Accessible Mobile Security Design for Individuals with Visual Impairments

Dan Black
DePaul University
243 S Wabash
Chicago, IL 60614, USA
danieljblack4@gmail.com

Mary Bungum
DePaul University
243 S Wabash
Chicago, IL 60614, USA
mbungum88@gmail.com

Jason Justice
DePaul University
243 S Wabash
Chicago, IL 60614, USA
jjustice90@icloud.com

Stella Sarbalieva
DePaul University
243 S Wabash
Chicago, IL 60614, USA
stella.sarbalieva@gmail.com

Abstract

Individuals with visual impairments are particularly susceptible to privacy and security threats while using mobile technologies in public. Limited work has been conducted to correlate security management habits and attitudes regarding mobile device security for visually impaired users. In this study, we conducted a contextual inquiry into security management habits and accessibility obstacles encountered by individuals with visual impairments. Our findings show that visually impaired users are aware of privacy and security threats and utilize security self-management methods. We also found obstacles to mobile device security accessibility are environment-related rather than interface-related. For example, participants required sighted assistance for credit card entry into secure applications. We propose that self-management techniques for visually impaired users are widespread and that broader design integration of non-accessible secure artifacts is necessary. Further work would include contextual inquiry with a wider age range and researching the motivations of users regarding security self-management methods.

Author Keywords

Security; Privacy; Individuals with Visual Impairments; Mobile; Screen Reader; Biometrics

ACM Classification Keywords

K.6.5 Security and Protection, Authentication, Physical security, Unauthorized access, Accessibility,

Introduction

Threats to privacy and security while using technologies are an increasing concern [1]. Individuals with visual impairments are particularly susceptible; for example, there is a high risk of aural and visual eavesdropping when logging into devices and private accounts [1,3]. In other words, while voiceover technology is a great aid to accessibility, it presents security risks to aural eavesdropping when individuals enter personal information such as passwords in public [3].

Additional accessibility concerns for users with visual impairments when entering private information have been reported. Individuals with visual impairments have difficulties entering and submitting online forms when they encounter CAPTCHA and other inaccessible online mechanisms [1]. Although individuals with visual impairments find online transactions including online banking and shopping more accessible than visiting brick-and-mortar retailers, they have security concerns about getting their credit cards and information stolen during online transactions [1].

Individuals with visual impairments use a variety of strategies to address their security concerns. Ahmed et al. (2015) found that individuals with visual impairments do have concerns about privacy when they enter personal information [1]. In such cases, they either arrange to be alone or with a family member or friend that can help them [1]. Ahmed et al (2016) found six strategies individuals with visual impairments use to cope with security concerns: avoidance, relocation, mitigation, help from others, adaptation, and acceptance [2]. For example, individuals with visual impairments change their location in public or turn off their mobile device's screen to confront shoulder-surfing and eavesdropping concerns [2]. Individuals with visual impairments also avoid certain security situations by not using their mobile phones outside their home and through confusion by intentionally making mistakes when typing their password [2].

Many applications have been created to combat against mobile security risks. Azenkot et al. (2012) created and evaluated 'Passchords', an accessible mobile device password entry application [3]. 'Passchords' uses a series of finger taps on a touchscreen surface for mobile device authentication [3]. The researchers found that 'Passchords' was 75% faster to enter than iPhone's Passcode with Voiceover with the same authentication rate [3]. More recently, other methods to assure privacy have been explored.

Researchers have created and evaluated technologies that use (a) an individual's gait pattern, (b) facial recognition, and (c) drawn patterns for accessible authentication. Poh et al. (2015) found that facial recognition software was not accessible and usable for individuals with visual impairments because they had trouble taking selfies [5]. However, other studies have shown success implementing alternative security authentication techniques. Haque et al. (2013) found that an individual's gait pattern is unique and can be used as an accessible authentication method with a mobile device's built-in accelerometer and gyroscope [4]. Sun et al. (2014) created and evaluated 'TouchIn', an accessible authentication system. 'TouchIn' allows users to draw on the touchscreen with one or more fingers to unlock their mobile device. The password authentication system is based on the geometric properties of user drawn curves and drawing speeds [6]. The researchers found that 'TouchIn' is highly usable and resilient to shoulder surfing attacks [6].

Biometric fingerprint reader technology is common, and little is known about the frequency of use for individuals with visual impairments. Additionally, limited work has been conducted in exploring how individuals with visual impairments feel about mobile security and privacy. In this study, we explore how people with visual impairments manage private and secure information on their mobile devices and what obstacles they encounter when accessing secure information.

Methods

In the following section, we will discuss participants, data collection, and data analysis.

Participants

We recruited four participants through our contacts at the Chicago Lighthouse. All participants were individuals with visual impairments and lived in the Chicago area. At the time of this study, all participants owned smartphones and used them daily.

Participants	Age	Gender	Fingerprint Biometrics
P1	67	Female	Yes
P2	31	Male	Yes
P3	29	Female	Yes
P4	26	Female	No

Data Collection

We conducted a contextual inquiry study to better understand security habits of those with visual impairments pertaining to smartphones. We asked participants about (1) interaction with smartphones in general, (2) security and privacy habits when using mobile devices, and (3) general security concerns. We observed three participants utilize mobile device authentication and access accounts that required their secure authentication.

The interviews were conducted with one moderator and one facilitator. Each session lasted approximately 30 to 60 minutes. The interviews were audio and video recorded and then transcribed. All interviews were conducted in person.

Data Analysis

We inductively coded the collected data for common and salient themes using *In vivo* and descriptive coding.

Findings

In this section, we describe the findings collected from our contextual inquiry. We focused our findings on the most relevant themes as it relates to our research questions.

Participant Security and Privacy Management Methods

VoiceOver

All four participants used VoiceOver to have the content on the phone interface read aloud. One of the participants stated that having VoiceOver set to a fast speed eased some of his security risks because he believed it was too fast for people to understand.

Awareness of Security and Privacy Threats in Public

All of our participants were aware of aural and visual eavesdropping threats in public spaces. The participants were all aware of PassCode and biometric authentication in regards to Touch ID and their Apple iPhone. All of our participants also took defensive steps regarding publicly accessing material they deemed private.

Touch ID Authentication

All of our participants were aware of Touch ID authentication on their mobile devices. Three of our four participants used an authentication method to unlock their phones. The three participants used Touch ID as the method to access their mobile devices.

One of those three participants, P1, used Touch ID but her fingerprint had not been authorized since it was purchased. She told us she was prompted to enter her password after three failed attempts of Touch ID every time she wanted to unlock her phone. P4 chose not to use Touch ID because she described herself as "fidgety with her hands" and frequently opened her phone. She did not want to use an authentication method each time she accessed her phone and have alerts read out loud including the time and text messages when opening her phone.

Screen Curtain
Three of the participants used a screen curtain feature that blocked onlookers from seeing how the participants interacted with their screens. The use of a screen curtain renders a screen black while remaining fully functional. P4 stated that the screen curtain was her only method of blocking visual eavesdropping threats. She felt that the obscured screen was enough of a security measure to prevent visual eavesdropping in public. P1 is aware of screen curtain features but chose not to implement it due to possible assistance needed for unspecified activities.

Earbud Habits
Earbuds provide a universal way to block unintentional audiences from listening to content on a mobile device. Earbuds were used variably by each participant. Their environment had the greatest effect in determining when they were used. P2 stated he did not use earbuds while walking in public. He preferred to focus on his surroundings while walking and could not afford distractions. However, he did use earbuds if he was stationary, such as sitting on a bus or in an office.

Public Habits
P1 stated she did not use her phone in public, except for special circumstances. P1 feared damage, theft, and breach of privacy by using her phone in public. She also stated she did not like talking on her phone in public. P3 and P4 said they did use their phones in public. P3 and P4 did not mention any specific reservations on using their mobile devices in public. P4 thought that using screen curtain and earbuds in public was adequate protection against potential security threats.

Security Accessibility Obstacles

Credit Cards
All four participants stated inputting credit card information into a phone was difficult and sometimes required outside assistance. P2 mentioned that he did not like having his credit card stored in his phone and uses gift cards instead. P1 did not like having credit card information stored in her phone but is not aware of alternatives. P4 had difficulty taking photos of her credit card when she wanted to enter payment information for Uber and Lyft. P3 and P4 had trouble making purchases on their phones when online orders required secure CAPTCHA authentication. P3 and P4 mentioned that CAPTCHA programs for making secure purchases online were entirely inaccessible.

Three out of four participants had a history of making purchases on their mobile devices. They all discussed their struggles to enter credit card information into a secure interface. Sites that allowed for a user to photograph a credit card to substitute user digit-entry were not accessible for our participants. P4 described her difficulty when she told us, "*I had to lay the card out a certain way to capture the information and I couldn't do that on my own.*" P3 spoke about needing sighted help to enter her prescription number from her medication bottle into her secure web ordering interface. P3 stated, "*When they asked me about my prescription number I had to have sighted assistance, and if I hadn't had the sighted assistance it would have been impossible for me.*"

Accounts Requiring Secure Login
P2 and P4 used their phones for online banking. P2 used a banking application that utilized Touch ID to authorize login. He liked that some applications had Touch ID as an alternative login procedure. P4 did not save her login credentials on her mobile banking account. She feared someone hacking her mobile account if she remained logged in. P3 used a secure account to access her prescription medication orders.

She described her struggles to login and enter her prescription medications in her online account. She used outside assistance and a Bluetooth keyboard as an aid when she had trouble with the account accessibility.

Typing Obstacles

Typing was one of the main accessibility obstacles participants encountered when using a mobile device. P3 and P4 mentioned difficulty typing using the touch-typing feature on the iPhone. One of the main reasons for this difficulty was the flat surface of the phone. There was nothing raised on the touchscreen to indicate what letter they were touching while using their smartphones. P4 was easily annoyed by touch typing since the touchscreen was sensitive and made it easy to type a letter incorrectly. This was one of the main reasons she did not use the Passcode security authentication feature on her iPhone. P4 additionally stated she was not satisfied with her current iPhone and missed her Blackberry device. The QWERTY keyboard on her Blackberry had been much easier for her to use. P3 overcame her touch-typing difficulties by using a Bluetooth keyboard.

VoiceOver Obstacles

P4 had issues with VoiceOver reading her text messages automatically when she opened her phone. She felt this was a privacy threat since her text messages are personal and they were sometimes read aloud in public when she was not using earbuds. She wished that VoiceOver would give a simplified alert without fully reading a new text message.

Discussion

In this section, we discovered four main themes from our contextual inquiry findings. Next, we discuss the limitations of our study and our plans for future research.

Use of Mobile Devices for Secure and Non-Secure Applications

Our participants made heavy use of mobile devices in their daily lives. They used their devices for a wide variety of purposes. Most common were non-secure uses including communicating with family and friends, general information, checking email, social media, and navigation. All four participants used the iPhone VoiceOver function as an aide to mobile device accessibility. Three of our participants used their mobile devices for applications requiring secure logins, and all four participants made purchases using their mobile devices. The limited use of mobile devices for highly secure applications meant that our participants felt comfortable interacting with their phones in a wide variety of contexts. However, participant privacy on mobile devices when engaging in personal communications did impact user mobile device behavior.

Awareness of Eavesdropping Threats in Public

All participants were aware of eavesdropping and shoulder surfing threats in public. This confirms previous research carried out by Ahmed et al. (2015) and Azenkot et al. (2012). The researchers found that aural and visual eavesdropping was a serious security threat to individuals with visual impairments when entering private information in a public setting. Also, individuals with visual impairments were aware of such threats [1,3].

The awareness of these security threats gave our participants an appreciation and desire for more accessible security design in their mobile devices. P3 explained how grateful she was to have Touch ID on her recent iPhone purchase: "*Fingerprint Touch ID has made it much easier for me and more private*." She also described her desire for more applications and mobile sites to integrate Touch ID into design. P2 stated, *"I think that all apps that require people to login should use the Touch ID feature."* P2's opinion complemented P3's thoughts that having Touch ID was a more viable option for authenticating accounts. He expressed that it would make it easier and accessible for users with visual impairments. Our findings support the need for easily accessible privacy and security features when designing for mobile devices.

Self-management of Security Threats

All participants used various self-management methods to mitigate security threats. Most common methods included iPhone's screen curtain, earbuds, and custom accessibility configurations. Our study confirms previous research by Ahmed at el. (2015) that individuals with visual impairments use various management methods to mitigate security and privacy threats [2, 3].

Using their own security self-management methods, three of our four participants felt comfortable using their mobile devices in public. P1 mentioned feeling uneasy using a smartphone in public. She also did not use screen curtain or earbuds. We attribute this to the participant describing how she was not comfortable with technology in general.

The overarching attitude towards mobile device security was that self-management was enough to keep their devices secure. However, their self-management methods were not robust or designated for the task of mobile device security. Therefore, there is a need for even greater awareness of mobile device security methods for those that are visually impaired. Broader adoption of dedicated accessible mobile security methods is warranted.

Difficulty with Secure Mobile Interactions

Our contextual inquiry led us to find unique obstacles to secure mobile device interactions. Our findings show that participants need sighted assistance to enter secure data such as credit card numbers into secure interfaces. The accessibility obstacle for secure application design is not due to the interface. Instead, our observations suggest that non-accessible secure artifacts need to be taken into account when designing secure applications.

Another obstacle to secure information entry was the actual surface of a mobile device. Our observations show that the flat screen of an iPhone has no tactile feedback for a visually impaired user to anchor their touch input. Secure password login requires accurate input or a user cannot login. Participants exhibited frustration when making secure password entry errors due to the lack of a tactile QUERTY keyboard. Our data suggests that participants would be more satisfied with tactile or haptic anchors on their mobile device screens.

Our findings show that advancements in technologies have made a noticeable difference for accessible secure applications. However, the obstacles faced by users with visual impairments when interacting with secure applications are no longer within the design of the interface. The current need is for a fully accessible experience designed to integrate secure data from a variety of sources.

Limitations

There were some limitations in our research that may have prevented us from gathering additional themes. It was difficult to generalize our findings to a larger population due to our small sample size. Furthermore, having a larger sample size may have increased our insights towards recognizing more patterns.

Future Work

In future work, we would like to learn about the motivations behind the self-management habits and how users with visual impairment came to adopt them into their lifestyle. We would also look to focus future contextual inquiries into topics such as age group and familiarity with technology.

References

1. Ahmed, T., Hoyle, R., Connelly, K., Crandall, D., & Kapadia, A. (2015, April). Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 3523-3532). ACM. doi:10.1145/2702123.2702334

2. Ahmed, T., Shaffer, P., Crandall, D., & Kapadia, A. (2016). Addressing physical safety, security, and privacy for people with visual impairments. In *Proceedings of the twelfth symposium on usable privacy and security.* (pp. 341-354). Retrieved from https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-ahmed.pdf

3. Azenkot, S., Rector, K., Ladner, R., & Wobbrock, J. (2012, October). PassChords: secure multi-touch authentication for blind people. In *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility* (pp. 159-166). ACM. doi:10.1145/2384916.2384945

4. Haque, M. M., Zawoad, S., & Hasan, R. (2013, November). Secure techniques and methods for authenticating visually impaired mobile phone users. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on* (pp. 735-740). IEEE. doi:10.1109/THS.2013.6699095

5. Poh, N., Blanco-Gonzalo, R., Wong, R., & Sanchez-Reillo, R. (2016). Blind subjects faces database. *IET Biometrics*, *5*(1), 20-27. doi:10.1049/iet-bmt.2015.0016

6. Sun, J., Zhang, R., Zhang, J., & Zhang, Y. (2014, October). Touchin: Sightless two-factor authentication on multi-touch mobile devices. In *Communications and Network Security (CNS), 2014 IEEE Conference on*(pp. 436-444). IEEE. doi:10.1109/CNS.2014.6997513