Understanding Authentication Method Use on Mobile Devices by People with Vision Impairment

Daniella Briotto Faustino and Audrey Girouard
Carleton University
Ottawa, ON, Canada
daniella.briottofaustino@carleton.ca, audrey.girouard@carleton.ca

ABSTRACT

Passwords help people avoid unauthorized access to their personal devices but are not without challenges, like memorability and shoulder surfing attacks. Little is known about how people with vision impairment assure their digital security in mobile contexts. We conducted an online survey to understand their strategies to remember passwords, their perceptions of authentication methods and their self-assessed ability to keep their digital information safe. We collected answers from 325 people who are blind or have low vision from 12 countries and found: most use familiar names and numbers to create memorable passwords, the majority consider fingerprint to be the most secure and accessible user authentication method and PINs the least secure user authentication method. This paper presents our survey results and provides insights for designing better authentication methods for people with vision impairment.

Author Keywords

Blind; low vision; vision impaired; password; user authentication methods; smartphones; mobile devices.

ACM Classification Keywords

Security and privacy → Human and societal aspects of security and privacy → Usability in security and privacy

INTRODUCTION

Currently, there is little information about security for people with vision impairment while interacting with mobile devices [22]. People with vision impairment are those who are blind in one or both eyes, or those who have low vision and cannot read a newspaper even when wearing typical corrective lenses [33]. Previous research showed the majority of people with vision impairment did not use authentication methods to protect their smartphones because they considered the alternative available (PINs) either inaccessible or inconvenient [7, 17]. In addition, researchers found accessibility issues in authentication with ATMs [13], CAPTCHAs [31], and patterns drawn on the screen [8]. Also, people with vision impairment are more vulnerable to shoulder surfing and aural eavesdropping when entering PINs [20]. However, even though more user authentication methods are now available (e.g. fingerprint and facial recognition), we do not have information about which of the existing methods people with vision impairment consider more secure, more accessible or preferable.

In 2015, Bourne et al. [12] estimated that 36 million people were blind and 217 million were moderately or severely vision impaired, for a total of 253 million people living with vision impairment around the world. Thanks to the rise of accessibility features and applications for mainstream devices, the number of people with vision impairment using smartphones is increasing [14, 20]. Consequently, they are relying more on the technology, making it essential to assure their privacy and security protections [22].

To better understand how people with vision impairment perceive and navigate user authentication methods, we conducted a comprehensive online survey to answer the following research questions:

1) How do people with vision impairment self-assess their ability to keep their digital data secure?
2) Which is the user authentication method considered more secure and accessible for people with vision impairment?
3) What are the differences between people who are blind and people who have low vision in their preference and opinion on user authentication methods?

To the best of our knowledge, this study is the first to extensively explore the relationship people with vision impairment have with passwords and user authentication methods. Through an analysis of the answers from 325 vision impaired respondents, the contributions of this work are: (1) an overview of the main challenges faced by people with vision impairment when dealing with passwords; (2) insights on how people with vision impairment perceive different user authentication methods; (3) a comparison between people who are blind and people who have low vision regarding digital security.

This paper starts with Related Work centered around user authentication methods and security concerns for people with vision impairment on a mobile context. Survey Methodology describes the development and distribution of

ASSETS '18, October 22–24, 2018, Galway, Ireland

ACM ISBN 978-1-4503-5650-3/18/10…$15.00
https://doi.org/10.1145/3234695.3236342

the online survey, while the Results reports on participants, password use, authentication methods in mobile devices, and use of smartphones and authentication. Discussion weights the most important findings and how they relate with previous work.

RELATED WORK

In 2016, 77% of sighted adults from the United States of America (US) said they own a smartphone, a large increase from 2011 where the percentage of smartphone owners was 35% [30]. With the increase in smartphone adoption, more personal data is stored in them, such as name, address, email and geolocation [22]. To protect smartphones from unauthorized access (and consequently the personal information saved in them), users have to prove they are who they are claiming to be, through a user authentication method [25]. The methods available can be categorized as: *something you know* (knowledge-based, such as PINs, alphanumeric passwords or patterns drawn on the screen), *something you have* (token-based, such as smart cards), and *something you are* (biometric-based, such as fingerprints, facial recognition, voice recognition, iris scans) [22]. The options most commonly used by sighted Americans were PINs (26%), fingerprint (23%), passwords (9%), and patterns (9%), but 28% did not use any method to lock their screen and avoid unauthorized access [30].

Besides from being the most ubiquitous option, PINs are considerably more secure than patterns, as even a 2-digit PIN is most secure than a pattern of dots connected by drawing on the screen, because people tend to create very simple patterns [4]. On the other hand, both PINs and alphanumeric passwords require users to memorize a sequence of characters, a disadvantage when compared to biometric methods. Fingerprints, for instance, allow for a reliable individual identification [11], though they have issues, such as high false rejection rates, and the impossibility of replacing one's fingerprint in case the information is compromised [25]. Ultimately, biometrics does not replace passwords, and "can be considered a re-authenticator or a secondary-authentication device as a user is still required to have a PIN or pattern that they enter rather frequently due to environmental impacts (e.g., wet hands)" [5].

Smartphones are powerful devices, offering a myriad of functions and access to different social spheres, but for the blind or vision-impaired user, they are limited by the ubiquity of touch screen interfaces [15]. Blind individuals can explore the UI elements on their touch screen with the support of embedded screen readers, even though this is a slow and error-prone process [6]. This extends to security, where typing PINs while using screen readers makes people with vision impairment more susceptible to others listening their passwords (aural eavesdropping), as the system reads out loud everything, even password entries [20]. Similarly, the use of screen magnifiers by those with low vision also increases the susceptibility for visual eavesdropping [20]. In addition, trying to type in a password is considered one of the most difficult things for people with vision impairment to do in a smartphone while using the internet [9].

Prior work from Ahmed et al. [2] indicates that most people with vision impairment feel uncomfortable to use passwords in public contexts for fear of eavesdropping and also have privacy concerns. However, other research indicate that the majority of people with vision impairment are choosing not to use passwords to protect their smartphones [7, 17]. One of the reasons given by participants for not using any authentication method was that they kept their smartphone close to them at all times [7, 38], even though this is not a secure practice. Another reason mentioned by some participants was the inconvenience of unlocking the device using PINs [7], potentially due to the penalty in time [36]. Additionally, among the user authentication methods currently available on smartphones, iris or retina scans can be problematic for people with vision impairment, *"who may have deformed or missing eyes, or no ability to open their eyelids"* [22], as patterns drawn on the screen are, because they require the selection of points on the touch screen [8, 22].

It is important to realize that users see security simply as a means to complete their tasks while having their data private. However, if security features are not accessible to them, it either makes them unable to access specific information or applications, or forces them to ask the help of others while completing required authentication procedures, possibly compromising their own security [22]. Prior research on the intersection of usability, security and accessibility are rare [31] and need further investigation [22]. This work aims to clarify both whether people with vision impairment are currently adopting user authentication methods and whether these pose accessibility issues to them.

SURVEY METHODOLOGY

We developed an online survey to collect data from blind and low vision individuals regarding their use of passwords and perceptions about user authentication methods and their own ability to protect their personal information in digital devices. Our hypotheses were:

H_1) People with vision impairment will not feel able to properly keep their digital information secure, because of accessibility issues with the visual cues and feedback provided [7] and the difficulty to assess if others are shoulder surfing their passwords [2].

H_2) People with vision impairment will choose fingerprints as the most secure authentication method due to its broad use [30]. They will also choose it as the most accessible method as it is a biometric method, which does not require entering a password and is available in most smartphones [26].

H_3) As to the best of our knowledge no previous work investigated differences in preference and opinions regarding authentication methods between people who are blind and people who have low vision, we expect no difference between the two groups.

Survey Design

We applied the guidelines proposed by Kaczmirek and Wolff [21] to create an effective self-administered survey for vision impaired participants. We developed 30 multiple-choice or text-entry questions, divided in four groups: 1) demographic information, 2) use of passwords in general, 3) point of view on existing user authentication methods available for mobile devices and 4) use and protection of mobile devices. We posted the survey in both English and Portuguese using the platform Qualtrics [28], where we numbered all questions and added additional explanation in brackets to help participants to answer (e.g. "choose all that apply", for multiple-choice questions or, "write your answer" for text-entry questions). We did not list consecutively alternatives starting with the same letters to facilitate their selection by participants using screen magnifiers, which focuses in a single area of the screen at a time. For this reason, we did not randomize the lists of alternatives in any of the questions.

Before distributing the survey, we tested it with two human-computer interaction specialists to evaluate the appropriateness of the questions and their sequencing to avoid introducing bias. We also tested it with two people who are blind, using both a smartphone and a computer, to identify accessibility issues or other problems that might impact completion or ease of use. We distributed the survey by email to organizations that support people with vision impairment from 31 countries (e.g. Lighthouse for the Visually Impaired and Blind, or the Canadian Council of the Blind). The survey was open for two and half months from December 2017 to February 2018. Participants who declared being vision impaired and at least 18 years-old qualified to participate. As a token of appreciation, we drew a $50 gift card to one participant at random. We obtained ethical clearance from the Carleton University Research Ethics Board (CUREB-B # 102815).

Terminology

According to Kleynhans and Fourie [3], the terms visually impaired, partially sighted and low vision are used interchangeably in the literature to indicate residual vision. In our survey, we opted to use the term vision impaired, in accordance with the World Health Organization (WHO) [34], the Center for Disease Control and Prevention [19] and the Government of Canada [16]. However, we also considered the suggestion from Cavender et al. [1] on clarifying if a person referred as "blind" is someone who uses screen readers to access a computer, by adding a question on what assistive technologies participants use.

Analysis of Results

One researcher performed quantitative analysis of the multiple-choice answers using R Studio [29] and qualitative analysis of the text-entry answers using NVivo [27]. Quantitative analysis included chi-square tests (χ^2) of categorical data and t-tests (t) of numerical data, but we only report statistically significant results. We conducted the qualitative analysis using grounded theory [17] to code the different themes that emerged for each question. Whenever necessary, we coded answers in more than one theme, but we did not code unclear answers.

PARTICIPANTS

This section presents participants' demographics (including their vision impairment) and assistive technology use.

Demographics

We collected 325 complete answers from adults with vision impairment. From those, 223 declared they were blind, 93 declared they had low vision and the remaining 9 declared they had other vision impairments such as tunnel vision and limited central vision. We grouped them with either the blind group or the low vision group based on the WHO classification [37], to consolidate the analysis in only two groups with similar characteristics. The regrouping resulted in a total of 225 blind participants (69.2%) and 100 with low vision (30.8%). Most participants have been vision impaired for their entire adult life, as they reported becoming impaired at a median age of 1 year old (*Mean (M)* = 8.29, *SD*=13.56).

Most participants resided in the US (72.3%) or Canada (15.1%). Other participants resided in 10 countries (Brazil: 5.2%; Portugal: 1.5%; Australia, Jamaica and New Zealand: 1.2% each; the U.K.: 0.9%; Barbados, Bosnia and Herzegovina, Mongolia and Trinidad and Tobago: 0.3% each). Gender was almost evenly distributed, with 169 (52%) females and 153 (47.1%) males. Ages ranged from 18 to 80 years-old, but most were middle-aged adults (*M*=45.73, *Median*=45). Besides being vision impaired, some (N=49, 15.1%) reported having another physical or cognitive impairment, most commonly related to hearing loss (N=27) as grouped by the WHO classification [37]. Considering participants with other impairments were equally spread among the two groups (blind and low vision), we choose not

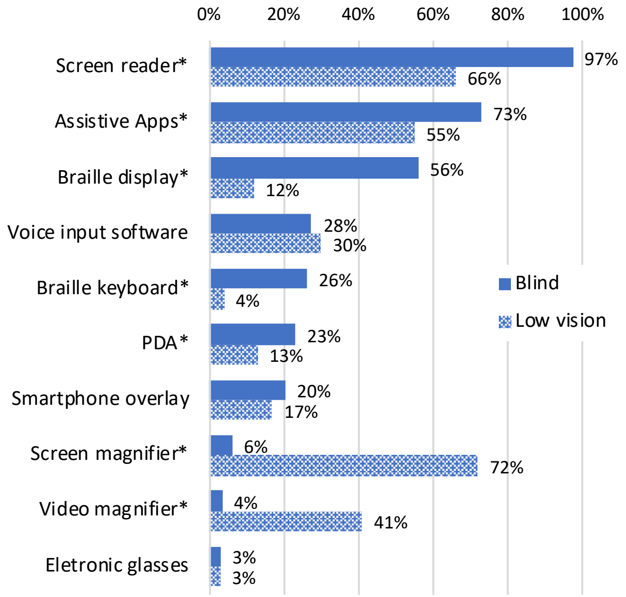

Figure 1: Blind and low vision participant's use of assistive technology. Significant differences marked with *.

to analyze their answers separately. Participants took a median time of 24 minutes to answer the online survey.

Use of Assistive Technology

We asked participants to select assistive technologies they used from a list with 10 options. Among the most commonly used were: screen readers (87.7%), assistive apps (67.4%) and Braille displays (42.5%). Figure 1 shows the assistive technology use. Only seven participants reported not using any of the devices listed in the question.

We compared the use between the two groups (blind and low vision). We found the use of the following assistive devices were significantly larger by blind participants than by participants with low vision: screen readers (χ^2 (1, N=325) = 62.98, p <.001), Braille display (χ^2 (1, N=325) = 54.86, p <.001), Braille keyboard (χ^2 (1, N=325) = 21.88, p <.001), assistive smartphone applications (χ^2 (1, N=325) = 10.08, p <.005), and personal digital assistant (PDA) (χ^2 (1, N=325) = 4.42, p <.05). On the other hand, the use of the following assistive devices was significantly larger by participants with low vision: screen magnifier (χ^2 (1, N=325) = 153.93, p <.001 and video magnifier (χ^2 (1, N=325) = 75.81, p <.001). The results on the use of screen magnifiers and screen readers are consistent with previous research [3]. But our results also indicate people who are blind require the use of more assistive technologies than people with low vision, except for devices that support the use of residual vision.

Participants who became vision impaired earlier in life were more likely to use Braille displays (M=3.9 vs. M=11.5, t (321) = 2.81, p <.005). This indicates Braille education is probably given to people who are blind since birth or since early childhood. Based on the use of assistive technology and following the suggestion of Cavender et al. [1], blind participants are those who use screen readers to interact with their digital devices, while low vision participants are those who are more likely use screen magnifiers, instead.

PASSWORD USE

This section reports the importance of passwords for participants, where they use them, their self-assessed ability to protect their digital information, their strategies for memorization and concerns with using passwords in public.

Importance of Passwords

We found that the large majority of the 325 participants showed concerns regarding securing their personal information, which is in line with previous findings [2]. Almost all participants (96%) said passwords are important or very important. Figure 2 illustrates the distribution of the results between the two groups (blind and low vision), although we did not find significant difference.

We asked participants to explain their rating of password importance, illustrated in Figure 3. Among participants who rated passwords as very important, important or neutral, most mentioned acknowledging the importance of passwords for protecting personal information (57.6%), followed by assuring their privacy and security (26%).

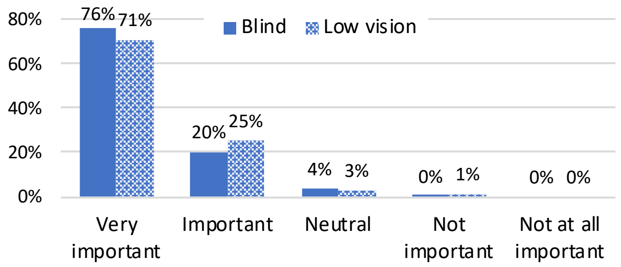

Figure 2: Blind and low vision participants' ratings for the importance of passwords.

Interestingly, twelve participants that chose very important or important discussed vulnerabilities of passwords, even citing the 2017 data breach on a credit information bureau, involving more than 140 million Americans [18]: "*[my information] should be protected as identity theft can be expensive to resolve. Unfortunately, no matter how secure we are, when companies like Equifax lose our data, all of our precautions are meaningless*" (P214). Some participants also said the importance of passwords depends on the context and the importance of the information being secured (N=6).

Previous experiences also affect how people with vision impairment perceive the importance of passwords. Two participants who said they did not have problems so far rated passwords as not important or neutral, whereas four that had bad experiences rated passwords as very important. For example, P23 said: *"Other people could easily gain access to my information as I cannot tell if they are watching me, I have had electronic devices stolen when I was not looking."*

Digital Presence

Participants' near unanimous evaluation of passwords as important is in line with their extensive password-protected digital presence (Figure 4). Only two participants declared not using passwords for any of the items we asked them about. We compared things participants reported to protect with passwords between the two groups and found that blind participants used online services more than those with low vision (χ^2 (1, N=325) = 3.86, p <.05).

Participants' digital presence significantly differ by age, as younger participants were more likely to use: email (M=44.3

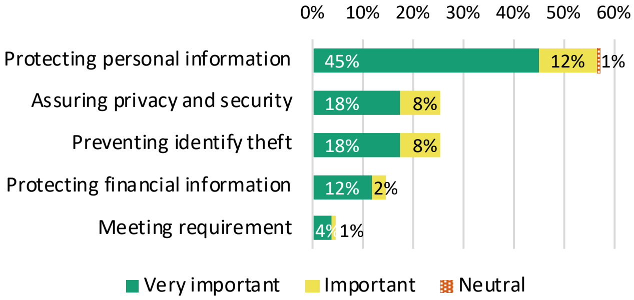

Figure 3: Participants' top five reasons for rating passwords as Very Important (green), Important (yellow) or Neutral (red).

vs. *M*=54.2, *t* (323) = 4.13, *p* <.001); social media (*M*=44.1 vs. *M*=50.5, *t* (323) = 3.26, *p* <.005); and personal devices (*M*=44.8 vs. *M*=50.8, *t* (323) = 2.53, *p* <.05). On the other hand, older participants were more likely to use: home security system (*M*=50.3 vs. *M*=44.8, *t* (323) = 2.14, *p* <.05); and online shopping (*M*=47 vs. *M*=42, *t* (323) = 2.52, *p* <.05).

The importance given by participants significantly differed by the items they secure with passwords. Participants who used the following were more likely to rate passwords as very important: online banking (χ^2 (3, N=325) = 36.13, *p* <.001), email (χ^2 (3, N=325) = 23.22, *p* <.001), password-protected personal devices (χ^2 (3, N=325) = 23.83, *p* <.001), and online services (χ^2 (3, N=325) = 12.61, *p* <.001). For example, 88% of participants who rated passwords as very important use them to protect their online banking, while half of those who rated neutral and all who rated not important do not use online banking. Therefore, participants who did not consider passwords important are likely not concerned as they do not risk their personal and financial data.

The number of unique passwords used daily did not significantly differ between blind and low vision participants (*M*=5.0 vs. *M*=4.7). It is similar to the sighted population, which reported having 5 passwords on average [32].

Strategies to Memorize Passwords

We asked participants to share the strategies they use to remember passwords. 33.5% mentioned creating passwords by using names of family members, pets, numbers or facts that are important for them: *"some configuration of the dates and names of my various Guide Dogs, our family's first phone number. Names of strange creatures […] in combo with either my birth or street number"* (P19). The second strategy most mentioned was creating a password model or structure and then slightly changing it to generate new passwords (24.9%): "*I use a base password […] and personalize it to each different site or service according to an algorithm that I use. This way I can remember the password, but it is different for each site/service."* (P233).

Other strategies include: relying on one's memory (16.6%), keeping a file with all the passwords (14.5%, while 11.7% save the file on the same device), keeping a written record of the passwords in a notepad or paper (11.4%), keeping a copy in Braille (8.3%), and either using a password management software or saving passwords in the browser (11.1%). Only participants who were blind mentioned saving passwords in a file in a different or disconnected device (N=9). Additionally, thirty participants admitted reusing passwords.

The strategies mentioned by our survey participants were similar to those found by Ahmed et al. [2]. Wash et al. [35], who also found that sighted people tend to reuse passwords, to both avoid having to memorize many of them, and to better memorize strong ones. Compared to strategies used by sighted people, we see a difference in proportion, as with the reuse of passwords (96%), password managers (81%), and written records (78%) [32].

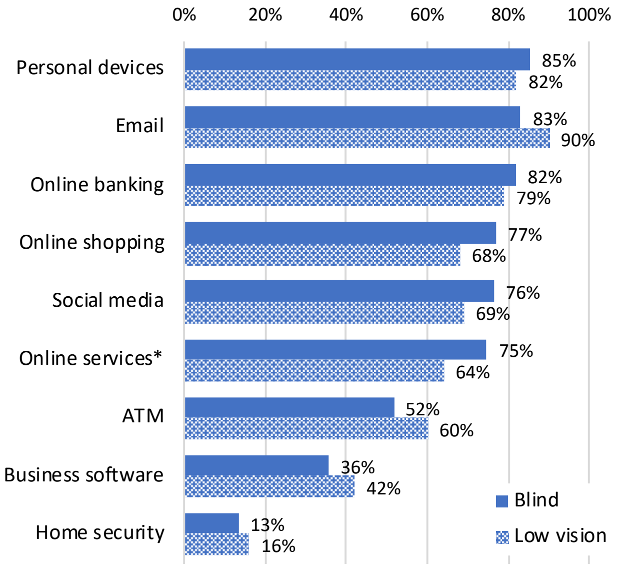

Figure 4: Blind and low vision participants' items protected with passwords. Significant differences marked with *.

Ability to Keep Digital Information Safe

We asked participants to rate their ability to keep their digital information safe. Most participants (47.4%) believed they were able to secure their digital information, followed by very able (33.8%) and neutral (14.8%) (Figure 5). We found no significant difference between the self-assessment of the two vision impairment groups. However, participants self-reported ability significantly differed by the importance they give to passwords (χ^2 (8, N=325) = 32.99, *p* <.001), as almost all participants who self-assessed as very able to protect their digital information also rated passwords as very important. As P303 said, "*This is because I understand the importance of a strong, safe password and use them all the time, plus I never give passwords to anyone."*

We compared the subset of participants who rated passwords very important and self-assessed very able to protect their information (VI-VA, N=96) to the rest of the participants in their use of online banking. We found a significant difference (χ^2 (1, N=325) = 5.12, *p* <.05), as VI-VA were more likely to do online banking than the others (88.5% vs. 62.7%). VI-VA used similar strategies to remember passwords as the others, but were more likely to use password management systems (*M*=0.19 vs. *M*=0.08, *t* (321) = 2.81, *p* <.005).

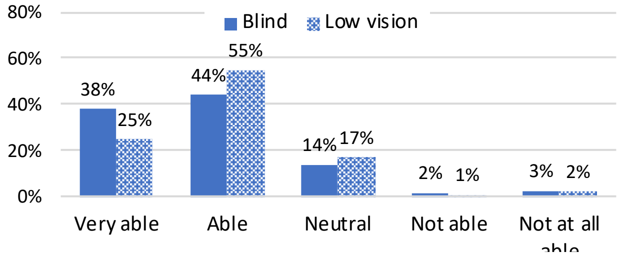

Figure 5: Blind and low vision participants self-assessed ability to protect their digital information.

We asked participants to explain their rating (Figure 6). Among the participants who rated themselves as able or very able to protect their digital information (N=264), the main reasons included their methods to create passwords (29.9%) and to save passwords (22.7%), such as using Braille version or password management systems. Other reasons included: being knowledgeable about security practises (13.6%) and having a good memory for passwords (10.9%).

The main reasons for not feeling fully able to protect their digital information were: the risk of attacks from hackers and malicious people (20%), the potential insecurity of services they use (13%), concerns with their methods to create (5.6%) and save passwords that could be improved (5.1%). A few other participants attributed their ability to accessibility issues (N=6), e.g. with websites that have moving numbers for passwords, and difficulty remembering passwords (N=7).

When comparing the two groups, participants who said they were able to protect their digital information justified it by their control over their security, e.g. *"My information is secure because of the methods I use to create the password."* (P178). However, participants who rated neutral or negatively tended to attribute their rating to external causes that they cannot control. For example, P140 who rated neutral said: *"Because if someone wants to hack into my PC there really isn't anything I can do to stop them, short of not being connected to the Internet, which isn't practical."*

According to P276, confidence might be acquired with appropriate training *"to learn how to get things done our way, it makes it very easy!"*. However, accessibility issues might prevent people with vision impairment to protect their privacy independently, as explained by P234: *"sometimes I have to ask for help to put in my numbers for the ATM [...] and the way that all the stores are going with touchscreen access for putting in your pin number and answering questions that they need you to answer is impossible to do because they do not have any screen readers on them whatsoever"*. Finally, six participants (split between very able and able) felt patronized with our inquiry about rating their ability of protecting their digital information.

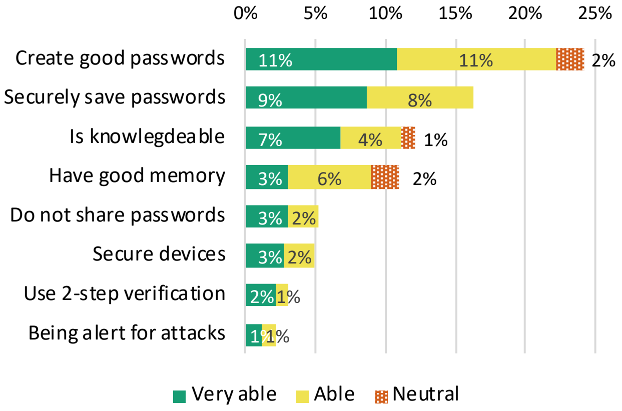

Figure 7: Participants' top five reasons to self-assess Very able (green), Able (yellow) or Neutral (red) to protect their digital information.

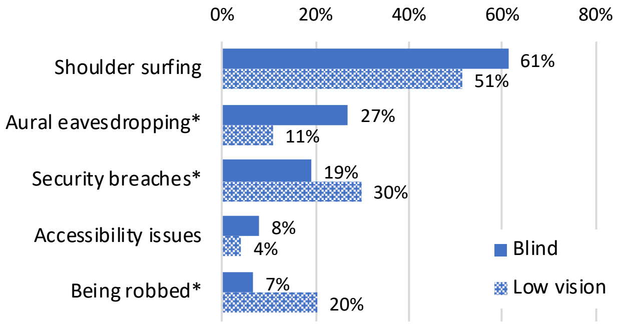

Figure 6: Blind and low vision participant's concerns with using passwords in public spaces, among those who had concerns (N=226). Significant differences marked with *.

Concerns with Entering Passwords in Public

69.5% of participants had concerns about entering passwords in public spaces (no significant difference between the two vision impaired groups). The main concern of participants was the risk of visual eavesdropping or shoulder surfing (N= 131, inclusively with the use of cameras), security breaches due to unsecured Wi-Fi networks or key logger programs (N=51), and the risk of aural eavesdropping, because screen readers read passwords aloud (N=49) (Figure 7). Blind participants were more concerned with aural eavesdropping than participants with low vision (M=0.27 vs. M=0.11, t (224) = 2.80, p <.005). Some participants also said they were afraid of being robbed (N=25). For example, P56 said he tries to type quickly to avoid others from seeing his passwords, as found in prior work [2], but notes *"if I do this I won't be able to type accurately, especially if I can't use speech"*. Additionally, a total of 15 participants said their concerns with using passwords in public spaces relate to accessibility issues, such as in stores that use inaccessible touchscreens.

Summary

We found that vision-impaired people have a strong digital presence and those who complete financial operations online are more likely to see passwords as a very important step to protect their digital information. Younger individuals are more likely to protect their personal devices with passwords. However, older participants are more likely to use online shopping, meaning they might be at higher risk of having their data compromised. In addition, as the most common strategy participants use to remember passwords is creating them using familiar names and numbers, most are at risk of using easily guessable passwords. Interestingly, participants' ability to protect their digital information is associated to the importance they give to passwords. This may be a function of a higher interest in learning how to better protect themselves, which in turn increases their self-confidence. Finally, vision-impaired people have concerns with using passwords in public because of the risk of shoulder surfing.

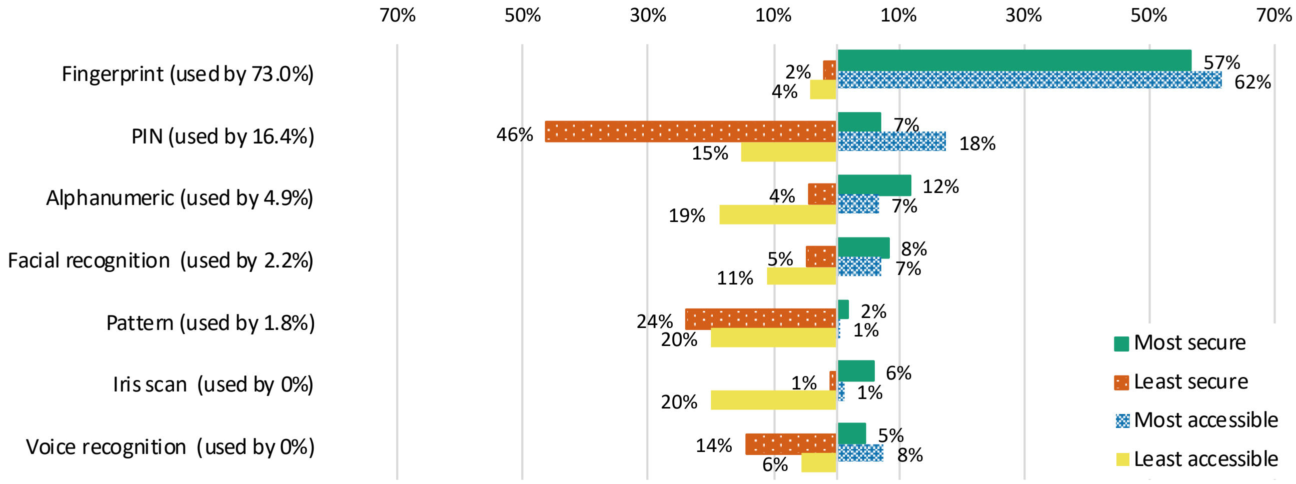

Figure 8: Participants most used selections of most secure (green), most accessible (blue), least secure (red), and least accessible (yellow) user authentication methods.

AUTHENTICATION METHODS IN MOBILE DEVICES

This section presents information on the security and accessibility of mobile authentication methods. Seven participants chose the same method as both the least and the most secure method, probably because they did not notice the questions were different. We removed their answers from the counting of least secure method, which came second.

Fingerprint: Most Secure and Accessible Method

We asked participants to choose which of the currently available user authentication methods they considered the most secure to unlock smartphones. The majority (N=184) selected fingerprint reader as the most secure, followed by alphanumeric passwords, and facial recognition (Figure 8). Participants who chose fingerprints did so because they are unique to everyone (36.9%), or impossible/difficult to duplicate (17.4%). Others considered it the most secure method due to its robustness (9.2%), and some mentioned vulnerabilities of other methods when compared to fingerprints (9.2%). Also, some participants mentioned its convenience with not having to memorize a password (N=4).

Interestingly, some participants (14.1%) said they chose fingerprint reader as the most secure method by mentioning accessibility issues that other authentication methods have. The user authentication method most questioned by participants was iris or retina scan, first because of the absence of eyes in some people who are blind (as suggested by Lazar et al. [22]), and second because of the difficulty of keeping the eyes in position to be scanned for people with vision impairment. Also, some participants (11.9%) commented on security issues with other biometric methods, including facial recognition that could be tricked by pointing the smartphone to the owner's face to obtain access, voice recognition that could be confused by external sound, and iris or face recognition that could be tricked by a replica.

Consistently, participants also chose fingerprint as the most accessible method (Figure 8). P176 summarized the main reasons of fingerprint's accessibility: *"Fingerprint: It is efficient, it does not require a blind person to be able to hear every letter they enter or have a Braille display as in pins or alphanumeric passwords, it does not require one to look in a specific direction to be secure such as with facial recognition or perhaps an iris scan, and one who really doesn't have the capability to visualize does not need to try to remember shapes such as in drawing a pattern."*

A few participants mentioned that fingerprints, although the quickest and most accessible method, does not give enough time for the person who have vision impairment to adjust the finger on the scanner, resulting in false negative authentication. Still, as biometrics such as fingerprints are faster than PINs, they are also considered more accessible: *"I think facial recognition or fingerprint identification are probably the most efficient right now. Entering a PIN is just as accessible as those but not as fast"* (P10).

Ten participants said accessibility depends on the target population: "*[There is no] one-size-fits-all answer. It depends on the users' experience. If they don't feel comfortable typing, [...] unlocking method [with] typing is out [...]. I think a security/convenience trade-off is definitely the fingerprint reader, which [...] is 'secure enough', and is accessible to most people. However, [it has] accessibility challenges; [...] such as for people with tremors"* (P229).

PINs: Least Secure Method

As the least secure method, most participants chose PINs (N=149), followed by pattern draw on the screen and voice recognition (Figure 8). From the 149 participants who selected PIN, most explained it was not secure because PINs are easy to guess (33.6%), and are more vulnerable to shoulder surf (30.2%) (as found by Haque et al. [20]). Others said PINs are easy to hack by computer programs (22.1%) and contain a small number of possible combinations. Fourteen participants said people generally choose simple PINs, which makes them easier to guess.

Table 1: Least accessible methods, for blind and low vision participants, ordered by the overall inaccessibility for both. Significant differences marked with *.

Method	Blind		Low vision	
	Ranking	***%***	***Ranking***	***%***
Pattern	1	24%	4	12%
Iris or retina scan	2	21%	3	18%
Alphanumeric	3	16%	1	25%
PIN	4	12%	2	23%
Facial recognition	5	11%	5	11%
Voice recognition	6	5%	6	6%
Fingerprint	7	5%	7	4%

Regarding shoulder surfing, P72 said, *"[PINs] could easily be remembered by someone who might see you entering it into a device. The thought of this happening at the ATM that I regularly visit is quite scary."* Also, some participants said they feel more secure with biometrics than PINs, such as P324 who said, "*if someone threatens me I'll have to give the password, my fingerprint no"*. Considering PINs are still the main authentication method, additional security measures such as a maximum number of attempts to try a PIN might be put in place to avoid risks, as mentioned by P146, *"A 4-digit pin can be guessed in a relatively short period of time, if no countermeasures in place."*

Among the participants who chose pattern as the least secure method, more than half of them said it is very easy for others to see the gestures drawn on the screen and replicate them afterwards. P103, for example, said, *"can be watched/copied easier, even with a so-called 'screen curtain' in place"*. Additionally, 14 participants said this method is difficult for them to use, due to its low accessibility.

Iris Scan and Patterns: Least Accessible Methods, but…

Tied in first place, the least accessible authentication methods are patterns drawn on the screen (20%) and iris or retina scan (20%), followed by alphanumeric password (18.8%), PIN (15.1%) and facial recognition (11.1%) (Figure 8). Iris or retina scan and facial recognition did not significantly differ between the two groups. However, patterns were significantly considered worse for accessibility for blind than for low vision participants (M=0.23 vs. M=0.12, t (323) = 2.42, p <.01). As P102 puts it *"this relies on being able to connect specific points of your screen, and it doesn't take much for a blind person to miss a spot"*.

On the contrary, both alphanumeric password and PIN were significantly worse for low vision than blind participants (M=0.25 vs. M=0.16, t (323) = 1.92, p <.05; and M=0.23 vs. M=0.12), t (323) = 2.68, p <.01). For people with low vision, alphanumeric passwords require effort to remember *"long strings"* (P182) and *"take longer to enter and therefore the device cannot be unlocked as quickly"* (P217), because *"it involves jumping from screen to screen"* (P13).

Summary

Fingerprint reader is considered the most secure and most accessible method for people who are blind or have low vision, as fingerprints are unique for everyone, and are quick and easy for people with vision impairment to use. The least accessible methods differed between the two groups. Pattern and iris or retina scan were the two least accessible methods for the blind, while alphanumeric password and PIN were the two least accessible methods for the low vision participants. Table 1 summarizes the differences between the two vision impairment groups by ranking the least accessible methods.

USE OF SMARTPHONES AND AUTHENTICATION

This section presents participants' use of smartphones and authentication methods, and reasons for not using authentication. We asked those questions at the end of the survey to avoid influencing their earlier answers on accessibility and security, as they might have considered only methods available in their own phones in their answers.

Mobile Devices Owned

296 respondents reported owning a smartphone (91%), for a median of 6 years (M = 10). The number of years owning a smartphone was not different between participants who are blind and those who have low vision. From the 296, 75.3% said they use an authentication method to protect their devices. These participants were balanced between the two groups. However, younger participants were more likely to have a user authentication method than older ones (M=43.2 vs. M=51.2, t (294) = 3.87, p <.001).

Similarly to what was found by Leporini et al. [23] and Ye et al. [38], iOS (Apple) was the most used operating system (OS) by people with vision impairment (80.4%). 16.9% used Android, 2.4% used a Windows device and one person used another OS. The operating system used differ between groups (χ^2 (3, N=296) = 27.92, p <.001), as blind were more likely to use iPhones than those who have low vision. We found iOS users were more likely to use a user authentication method in their smartphones (81.5% vs. 71.4% of Windows users and 62% of Android users, not significant (*n.s.)*).

Choice of User Authentication Method

When selecting an authentication method, most smartphone users use fingerprints (73%) (Figure 8). As with the selection of most secure method, blind participants more likely used fingerprint readers as their main user authentication method (75%) when compared to participants with low vision (68%), who were slightly more likely to use PINs (21% vs 15%, *n.s.*). The median PIN was 4 digits (M=5.3) and the median alphanumeric passwords had 12 characters (M=15.8).

From 165 participants who use fingerprints, the most mentioned reasons for using it are: its security (47.3%, e.g. against duplication and against aural eavesdropping), its quick unlocking process (43.6%), its easiness to use (38.8%, also noted by Dosono et al. [17]). Other reasons include the convenience to use (14.5%), accuracy or reliability (9.1%), and the fact that is the alternative available (6.7%). However, some participants seem not to notice methods can be broken in: *"harder to hack than numeric password, which I also use"*. (P35) and *"Quick, easy, don't have to remember the passcode, nearly impossible for others to access iPhone when locked."* (P212). From the 165 participants, 23.6% said they did not have reasons to dislike the method, while 67.3% mentioned having some inconvenience while unlocking their smartphones using their fingerprints, such as the fingerprint reader not recognizing them because of wet, recently dried or oily fingers (N=39) or cold fingers (N=20), malposition of the fingers (N=9) or when wearing gloves (N=7).

Participants who use PIN to unlock their smartphone (N=38) choose it because of its ease to use (N=10), availability (N=9), security (N=5), convenience (N=5), easiness to remember (N=4), and speed (N=4). Only two participants mentioned the accessibility of the method. P301 said, *"It is the best and most consistent method for me, given my tremors."* 18 mentioned they dislike the inconvenience of using it, as it is a repetitive method (N=4), slow (N=4), and requires them to remember another password (N=3). P83 mentioned having trouble with the audio feedback: *"When you press the number it does not always say, 'it is the correct number'. For example, when you press 2 it says 2 A B C but when you press 1 it does not say anything"*. Also, 14 participants dislike the security provided by PINs, because they can be shoulder surfed (N=5), guessed (N=4), or heard by others when read by screen readers (N=3).

Reason for Not Using an Authentication Method

A quarter of participants who own a smartphone did not use a user authentication method on it (24.7%). This number is slightly lower than what was found among sighted participants (24.7% vs 28% [30]), but the choice of protecting the smartphones did not differ between the two groups. These participants indicated not having personal information stored in the smartphone (N=13), not considering necessary to have a method (N=12), not wanting to slow down the access to the phone (N=8), complexity of methods (N=7), annoyance of methods (N=7), and considering the smartphone protected because it is kept close by (N=7). P16 said, *"I don't want to be bothered with it, and if my phone were stolen, I'd just call the company and have it disabled."* Another participant mentioned *"I don't know how to do that, and I do not know anybody who does"* (P126), what enforces the importance of adequate training.

Other Comments

Two interesting issues reported by participants relate to applications to track lost devices and CAPTCHAs. P296 said: *"the location of the device may be shown on a map. I feel that there should be an address given in a text form, which would make the locating and finding the device that much easier."* In an Apple device, for example, it is indeed possible to get the address where a device is located, but the process requires accessing two other screens by tapping small buttons. P46 said: *"I hate the password confirmation methods on sites that require one to type in the secret confirmation code which is normally a graphic and inaccessible! [...] What about if you are not sighted? Grrr."*

Some participants mentioned being supportive about the survey. However, P131 was skeptical about it: *"Interesting survey, but I can't see the use. Tech will progress and is driven by the needs of those who are sighted."*

Summary

We found that 91% of survey participants own a smartphone, and 75.3% of those protect their smartphones with a user authentication method. Most of them use fingerprint for unlocking their devices because they consider this method secure and fast. Among the participants who did not use a user authentication method to unlock their devices, their reasons include not storing personal information in their smartphones and considering it unnecessary.

DISCUSSION AND FUTURE WORK

Our results represent the mobile password use and perceptions on security of 325 people with vision impairment. We found that participants self-assessed ability to protect their digital information is related to the importance they give to passwords, that fingerprint is considered the most secure and most accessible authentication method, and that three quarters of those who own smartphones protect them with authentication methods.

Survey Participants

Before discussing our results further, it is important to address the pool of participants who answered this survey. By the nature of an online survey, our sample had to have access to the internet and most likely have an email, as this is how the survey was mainly distributed. In addition, while it is estimated that there are six times more people with low vision than blind people in the world [12], almost 70% of our participants were blind, similar to an online survey by Azenkot and Lee [6], in which 84% of participants were blind. In our case, this distribution might be a function of our recruiting method targeted to organizations providing support to people with vision impairment, which might also count with more blind clients. Our results may not reflect the full experience of people with low vision.

Broad Smartphone Use

More people with vision impairment owned a smartphone (91%) than sighted people (77%) [30]. This may relate to the importance smartphones have for people with vision impairment *"for everyday tasks"* (P217) and to access assistive apps (used by 73% of the blind), though we acknowledge again that these numbers might be related to our survey recruitment method and focus. Either way, it is important to consider the specific needs of people with vision impairment when designing mobile solutions.

Importance of Passwords

Our results show that people with vision impairment are aware of the importance of protecting their personal information and privacy, including knowledge about the risks of breaches. They also have a strong digital presence, which supports the importance of accessible websites for both companies and governments. Solving accessibility issues, including those related to CAPTCHAs, will allow people with vision impairment to fully use those websites.

Ability to Keep Data Secure

Most participants felt able or very able to protect their digital information, so we reject our first hypothesis (**H_1**). In addition, participants who attributed a higher importance to passwords also felt more confident about their own ability to protect their data. The use of password managers was also associated with higher levels of confidence. Additionally, we found that shoulder surfing was the main concern among blind and low vision participants, as in previous research [2].

However, we recognize that both the questions about password importance and perceived ability to protect digital information, the scale containing "able" and "very able" and "important" and "very important" might have confused participants. Similarly, the use of "not able" and "not at all able" might have conflicted participants when responding.

Secure and Accessible Authentication Methods

The proportion of survey participants who declared to use user authentication methods to protect their personal devices was higher than in previous research (75.3% vs 33.3% and 0%) [7, 17]. This might be related to the fact that three and six years, respectively, separates the previous studies from our research. In this time, information about digital security may have become more accessible and widespread. Another explanation may relate to the selection of participants in our survey, who might be more knowledgeable about digital security and risks of not securing their personal information.

Most participants chose fingerprints as the most secure and accessible method to unlock mobile devices, because it is fast to authenticate and easy to use, confirming our second hypothesis (**H_2**). In addition, most participants rely on fingerprints to unlock their devices, because they are fast (when it works) and do not force them to repetitively type PINs. They also considered PINs the least secure method. However, they seem to neglect that PINs are still their main barrier against unauthorized access to their phones, possibly implying they use easier to guess PINs. Only P216 seemed to recognize that by saying, *"I'm not sure if a fingerprint is much safer if someone can still figure out the numeric passcode number."* The main advantage of having a fingerprint set up is avoiding (most of the time) to type a password that might be seen by others. However, fingerprint and other biometric authentication methods are not more secure than typing a PIN, as they have PINs as an alternative.

We also found that a third of the participants, who did not have a method to protect their mobile devices (22 out of 67), said their reasons lie on the complexity and inconvenience of the existing user authentication methods. An alternative is developing special methods, as mentioned by P119: "*Any method that was developed to be accessible for the blind.*"

Blind vs Low Vision

Most behaviours and preferences were equal between participants who were blind and those with low vision, such as online presence, use of smartphones, authentication method used, and opinion on the most secure and accessible method. However, we found some differences in opinion on authentication methods between the two groups, rejecting our third hypothesis (**H_3**): Blind people considered patterns and iris scans the least accessible methods, because they require some level of visual interaction; while people with low vision selected alphanumeric passwords and PINs, possibly due to difficulty of typing using a screen magnifier.

Final Message

Our results provide insights on accessibility issues faced by people who are blind and people with low vision when using different user authentication methods. We hope readers will consider the needs of both groups, as well as their perceptions and technology use when creating new and more accessible user authentication methods.

Limitations

This was a self-conducted survey and its findings may change with time due to improvements in existing user authentication methods and the rise of new ones. To avoid participants changing their answers based on later questions, we did not provide a previous button. In addition, while we tried to ensure that the survey was accessible, two participants contacted us due to issues with the platform Qualtrics when using the screen reader Jaws on Windows. Upon investigation, we found that Qualtrics does not work properly with older versions of Internet Explorer, Firefox or Google Chrome, which might have prevented participation.

CONCLUSION

We conducted an online survey with people who are blind or have low vision to understand their strategies to remember passwords, their perceptions on user authentication methods and their self-assessed ability to keep their digital information safe. We found that most use familiar names and numbers to memorize their passwords, that the majority consider fingerprints to be the most secure and most accessible user authentication methods, and that PIN was considered the least secure user authentication method. We also found that blind people considered patterns and iris scans the least accessible methods, while people with low vision selected alphanumeric passwords and PINs. This shows us a truly accessible solution for vision-impaired people should not require precise manipulation of visual items, the use of the users' eyes or the use of keyboards with screen magnifiers.

Future work will include the investigation of alternative authentication methods and their potential for people with vision impairment. For instance, researchers have created tactile methods for unlocking devices, such as Haptic Keypad [10], BoD Shapes [24] and Bend Passwords [25]. These devices have yet to be explored for vision-impaired people, who could benefit from this technology.

ACKNOWLEDGMENTS

This work was supported and funded by the National Sciences and Engineering Research Council of Canada (NSERC) through a Discovery grant (2017-06300) and the *Collaborative Learning in Usability Experiences* Create grant (465639-2015). We thank Kim Kilpatrick and Nolan Jenikov from the Canadian Council of the Blind in Ottawa for their great help. We also thank Dr. Jonathan Lazar for providing useful comments on the initial version of this paper.

REFERENCES

[1] Accessible Writing Guide: 2015. *http://www.sigaccess.org/welcome-to-sigaccess/resources/accessible-writing-guide/*. Accessed: 2018-03-12.

[2] Ahmed, T., Shaffer, P., Connelly, K., Crandall, D., Kapadia, A., Ahmed, T. and Connelly, K. 2016. Addressing Physical Safety , Security , and Privacy for People with Visual Impairments. *Proceeding of the Twelfth Symposium on Usable Privacy and Security (SOUPS)*. (2016), 341–354.

[3] Andreas Kleynhans, S. and Fourie, I. 2014. Ensuring accessibility of electronic information resources for visually impaired people. *Library Hi Tech*. 32, 2 (2014), 368–379. DOI:https://doi.org/10.1108/LHT-11-2013-0148.

[4] Aviv, A.J., Budzitowski, D. and Kuber, R. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. *Proceedings of the 31st Annual Computer Security Applications Conference on - ACSAC*. (2015), 301–310. DOI:https://doi.org/10.1145/2818000.2818014.

[5] Aviv, A.J., Davin, J.T., Wolf, F. and Kuber, R. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. *Proceedings of the 33rd Annual Computer Security Applications Conference on - ACSAC*. (2017), 486–498. DOI:https://doi.org/10.1145/3134600.3134609.

[6] Azenkot, S. and Lee, N.B. 2013. Exploring the use of speech input by blind people on mobile devices. *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility* (2013), 1–8.

[7] Azenkot, S. and Rector, K. 2012. Passchords: secure multi-touch authentication for blind people. *Assets '12 Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*. (2012), 159–166. DOI:https://doi.org/10.1145/2384916.2384945.

[8] Balaji, V. 2017. Towards Accessible Mobile Pattern Authentication for Persons With Visual Impairments. (2017).

[9] Barbosa, N.M., Hayes, J. and Wang, Y. 2016. UniPass: design and evaluation of a smart device-based password manager for visually impaired users. *UbiComp*. (2016), 49–60. DOI:https://doi.org/10.1145/2971648.2971722.

[10] Bianchi, A., Oakley, I. and Kwon, D.S. 2010. The secure haptic keypad: a tactile password system. *In Proceedings of the 28th international conference on Human factors in computing systems*. (2010), 1089–1092. DOI:https://doi.org/http://doi.acm.org/10.1145/1753326.1753488.

[11] Bose, P.K. and Kabir, M.J. 2017. Fingerprint: A Unique and Reliable Method for Identification. *Journal of Enam Medical College*. 7, 1 (2017), 29–34.

[12] Bourne, R.R.A. et al. 2018. Magnitude, temporal trends, and projections of the global prevalence of blindness and distance and near vision impairment: a systematic review and meta-analysis. *The Lancet Global Health*. 5, 9 (Feb. 2018), e888–e897. DOI:https://doi.org/10.1016/S2214-109X(17)30293-0.

[13] Cassidy, B., Cockton, G. and Coventry, L. 2013. A haptic ATM interface to assist visually impaired users. *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility - ASSETS '13*. (2013), 1–8. DOI:https://doi.org/10.1145/2513383.2513433.

[14] Csapó, Á., Wersényi, G., Nagy, H. and Stockman, T. 2015. A survey of assistive technologies and applications for blind users on mobile platforms: a review and foundation for research. *Journal on Multimodal User Interfaces*. 9, 4 (2015), 275–286. DOI:https://doi.org/10.1007/s12193-015-0182-7.

[15] D'silva, C., Parthasarathy, V. and Rao, S.N. 2016. Wireless Smartphone Keyboard for Visually Challenged Users. *Proceedings of the 2016 Workshop on Wearable Systems and Applications - WearSys '16*. (2016), 13–17. DOI:https://doi.org/10.1145/2935643.2935648.

[16] Diseases: 2018. *https://www.canada.ca/en/public-health/services/diseases.html*. Accessed: 2017-02-21.

[17] Dosono, B., Hayes, J. and Wang, Y. 2015. " I'm Stuck !": A Contextual Inquiry of People with Visual Impairments in Authentication. *Proceedings of the eleventh Symposium On Usable Privacy and Security*. (2015), 151–168.

[18] Equifax's Enormous Data Breach Just Got Even Bigger: 2018. *https://www.forbes.com/sites/nickclements/2018/03/*

05/equifaxs-enormous-data-breach-just-got-even-bigger/#fb62c5753bc5. Accessed: 2018-03-26.

[19] Gateway to Health Communication & Social Marketing Practice: 2017. *https://www.cdc.gov/healthcommunication/toolstemplates/entertainmented/tips/Blindness.html*. Accessed: 2018-02-20.

[20] Haque, M.M., Zawoad, S. and Hasan, R. 2013. Secure Techniques and Methods for Authenticating Visually Impaired Mobile Phone Users. *IEEE International Conference on Technologies for Homeland Security (Hst)*. (2013), 735–740.

[21] Kaczmirek, L. and Wolff, K. 2007. Survey Design for Visually Impaired and Blind People. *Universal Acess in Human Computer Interaction. Coping with Diversity*. 4554, (2007), 374–381. DOI:https://doi.org/10.1007/978-3-540-73279-2_41.

[22] Lazar, J., Wentz, B. and Winckler, M. 2017. Information Privacy and Security as a Human Right for People with Disabilities. *Disability, Human Rights, and Information Technology*. J. Lazar and M. Stein, eds. University of Pennsylvania Press. 199–211.

[23] Leporini, B., Buzzi, M.C. and Buzzi, M. 2012. Interacting with Mobile Devices via VoiceOver : Usability and Accessibility Issues. *Proceedings of the 24th Australian Computer-Human Interaction Conference*. (2012), 339–348. DOI:https://doi.org/10.1145/2414536.2414591.

[24] De Luca, A., von Zezschwitz, E., Nguyen, N.D.H., Maurer, M.-E., Rubegni, E., Scipioni, M.P. and Langheinrich, M. 2013. Back-of-device authentication on smartphones. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. (2013), 2389. DOI:https://doi.org/10.1145/2470654.2481330.

[25] Maqsood, S., Chiasson, S. and Girouard, A. 2016. Bend Passwords: using gestures to authenticate on flexible devices. *Personal and Ubiquitous Computing*. 20, 4 (2016), 573–600. DOI:https://doi.org/10.1007/s00779-016-0928-6.

[26] More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018: 2017. *https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/*. Accessed: 2017-02-01.

[27] NVivo: *http://www.qsrinternational.com/nvivo/nvivo-products/nvivo-for-mac*.

[28] Qualtrics: *https://www.qualtrics.com*.

[29] R Studio: 2016. *https://www.rstudio.com*.

[30] Rainie, L. and Perrin, A. 2017. 10 facts about smartphones as the iPhone turns 10. *Pew Research Center*.

[31] Sauer, G., Holman, J., Lazar, J., Hochheiser, H. and Feng, J. 2010. Accessible privacy and security: A universally usable human-interaction proof tool. *Universal Access in the Information Society*. 9, 3 (2010), 239–248. DOI:https://doi.org/10.1007/s10209-009-0171-2.

[32] Stobert, E. and Biddle, R. 2014. The password life cycle: User behaviour in managing passwords. *SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security*. (2014), 243–255.

[33] The Lighthouse National Survey on Vision Loss: Experience, Attitudes, and Knowledge of Middle-Aged and Older Americans: 1995. *http://li129-107.members.linode.com/research/archived-studies/national-survey/*. Accessed: 2018-03-20.

[34] Vision impairment and blindness: 2017. *www.who.int/mediacentre/factsheets/fs282/en/*. Accessed: 2017-12-20.

[35] Wash, R., Rader, E., Berman, R. and Wellmer, Z. 2016. Understanding Password Choices : How Frequently Entered Passwords Are Re-used across Websites. *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS)*. (2016), 175–188.

[36] Wolf, F., Kuber, R. and Aviv, A.J. 2018. An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication. *Behaviour & Information Technology*. 0, 0 (2018), 1–15. DOI:https://doi.org/10.1080/0144929X.2018.1436591.

[37] World Health Organisation 1980. *International Classification of impairments, disabilites and handicaps (ICIDH)*.

[38] Ye, H., Malu, M., Oh, U. and Findlater, L. 2014. Current and future mobile and wearable device use by people with visual impairments. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*. (2014), 3123–3132. DOI:https://doi.org/10.1145/2556288.2557085.