 2893)."

Phishing by Design: Software Design, Culture, and Undermining Accessibility

The persistent inaccessibility of software for visually impaired users when preventing phishing attacks is not just a failure of individual design choices, it reflects a broader cultural pattern within the tech industry. Accessibility is often sidelined, treated as an afterthought rather than a foundational element of cybersecurity. This is especially dangerous in the context of phishing, where missing or poorly implemented accessibility features can leave users unaware of threats. As web design trends push for sleek visuals, dynamic interfaces, and minimalist layouts, they often sacrifice the clarity and structure required by assistive technologies. In doing so, these

trends inadvertently increase the phishing risk for blind and visually impaired users.

This culture of ignoring disabilities and disenfranchising visually impaired users stems from the profit-driven, progress-focused mindset that dominates the tech industry. Corporations and software engineers often prioritize aesthetics, speed, and marketability over accessibility, viewing it as a secondary concern. The pressure to innovate quickly and maintain competitive advantage leads to decisions that overlook the needs of marginalized groups, particularly those with disabilities. As a result, accessibility is frequently treated as an additional feature rather than an integral part of design and security. This self-perpetuating cycle ensures that the technology remains inaccessible to vulnerable populations, reinforcing the disparity in digital safety and leaving visually impaired users more exposed to threats like phishing. Without a concerted effort to address accessibility in both design and development practices, this cycle will continue, leaving these users at greater risk.

Conclusion

In conclusion, the persistent challenges faced by visually impaired users in identifying and preventing phishing attacks are a direct result of systemic issues within both web design and cybersecurity development. Despite the increasing recognition of the importance of accessibility, the design and implementation of software, websites, and anti-phishing tools remain insufficient for this vulnerable population. The reliance on visual cues and design trends that prioritize aesthetics and efficiency over clarity and accessibility only increases the risk posed by phishing attacks to visually impaired individuals. The lack of standardized, accessible security features and the incompatibility between screen readers and modern web design highlight a critical gap in the tech industry's approach to inclusivity.

In conjunction with the profit-driven tech industry, the culture fostered by growing profits and being first to market leaves the safety and accessibility of the visually impaired as an afterthought rather than being an integral part of the development process. This culture self-perpetuates a cycle of exclusion that makes visually impaired individuals disproportionately more vulnerable to phishing attacks.

Moving forward, it is essential for developers, designers, and industry leaders to adopt an accessibility-first mindset in both the creation of digital tools and the establishment of web design standards. unique needs of visually impaired users from the outset and integrating comprehensive accessibility features into cybersecurity measures, we can work toward bridging the current gaps in Internet safety. In doing so, we not only enhance the security of visually impaired users but also promote a more inclusive digital world where all individuals, regardless of ability, can confidently navigate the internet without fear of falling victim to phishing attacks.

References

Adams, R., Reiss, B., Serlin, D., & Ebook Central Diversity, E., & I. S. (2015). *Keywords for disability studies*. New York University Press.

Ahmedshareef, Z., Hughes, R., & Petridis, M. (2014). Exposing the influencing factors on software project delay with actor-network theory. *Electronic Journal of Business Research Methods*, 12(2), 139–146.

Aljallad, H., & Capra, L. (2023). Design and Evaluation of Inclusive Email Security Indicators for People with Visual Impairments. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–14. https://doi.org/10.1145/3544548.3580722

Baker, K. (2024, May 13). *12 most common types of cyberattacks*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

Barbosa, N. M., Hayes, J., Kaushik, S., & Wang, Y. (2022, September 1). “Every website is a puzzle!”: Facilitating access to common website features for people with visual impairments. *ACM Transactions on Accessible Computing*, *15*(3), 1–35. https://doi.org/10.1145/3491234

Gaggi, O., Quadrio, G., & Bujari, A. (2019). Accessibility for the visually impaired: State of the art and open issues. *Proceedings of the 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1-6. https://doi.org/10.1109/CCNC.2019.8651676

Griffiths, C. (2024, June 26). *The latest phishing statistics (updated June 2024): AAG IT Support*. AAG IT Services. https://aag-it.com/the-latest-phishing-statistics/#:~:text=With%20an%20average%20of%20%24136,emails%20per%20100%20internet%20users

Hanson, V. L., & Richards, J. T. (2013). Progress on website accessibility? *ACM Transactions on the Web*, *7*(1), Article 2, 1-30. https://dl.acm.org/doi/abs/10.1145/2435215.2435217?casa_token=YdxtJjt3OkIAAAAA:0uHHP1E39kkVcA8ZqNujzCVRl5TXVBFQKf_CfxoDxnVkqsK6yS-qxxiFE0T0A7LF3zdfWHS7uP6E

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

Internet Crime Complaint Center. (2023). *Internet crime report*. FBI. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

James, L., Ebook Central - Academic Complete, & O'Reilly Online Learning: Academic/Public Library Edition. (2006). *Phishing exposed*. Syngress Press.

Janeiro, J., Alves, S., Guerreiro, T., Alt, F., & Distler, M. (2024, September 1). Understanding phishing experiences of screen reader users. *IEEE Security & Privacy*, *22*(5), 63–72. https://doi.org/10.1109/MSEC.2024.3456789

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard University Press.

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

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017). 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* (pp. 6412–6424). Association for Computing Machinery. https://doi.org/10.1145/3025453.3025831

Rembis, M. A., Kudlick, C. J., & Nielsen, K. E. (Eds.). (2018). *The Oxford handbook of disability history*. Oxford University Press.

Shi, L., Jain, A., Vu, K., & Findlater, L. (2015). Analyzing the efficiency of touch-based text entry for visually impaired users. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery. https://doi.org/10.1145/2702123.2702334

Sonowal, G., Kuppusamy, K. S., & Kumar, A. (2017, January 7). 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)*. IEEE. https://doi.org/10.1109/ICACCS.2017.8014650

Teo, C. H., Hotez, P. J., Foreman, K. J., & Hay, S. I. (2024). Global and regional burden of vision loss due to uncorrected refractive error and other causes. *The Lancet Global Health*, *12*(3), e512–e524. https://pubmed.ncbi.nlm.nih.gov/38461217/

Toye, J. (2024, April 1). The Americans with Disabilities Act: Website accessibility and a foreign solution to a domestic problem. *St. Mary's Law Journal*, *55*(2), 607–639.

World Health Organization. (n.d.). *Blindness and visual impairment*. https://www.who.int/news-room/fact-sheets/detail/blindness-and-visual-impairment