Security Implications of Online Accessibility Obstacles for Users with Visual Impairments

Daniela Napoli
Carleton University
Ottawa, Ontario, Canada
daniela.napoli@carleton.ca

Khadija Baig
Carleton University
Ottawa, Ontario, Canada
khadija.baig@carleton.ca

Paulina Chametka
Carleton University
Ottawa, Ontario, Canada
paulina.chametka@carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Ontario, Canada
chiasson@scs.carleton.ca

Abstract

Like most, people with visual impairments are increasingly reliant on the Internet. Yet, existing security mechanisms are inadequate to enable these users to protect their online security and privacy. We conducted a task-based user study with 14 participants with visual impairments, observing their security habits and concerns when navigating popular transactional websites and a phishing site. We found severe usability issues that led users to take risks or forced them to choose between accessibility or security. Our findings contribute to the knowledge base of *inclusive security* and we suggest tailoring security information to better communicate digital threats to these users.

Introduction

There is a need for expanding security and privacy research to include different computing environments and user populations, including those with disabilities [15] [9]. Working towards *inclusive security and privacy*, we discuss our findings from a recent user study conducted with people with visual impairments. We observed participants complete tasks online that required sensitive information such as credit card numbers and home addresses. We probed further to uncover users' security and privacy concerns related to the accessibility and usability issues they faced during these tasks. We present our main findings and discuss the related security implications.

Website 1:
https://www.amazon.ca

1. Verify website's legitimacy
2. Log in
3. Complete a purchase

Website 2:
https://mail.google.com

1. Verify website's legitimacy
2. Log in
3. Download an email attachment

Website 3:
http://www.ccnib.ca[a]

1. Verify website's legitimacy
2. Find the donation page
3. Complete a $10 donation

[a]We extracted the site files from http://www.cnib.ca and uploaded them to a domain we purchased. Our spoof site was hosted on our research lab's server and was only available during the two weeks of testing. It is no longer live.

Background

The following security obstacles faced by users with visual impairments have previously been documented.

Ahmed et al.'s [2] findings suggest users with visual impairments must rely on inconvenient coping solutions to maintain their security, such as: disabling the screen even if they required visual cues, wearing headphones which minimized their awareness of physical surroundings, and relying on trusted sighted assistants to complete transactions on their behalf.

Inan et al. [10] found that many people with visual impairments actively bank and shop online but have a number of severe security concerns related to the accessibility obstacles they face while completing these tasks. Some of their top concerns include computer viruses, CAPTCHAs, spam emails, unauthorized access to search history, and location-based data tracking. Some of these concerns could be addressed through security software like an anti-virus, but these are often inaccessible and incompatible with screen readers [14] .

Several expert evaluations [7] [8] [13] have assessed the security mechanisms involved in common security tasks. They suggest that security mechanisms were inaccessible and can impede a blind user's ability to behave securely. Perhaps for this reason, Abdolrahmani and Kuber [1] found that users with visual impairments do not rely on HTTPS or SSL dialogues to assess phishing websites.

Proposed accessible security solutions have included observation-resistant password schemes [6] [12] and systems like PassChords [3] which allow users with visual impairments to access their smartphones faster than with traditional PINs. Password managers, like UniPass [4], can lend themselves well to non-visual users if they support bio-metric authentication options, avoid touch-screen gestures that require visual navigation, eliminate time limits, and use concise audio descriptions for dialogues. The SoundsRight CAPTCHA [11] is a security mechanism allowing users to use their hearing abilities rather than vision and, thus, can accommodate users with visual impairments. While these advances are helpful, they are far from ubiquitous and further work is needed towards *inclusive* security.

Methodology

Our study was cleared by the university's Research Ethics Board and by the CNIB[1] Research Department. We provided each participant a $50 honorarium and compensated their study-related travel expenses.

Fourteen people (6 female and 8 male) with visual impairments, 7 blind and 7 partially sighted, participated in our study. Each 90-minute session included three segments. First, we verbally collected demographic information. Second, participants engaged in a task-based scenario where they attempted three site-specific security tasks on one of three randomly assigned websites. Some participants repeated these tasks on a second site where time permitted. The tasks and websites are listed in the left sidebar. Websites 1 and 2 were legitimate, while Website 3 was spoofed. Participants were familiar with the legitimate versions of all three websites. We provided participants with login credentials, addresses, and credit card information so that they did not have to input their personal information to complete the tasks. Third, we collected more qualitative information through verbal security themed Likert-scale questionnaires and a semi-structured interview.

[1]CNIB Foundation is a charitable organization assisting Canadians who are blind or living with vision loss.

Figure 1: Three hundred and twenty-six quotes were extracted and sorted per our themes: attitudes (112), behaviours (142), and concerns (72).

Many participants reported that they use their smartphone or laptops to surf the web, and they supplement these devices with additional screen-reading (e.g., JAWS, Apple VoiceOver) and/or screen-magnifying (e.g., ZoomText) software. To support ecological validity within the lab setting, we adapted each session's apparatuses depending on the participant's preferred devices.

All on-screen interactions were captured, and conversations during the tasks and interviews were recorded and transcribed. We analyzed the transcripts using Braun & Clarke's thematic analysis framework [5]. We identified our main themes (*Attitudes*, *Behaviours* and *Concerns*) of interest prior to coding to align with our research goals.

Pictured in Figure 1, the main researcher completed an initial pass through of the transcripts. They grouped related extracts to form trends, or codes, and then created a code book based on these findings. Another researcher used this code book to analyze five of the 14 transcripts.

The average inter-rater agreement across all codes between the two researchers ranged from 0.52 to 0.85 with a median of 0.68. This can be interpreted as good agreement, or that our analysis of the data is suitable. Areas where researchers disagreed pertained mainly to two codes: *guesswork* (extracts where participants hypothesized about how the system works, what it is doing, or how to interact with the system to achieve their ends) and *obstacle workarounds* (extracts where participants tried overcoming obstacles while completing tasks). The researchers credited these disagreements to the ambiguous nature of the codes and worked together to reach agreement on these excerpts.

Results

In this short paper, we focus on a few key points relating to participants' performance during the tasks and the concerns they reported during the interviews.

Verifying website legitimacy

Zero out of six participants identified our spoof website as illegitimate. Their decisions in assessing legitimacy were heavily influenced by familiar logos, links, and page content expected from past experience with the legitimate website. This is concerning because we easily duplicated these aspects of the CNIB website on our spoof website.

The domain of our spoof website, `ccnib.ca`, did not match the legitimate website's, `cnib.ca`. We intended this to hint towards its illegitimacy, but it was easily missed by participants. Blind participants were at a greater disadvantage when detecting the spoofed URL as JAWS pronounced both as "cuh-nib dot cah." These participants would need to parse the URL one letter at a time to detect the phishing cue but none did so, and it is likely no user would unless they were already suspicious of the website.

Logging in

Form fields were not consistently compatible with accessibility software. Additionally, error messages for failed logins were buried within page content and users had to meticulously parse the site to find why the login failed.

Users also received insufficient feedback to signify a successful login. Upon success, the login page typically refreshed with new content. After scanning the page, partially sighted participants were able to see the content change and confirm they had signed in. Blind participants using screen readers would have to parse the entire page to decipher if content had changed and if their private information was now being shown on the screen.

Websites masked passwords with asterisks, and the screen reader read out the characters as “star” while typing. These masking techniques were intended to keep passwords private from someone who might be watching (or listening) but, those with severe vision loss cannot see the keyboard while they type nor receive feedback confirming which key was pressed.

All participants with visual impairments faced usability issues when logging into the websites. Blind participants were at a greater disadvantage as they were left to guess if the login succeeded and if they were typing their password correctly. These issues greatly hinder users’ abilities to manage their account security and protect private information available through their accounts.

Making a financial transaction
Participants expressed great concern in protecting their financial information and identity so, issues pertaining to tasks involving making a purchase or donation were of particular interest.

Two blind participants were unable to complete a purchase on Amazon due to insufficient error handling. Essentially, Amazon wanted the user to reformat their shipping address before proceeding. The differences between the participant’s input and the “correct” version was shown with red, bold letters yet the screen-reader read the original and modified versions in the same way. Blind participants could not detect these necessary changes and would require aid from a sighted individual to advance. This issue compromises participants’ independence and control over their private information.

No significant accessibility or usability issues hindered participants’ success in making a donation through our spoof website. We provided participants with credit card information and the site was hosted on our lab servers, therefore participants were not at risk nor did they lose money. However, there were no mechanisms in place to protect the users from completing this transaction on a fraudulent website. In addition to JAWS reading the spoofed URL just like the legitimate URL, there were little reliable cues protecting users with visual impairments from such phishing risks.

Discussion

Like sighted users, users with visual impairments use unreliable cues to assess whether they are browsing securely. Their difficulties are compounded, however, because their ability to access recommended security indicators is limited by severe usability and accessibility obstacles. Despite increased awareness about accessibility, even popular websites and web browsers lack compatibility with assistive technology such as screen readers and magnifiers, especially when it comes to security cues.

Without addressing these issues, users with visual impairments will continue to be vulnerable. Even when the required information was accessible through screen-readers and screen-magnifiers, the contextual meaning required to perform a task securely was lost. This suggests that adhering to existing accessibility guidelines (e.g. providing large fonts, high-contrast colours, and alternative text) is insufficient for enabling secure and privacy-conscious behaviour. Future work should focus on finding inclusive solutions that recognize the unique challenges posed by security and privacy.

Acknowledgements

This work was supported by an eCampusOntario Digital Inclusion Research Grant for 2017-2018.

REFERENCES

1. A. Abdolrahmani and R. Kuber. 2016. Should I Trust It When I Cannot See It?: Credibility Assessment for Blind Web Users. In *ASSETS*. ACM, 191–199.
2. T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia. 2015. Privacy Concerns and Behaviors of People with Visual Impairments. In *CHI*. ACM, 3523–3532.
3. S. Azenkot, K. Rector, R. Ladner, and J. Wobbrock. 2012. PassChords: Secure Multi-touch Authentication for Blind People. In *ASSETS*. ACM, 159–166.
4. N. Barbosa, J. Hayes, and Y. Wang. 2016. UniPass: design and evaluation of a smart device-based password manager for visually impaired users. In *UbiComp*. ACM, 49–60.
5. V. Braun and V. Clarke. 2012. Thematic Analysis. In *APA handbook of research methods in psychology*. Vol. 2. American Psychological Association, Washington, DC., Chapter 4.
6. D. Briotto Faustino and A. Girouard. 2018. Bend Passwords on BendyPass: A User Authentication Method for People with Vision Impairment. In *ASSETS '18*. ACM, 435–437.
7. M. Buzzi, M. Buzzi, B. Leporini, and F. Akhter. 2009. User trust in ecommerce services: perception via screen reader. In *NISS'09*. IEEE, 1166–1171.
8. B. Dosono, J. Hayes, and Y. Wang. 2015. "I'm Stuck!:" A Contextual Inquiry of People with Visual Impairments in Authentication. In *SOUPS*. USENIX, 151–168.
9. S. Garfinkel and H. Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124.
10. F. Inan, A. Namin, R. Pogrund, and K. Jones. 2016. Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society* 19, 1 (2016), 28.
11. J. Lazar, J. Feng, T. Brooks, G. Melamed, B. Wentz, J. Holman, A. Olalere, and N. Ekedebe. 2012. The SoundsRight CAPTCHA: An Improved Approach to Audio Human Interaction Proofs for Blind Users. In *CHI*. ACM, 2267–2276.
12. D. Marques, T. Guerreiro, L. Duarte, and L. Carriço. 2013. Under the table: tap authentication for smartphones. In *Proceedings of the 27th International BCS Human Computer Interaction Conference*. British Computer Society, 33.
13. D. Napoli. 2018. Developing Accessible and Usable Security (ACCUS) Heuristics. In *CHI EA '18*. ACM, SRC16:1–SRC16:6.
14. G. Regal, E. Mattheiss, M. Busch, and M. Tscheligi. 2016. Insights into Internet Privacy for Visually Impaired and Blind People. In *International Conference on Computers Helping People with Special Needs*. Springer, 231–238.
15. Y. Wang. 2017. The Third Wave?: Inclusive Privacy and Security. In *Proceedings of the 2017 New Security Paradigms Workshop (NSPW 2017)*. ACM, 122–130.