BEND PASSWORDS FOR PEOPLE WITH VISION IMPAIRMENT

by

Daniella Briotto Faustino

A thesis submitted to the
Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF APPLIED SCIENCES
in
Human Computer Interaction

at

Carleton University
Ottawa, Ontario

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 with 325 people who are blind or have low vision and found they are concerned about entering passwords in public because of the risk of others observing their passwords. We also found PINs, commonly required on smartphones, are considered insecure and poorly accessible. To solve those issues, we investigated the usability of bend passwords, a recently proposed method for authentication that uses a combination of pre-defined bend gestures performed on a flexible device. We designed a new deformable prototype and ran a user study with 16 vision-impaired participants, finding that bend passwords are as easy to learn and memorize as PINs, but are faster to enter than PINs.

Acknowledgments

First, I want to thank my wonderful supervisor, Dr. Audrey Girouard, who gave me the amazing opportunity to study with her, introduced me to the world of physical computing and prototyping and taught me to trust my research abilities.

Thank you to all my lab mates, who, together with my supervisor, provided timely feedback on my early ideas and different prototype iterations. My special thanks to Alex Eady and Victor Cheung, for their great support, and to Leona Lassak, who worked closely with me during the final prototype preparation and in the user study.

Another special thanks to Kim Kilpatrick, coordinator of the Get Together with Technology group at the Canadian Council of the Blind (CCB), for agreeing to help me with this project since the beginning. Thanks to both Kim and Nolan Jenikov, also from the CCB, for providing early feedback on the online survey and on various versions of the prototype. Their expertise was essential to assure our online survey and prototype were appropriate for testing with vision-impaired participants. I also thank Kim, for generously providing space for the user study at the CCB, a familiar space to participants that certainly facilitated their participation. Kim was also essential in recruiting participants for the user study, and I am really thankful for that.

I also thank Dr. Sonia Chiasson, for her great classes, support and advice on prior work on user authentication methods and security. I also want to thank her student Sana Maqsood, who kindly shared her experiences exploring her creation (bend passwords) with sighted participants.

Thank you Dominira Saul and Shaun Illingworth, for the great learning opportunities during my internship at Akendi, the User Experience certification training and for all their support. My thanks also to David Berman, for his inspiring talks on the importance of

accessibility and for kindly helping me with both accessibility tips and spreading the word about the user study.

Thanks to Gerry, Reham and Daniela, who contributed with thoughtful feedback about the user study. Thanks to all the user study participants, who accepted to participate in the two one-hour sessions and provided me with amazing insights. And also thanks to all online survey participants, who generously shared their thoughts about user authentication methods with me.

Finally, my most special thanks to my dear husband Werbeson, my source of strength and inspiration, who always cheers me up and supports me in all my endeavours: you know I love you more than anything!

Table of Contents

List of Tables

List of Figures

1 Chapter: Introduction

1.1 Motivation

Smartphones play an important role not only in the lives of sighted users, but also in the lives of vision-impaired users, because of their portability and the myriad of services they connect users to. For people with vision impairment, who are blind or have low vision, interacting with visual elements on smartphone touch screens became feasible thanks to the advent of smartphone accessibility features, such as screen readers VoiceOver from Apple Inc. [96] and TalkBack from Google [89]. As a matter of fact, smartphones now act as an assistive tools aggregator, giving users access to apps that help them identify bills [42], street names [24], colours [90], objects and faces [85], and read printed text [91].

However, by accessing and generating content on their smartphones, users leave tracks of identifiable personal information, which might represent a threat of identity fraud in case the smartphone is lost, stolen or used without the users' consent [50]. To protect smartphones from unauthorized access, smartphones come with various native user authentication methods, which users can activate so that the smartphone will ask for identity proof before giving access to its content. For example, smartphones can be configured to automatically lock once the screen is off and can be unlocked by the user via either typing a Personal Identification Number (PIN) or scanning their fingerprint.

User authentication methods such as passwords help people avoid unauthorized access to their personal devices but are not without challenges, like memorability and shoulder surfing attacks, in which "attackers learn a password by observing users enter it in a public space" [67]. Previous research shows people with vision impairment are concerned

with entering passwords in public because screen readers and screen magnifiers make their passwords more vulnerable to attackers [5]. Nevertheless, other research indicates that the majority of people with vision impairment choose not to protect their smartphones against unauthorized access [16, 37]. In fact, little is known about how people with vision impairment currently assure their digital security in mobile contexts or how they perceive and use different user authentication methods.

Due to the importance of user authentication methods to protect users' personal information, researchers have been exploring the topic of usable security, generally focusing on a combination of the following aspects:

1. Reducing the cognitive load required for users to remember passwords.
2. Increasing security against guessing or shoulder surfing attacks.
3. Exploring new interaction techniques.
4. Improving accessibility.

For example, Azenkot et al. [14] proposed a user authentication method based on recognizing the fingers the user uses to tap a pattern on the screen. Their method aimed to be memorable (aspect 1), secure against guessing and shoulder surfing attacks (aspect 2), and accessible for blind people (aspect 4).

As another example, Maqsood et al. [68] developed a novel user authentication method on deformable flexible devices, by using a pattern of bend gestures called a bend password. Deformable flexible devices are devices made of flexible materials, which can accept deformation such as bending the corners as an input method. By using a prototype made of vinyl with embedded flex sensors, the researchers investigated the memorability (aspect 1) and security against shoulder surfing attacks (aspect 2) of their new password input method (aspect 3). One of the motivations for this study was the advancement in the development of flexible displays, which may be available in the near future, pushed by companies like Samsung [82]. When flexible displays are available, bend passwords could

potentially benefit people with vision impairment, because of their tactile nature and their positive results in terms of security and memorability [68]. However, this user authentication method has yet to be evaluated with people with vision impairment.

Considering that research at the intersection of usability, security and accessibility is rare [83] and needs further investigation [60], this thesis's objectives are two-fold:

1. investigate how people with vision impairment deal with passwords in a mobile context and
2. explore the use of bend passwords on a deformable device as a password input method for people with vision impairment.

1.2 Research Question

The main research question guiding this research project is:

- What is the potential of bend gestures as a method of user authentication on mobile devices for people with vision impairment?

To address this research question, we started by collecting data about how people with vision impairment protect their digital information in a mobile context, the accessibility issues they face and how they perceive existing user authentication methods. We specifically aimed at identifying how people with vision impairment evaluate the security of the ubiquitous PINs, and whether there was a difference in preference for user authentication methods on smartphones between people who are blind and people who have low vision.

Taking into account the results from the online survey, we developed a new deformable flexible prototype able to capture a sequence of bend gestures composing a bend password, similar to what was done in prior work [68]. Finally, we ran a user study with people who are blind or have low vision to evaluate the learnability and memorability of bend passwords in comparison with PINs. By running this user study, we determined how bend passwords are perceived by people with vision impairment and whether they have potential as an alternative user authentication method.

1.3 Contributions

To the best of our knowledge, our online survey constitutes the first study to extensively explore the relationship people with vision impairment have with passwords and user authentication methods on mobile devices. Through an analysis of the answers from 325 vision-impaired respondents, the contributions of the survey 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.

Additionally, our user study is the first to explore the use of bend gestures on deformable devices as a password input method for people with vision impairment, resulting in the following contributions:

4. The design and fabrication of a new deformable prototype for password input specially developed for people with vision impairment;
5. Insights on how easy to learn and how easy to memorize bend passwords are for people with vision impairment;
6. Potential applications for bend passwords;
7. Design recommendations for new deformable devices.

1.4 Thesis Outline

This thesis is organized into six chapters. In Chapter 2, we present a literature review on accessibility for people with vision impairment, user authentication methods and deformable flexible devices. In Chapter 3, we describe the online survey we conducted with people with vision impairment about their strategies to remember passwords, their perceptions on user authentication methods and their self-assessed ability to keep their digital information safe. In Chapter 4, we present the design and fabrication of a new deformable flexible prototype for password input, the preparation of a touch screen PIN entry system and the development of a website to capture and verify passwords. In Chapter 5, we describe the methodology and results from our user study with people with vision impairment, comparing bend passwords and PINs. In Chapter 6, we propose design recommendations for deformable devices for password input and finally we present our conclusion in Chapter 7.

1.5 Associated Publications

Portions of this work have been accepted for publication:

- Briotto Faustino, D. 2018, Understanding Password Use by People with Vision Impairment: Initial Results of a Survey. ACM Student Research Competition at the 2018 Grace Hopper Celebration (2018), (3-page paper to appear, poster).
- Briotto Faustino, D. and Girouard, A. 2018. Understanding Authentication Method Use on Mobile Devices by People with Vision Impairment. ACM SIGACCESS conference on Computers and accessibility (2018), (10-page paper to appear).
- Briotto Faustino, D. and Girouard, A. 2018. Bend Passwords on BendyPass: A User Authentication Method for People with Vision Impairment. ACM SIGACCESS conference on Computers and accessibility (2018), (2-page paper to appear, demo).

2 Chapter: Background

This thesis explores the intersection of usability, security and accessibility for people with vision impairment. In this chapter, we review prior work on accessibility, security on mobile devices and deformable devices.

2.1 Accessibility

Before reviewing prior work on accessibility for people with vision impairment, we discuss terminology related to vision impairment. Following, we review the use of smartphones by people with vision impairment and we list some accessibility issues on smartphones. This section finishes with an overview of privacy concerns related to the use of smartphones for vision-impaired people.

2.1.1 Terminology Regarding Vision Impairment

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 [92]. The current classification from the World Health Organization (WHO) includes normal vision, moderate vision impairment, severe vision impairment and blindness [95]. Still according to the WHO, low vision is the term used to refer to moderate or severe vision impairment. The term vision impairment is also used by the Center for Disease Control and Prevention [45] and the Government of Canada [36] to refer to the group composed of blindness and low vision.

However, Kleynhans et al. [8] caution that the terms visually impaired, partially sighted and low vision are used interchangeably in the literature to indicate residual vision. Due to the differences in the interpretation of terms referring to vision impairment, Cavender et al. [2] suggested clarifying if a person referred to as “blind” is someone who uses screen readers to access a computer, for example.

In 2012, the WHO issued a report estimating the “number of people visually impaired in the world is 285 million, 39 million blind and 246 million having low vision.” According to Bourne et al. [26], “in 2015, an estimated 36 million people were blind, 217 million were moderately or severely vision impaired, and 188 million had mild vision impairment.” To function more independently, people with vision impairment commonly use assistive technology devices, which can be defined as “any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities” [11]. For example, screen magnifiers and refreshable Braille displays are assistive technology devices, or simply assistive devices.

2.1.2 Smartphone Use by People with Vision Impairment

A survey conducted in Germany with 235 vision-impaired participants published in 2007, identified that 81.5% of them did not have access to the internet [54]. However, in the same year it was estimated that 74% of sighted people in the US used the internet [7]. From 2005 to 2017, the proportion of people with access to the internet increased from 35.9% to 65.9% on the American continent, and from 46.3% to 79.6% on the European continent [47].

In 2008, a US study reported each of their 8 blind participants used an average of 3.6 mobile devices, including laptops, mobile phones and PDAs [55]. But in the last few years, smartphones have become widely adopted not only by sighted individuals, but also by

individuals with vision impairment, thanks to the rise of accessibility features and assistive applications in mainstream devices [34, 50]. This adoption has improved the quality of life among people with vision impairment by giving them access to all sorts of information [6], while replacing a number of specialized assistive devices they had to resort to in the past. People who are blind or have low vision now use smartphones to complete a variety of activities such as making phone calls, sending and receiving text messages and emails, reading the news, navigating the internet, doing online shopping and banking, and accessing entertainment content and government services [62, 103]. Even those who still do not have smartphones believe new services should become available on the smartphone platform [78].

Depending on the degree of vision impairment, a person might use different accessibility features to interact with smartphones. People who have low vision can use screen magnifiers embedded in smartphones to zoom into particular screen areas, using a movable magnifying box on the screen for better visibility. On the other hand, people who are blind can interact with a touch-screen smartphone by using a screen reader, such as VoiceOver [96] in iOS devices and TalkBack [89] in Android devices, to hear both the name of screen elements and text read aloud [15]. People with vision impairment can also opt to use virtual Braille keyboards [53] or physical Braille keyboards connected to the smartphone via Bluetooth [27, 52].

To operate the screen reader, both iOS and Android smartphones have a set of shortcut gestures available. Android smartphones come with 12 possible gestures, to be performed mainly with one finger tapping or swiping, while iOS smartphones have more than 20 available gestures, using from one to four fingers in single, double or even triple taps [31]. Although iOS requires the use of potentially complex interactions, previous research showed iPhones are the most commonly used smartphones among people with vision impairment [62, 103].

2.1.3 Accessibility Issues on Smartphones

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 [35]. Interacting with smartphones is often complex for people with vision impairment, as they need to reproduce precise touch screen gestures, even though accuracy in reproducing gestures is challenging for those who lost their vision early in life [31]. Prior work found that people who are blind face usability issues while interacting with touch-screen devices, including learning where objects are located and accidentally activating features on the touch screen [55]. In addition, the sequence in which elements are read by the screen readers is cumbersome [62] and users cannot easily identify if protection screen mode[1] is on [103].

Screen readers have various usability issues. Blind individuals use them by touching the smartphone touch screen and hearing the names of the UI elements available until they find the element they are looking for. Then, they select it by double tapping the screen, through a slow and error-prone process [15]. The interaction is also hindered by inconsistent focus on UI elements and conflicting operating system and app controls [62], as some apps do not conform with the smartphone OS guidelines [34]. Additionally, interacting with screen readers requires users to perform complex multi-finger interactions and precise gestures, without having any tactile feedback [39].

Entering data on smartphones is particularly challenging for people with vision impairment, not only because of the small size of virtual keyboards, but also because of the complexity of text editing [30, 62]. Using virtual keyboards with screen readers requires

[1] This accessibility feature is called *Screen Curtain* on iOS, and *Dark Screen* on Android.

users to explore the touch screen to find the keys they want to press, while trying to avoid activating alternative keyboards by accident and without being able to use predictive words, which are not accessible to them [6]. Similarly, the text editing menu is activated by complex three-finger gestures [62], .

Most of the alternatives for text input also require two-hand use, an issue when the person needs to have a hand free for holding a guide dog's leash or a white cane [6]. Besides, even though voice commands are more popular among vision impaired than sighted smartphone users, blind individuals face challenges when trying to edit and review the text entered through speech input; a step usually accomplished by resorting to external physical keyboards [15].

In fact, a study with 114 vision-impaired participants found that almost half of them use a Bluetooth keyboard while using their smartphones [103], in addition to ubiquitous earphones for hearing screen-reader instructions in public spaces [4, 16, 103]. Nevertheless, as people who are blind or have low vision usually depend on having one hand free to employ a white cane or guide a service dog while walking, using a smartphone by itself is not an easy task [6, 103], much less using it with an additional keyboard.

Azenkot et al. [15] evaluated the use of speech recognition available on smartphones as the main interaction method for input, in replacement of virtual QWERTY keyboards. In their research with 65 people with vision impairment, they detected that speech input can be almost five times faster than the virtual QWERTY keyboard input, but error correction takes 80% of the text entry time and requires the use of a virtual keyboard. Other issues related to the use of speech recognition as a text input method include: risk of aural eavesdropping in public spaces [62], inaccuracy in noisy places [57] or inappropriateness for quiet public spaces [103].

Also using the hardware available in smartphones, researchers proposed the use of a Braille recognizer to identify touch gestures forming a six-dot Braille character on the

screen [6, 77]. Oliveira et al. [77] proposed the use of six large targets mapped to the corners and edges of the screen, to be touched using only one finger. They found their solution for text input was significantly less error-prone than the virtual keyboard with VoiceOver, but significantly slower. Evolving this concept, Alnfiai et al. [6] developed SingleTapBraille, in which the user could tap anywhere on the screen to create a six-dot characters and had special gestures for common functions (e.g., send email). After testing it with seven participants, researchers found SingleTapBraille was significantly faster and more accurate than the virtual keyboard entry. Currently, a similar function is available in Apple iPhones, called VoiceOver Braille keyboard [1], as shown in Figure 1.

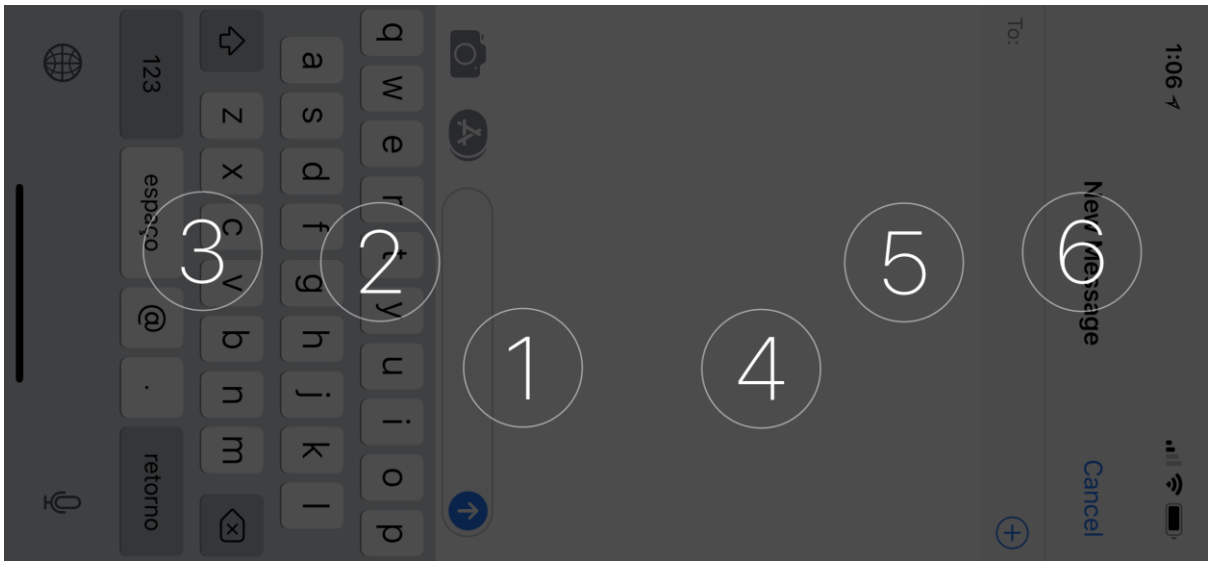

Figure 1: Screenshot taken on an iPhone showing VoiceOver Braille keyboard. The 6 keys represent each of the 6 dots that compose each Braille character.

Although study participants showed interest in Braille recognition software, Braille literacy is not widespread within the vision-impaired community. Among vision-impaired Americans and Canadians, fewer than 10% read Braille [23, 100] and among the British, less than 1% of the people with vision impairment can read Braille [28]. These numbers are similar to those found in a survey conducted by Ye et al. [103] with 67 vision-impaired people, where only 10% of participants mentioned Braille as a good output method.

Considering that entering text is a difficult task for people using screen readers, precisely typing in a password tends to be even more challenging. In a user study on password managers, a blind participant pointed out that the most difficult thing for him while accessing the internet via his smartphone was typing in a password [18].

2.1.4 Privacy Concerns for People With Vision Impairment

Though useful, smartphones brought new privacy concerns for their vision-impaired users. Reading emails and typing passwords are tasks they do not feel comfortable about doing in public places, feeling afraid of having their information stolen by shoulder surfers [5]. Typing PINs while using screen readers makes people with vision impairment more susceptible to others listening to their passwords (aural eavesdropping), as the system reads everything out loud, even password entries [50]. Similarly, the use of screen magnifiers by those with low vision also increases the susceptibility for visual eavesdropping [50].

As a coping strategy, most avoid performing those activities in public spaces, even keeping the phone out of sight [103]. Ahmed et al. [5] found that people with vision impairment tend to fear using smartphones in public and being targeted by thieves. In contrast, Ye et al. [103] found some people with vision impairment tend to feel safer when using their smartphones in public, because they can use it to call for help, should they need it.

By interviewing 19 people with vision impairment, researchers concluded that they have privacy and safety concerns which they cope with by avoiding situations and changing their behaviour whenever possible [5]. Study participants expressed interest in being able to know how many people are around them, whether they are close and what they are doing, in order to assess other people's intentions. This information was considered useful for the vision impaired to reposition themselves and avoid visual or aural eavesdropping.

The widespread use of smartphones resulted in a higher volume of personal data stored in those personal devices [68]. Understandably, many vision impaired said computers and smartphones are helpful to communicate and achieve personal independence, but also pose a challenge to safeguard all the personal information stored in them [4]. With more people with vision impairment relying more on smartphones, it is essential to assure their privacy and security protections [22].

2.2 Security

In this section, we present our literature review regarding user authentication methods, how people with vision impairment use them in various contexts and specifically on smartphones. We conclude this section by reviewing previous research on new user authentication methods.

2.2.1 User Authentication Methods

In 2016, 77% of sighted adults from the United States of America (US) said they own a smartphone, a large increase from 2011 when the percentage of smartphone owners was 35% [81]. With the increase in smartphone adoption, more personal data is stored in them, such as name, address, email and geolocation [60], and exchanged with third-party apps [9, 21, 49, 99]. To protect smartphones from unauthorized access (and consequently the personal information saved in them), users have to prove their identity through a user authentication method [68].

Many alternatives are available to protect mobile devices (e.g. smartphones) from unauthorized access, such as PINs, alphanumeric passwords, patterns drawn on the

screen, and biometric authentication, including fingerprint reader and face recognition [68]. According to Lazar et al. [60], user authentication methods can be categorized as:

- knowledge-based: something you know, such as PINs, alphanumeric passwords or patterns drawn on the screen;
- token-based: something you have, such as smart cards; and
- biometric-based: something you are, such as fingerprints, facial recognition, voice recognition, iris scans.

Besides being the most ubiquitous option, PINs are considerably more secure against random guessing than patterns. Even a 2-digit PIN is more secure than a pattern of dots connected by drawing on the screen, mainly because people tend to create very simple patterns [12], and patterns are more secure the longer their paths are [14]. Also, 6-digit PINs are considerably more secure against shoulder surfing attacks than 6-point patterns, after a single observation [12]. However, the commonly used 4-digit PIN is unable to provide a strong enough protection for smartphones [50] against random guessing and eavesdropping attacks.

Both PINs and alphanumeric passwords also require users to memorize a sequence of characters [68], a disadvantage when compared to biometric methods. According to Perez [48], in an era when passwords and PINs can be easily stolen by hackers, biometrics represents a better option to grant individual access. Fingerprints, for instance, are detailed and allow for a reliable identification of individuals [25]. However, fingerprints also have issues, such as high false rejection rates[2], caused by the derecognition of user's fingerprint during authentication, and the impossibility of replacing one's fingerprint in case the information is compromised [68]. Also, voice recognition suffers disruption from background

[2] False rejection rate is "the probability that a user's verification template will not be correctly matched with the same user's sample. Also known as false non-match rate." [48]

noises during identification and face recognition presents poor resistance to fraud [48]. Moreover, even though biometrics have been widely adopted due to their accuracy, evidence suggests that imposters can fake them [48]. In a survey conducted by Visa on using biometrics to authorize credit card operations, 49% of respondents feared the risk of security leaks [94].

Ultimately, biometrics do 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)" [13]. For a user, the complexity of choosing a user authentication method is worsened by the fact that methods that have high security have low usability and vice-versa [68].

2.2.2 Authentication Use for People With Vision Impairment

Based on a contextual enquiry with vision-impaired individuals, Dosono et al. [37] concluded that the "unique privacy and security needs of blind users remain largely unaddressed." They found that the lack of standardization of terminologies poses challenges to the users of screen readers, as different websites use different terms to name things. Moreover, the lack of appropriate feedback on an authentication attempt via password entry or fingerprint reader leaves users wondering whether they were able to successfully authenticate. Also, the absence of control for unmasking website password fields impede users from reviewing passwords when they are in a secure context (e.g. at home), as the system does not allow them to review the password once it is typed. On the other hand, security questions are not masked and are read aloud by screen readers. Researchers also found vision-impaired users have difficulty differentiating usernames and passwords [37], and face accessibility issues in authentication with Automated Teller Machines (ATMs) [33] and Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) [83].

Additionally, using screen readers in public spaces makes people with vision impairment more susceptible to aural eavesdropping, because the system reads out loud every character typed for a password or PIN. Similarly, the use of screen magnifiers by those with low-vision also increases the susceptibility for visual eavesdropping [50]. Unattended devices might be easily used to collect personal information after a password was identified by eavesdropping. A recent study with 14 participants found that half had concerns with having their interactions watched, and 6 were concerned with eavesdropping [74].

Ahmed et al. [4] found that, in order to prevent eavesdropping and keep their data secure, some people with vision impairment resort to typing rapidly and changing passwords every three months. They also tend to memorize long passwords by writing them down in Braille or saving them in the browser's password management feature, even though some struggle with using password management systems due to their impairment. This explains why some choose to save their passwords in computer files and then use screen reader software to read them aloud, creating additional risk of aural eavesdropping [4].

Prior work also suggests that vision-impaired people consider using strong passwords as the most effective protective action, but also tend to consider using unique passwords, and multi-factor authentication as effective practices [74]. However, that study found that only 4 out of 14 participants use passwords that contain a mix of letters, cases, numbers and symbols.

As little is currently known about how people with vision impairment assure their digital security in their smartphones, our research will start by an online survey with people who are blind or have low vision about their security habits and perceptions.

2.2.3 Authentication Use on Smartphones by People With Vision Impairment

In research published in 2017, the options most commonly used by sighted Americans to unlock their smartphones were PINs (26%), fingerprint (23%), passwords (9%), and patterns (9%) [81]. Though, the researchers found that 28% of the participants did not use any method to lock their screens and avoid unauthorized access.

Ahmed et al. [5] reported that most people with vision impairment feel uncomfortable to use passwords in public contexts for fear of eavesdropping and also that they have privacy concerns. However, 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 (mostly PINs) either inaccessible or inconvenient [16, 37]. Azenkot et al. [16] pointed out that most of their study participants were also unaware of potential security threats. One of the reasons given by people with vision impairment for not using any authentication method was that they keep their smartphone close to them at all times [16, 103], even though this practice does not assure the smartphone will be protected in case it is lost or stolen. Another reason mentioned by some participants was the inconvenience of unlocking the device using PINs [16], potentially due to the penalty in time [101].

Additionally, some user authentication methods currently available on smartphones might be problematic for people with vision impairment. For example, iris or retina scans might not work for people who have “deformed or missing eyes, or no ability to open their eyelids” [60]. Also, patterns drawn on the screen are poorly accessible for people with vision impairment, because they require the selection of points on the touch screen [17, 60].

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 for the help of others while completing required authentication procedures, possibly compromising their own security [60].

People with vision impairment are more vulnerable to shoulder surfing and aural eavesdropping when entering PINs [50]. However, even though other user authentication methods besides PINs 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.

2.2.4 Alternative User Authentication Methods

Prior work has considered the challenges faced by people with vision impairment when interacting with user authentication methods. Barbosa et al. [18] evaluated the accessibility of existing password managers for people with vision impairment, before designing and evaluating a new password management system. In their system, the user would log into a website on a computer by using his/her password stored in a smartphone. This caused confusion among participants, who were not sure whether they were logging in on the smartphone or logging in on the website by using the smartphone.

In another study, Haque et al. [50] proposed that each person's gait is unique and the pattern it forms could be used as an alternative authentication method for the vision impaired. They used accelerometer sensor data from smartphones to identify the user, requiring the user to walk 5 steps to allow the system to perform the authentication. While inexpensive, this method might present a burden for users willing to authenticate [50], but may also be imprecise due to potential changes in gait.

Azenkot et al. [16] proposed a knowledge-based user authentication method for touch-screen devices in which the user taps the screen with a set of fingers and each tap corresponds to a password character. In the method, users create a four-tap password using

15 possible finger combinations, making this password more secure against guessing than a 4-digit PIN, which has only 10 possible digits. After conducting an evaluation with 16 blind participants, the researchers found their method was three times faster than typing a 4-digit PIN using VoiceOver, while providing no audio feedback to avoid aural eavesdropping.

In a study focused on colour blind individuals, Balaji et al. [17] proposed a new pattern mechanism in which the users can choose both the colours and the pressure sensitivity of the touch screen. Although this method was considered easy to use by study participants, it does not solve the low security of the pattern method.

Other researchers have created tactile methods for unlocking devices, such as Haptic Keypad [19], Back-of-Device Authentication (BoD) Shapes [65] and Bend Passwords [68]. However, these devices have yet to be explored for people with vision impairment, who could benefit from this technology. We believe deformable devices, such as those proposed for bend password input, have potential for people with vision impairment, due to their tactile nature. Thus, next we review literature on deformable devices.

2.3 Deformable Devices

This section discusses what deformable devices are and refers to prior work on this area. Additionally, we present previous research on deformable devices for people with vision impairment and on a user authentication method using deformable devices.

2.3.1 Deformable Devices and Bend Gestures

Deformable devices are those that allow users to physically manipulate their shapes as a form of input, by bending, twisting or deforming them [3, 41]. The manual deformation forms a curvature on the device for the purpose of triggering a software action and it is generally

called a bend gesture [59]. Deformable devices support deformable user interfaces (DUIs) [87]. Similarly, “flexible display devices allow users to interact with the device by deforming the surface of the display to trigger a command” [70]. Commercial deformable devices are currently not available, but manufacturers seem to believe this is the future of smartphones [72].

The first computing device created to explore physical interaction techniques by accepting deformation as input was Gummi [84]. Gummi was made of flexible electronic components including sensors able to measure deformation. In their study, Schwesig et al. [84] evaluated the use of Gummi for zooming, blending and preview and found that participants were able to grasp Gummi’s basic interaction principles after a brief explanation spanning from 2 to 3 minutes.

Considering the novelty of DUIs, Warren et al. [97] proposed a classification method of bend gestures including location, direction, size and angle, to facilitate the communication about deformation as a method of interaction. After collecting 36 bend gestures performed by participants, they found location and direction are the easiest characteristics for users to differentiate.

Most research on deformation interactions considers the use of two hands. Girouard et al. [46] were the first to explore one handed bend interactions on deformable smartphones. They designed a prototype made of silicone and with the size similar to a smartphone, to be held in portrait orientation. They evaluated a series of bend gestures including bending corners and squeezing the centre and found that users preferred up gestures to down gestures and the corner closest to the thumb. The preference for top gestures was also a finding of other previous work [59, 64].

2.3.2 Deformable Devices for People With Vision Impairment

Considering deformation is a tactile form of input, and blind users solely rely on non-visual feedback, such as tactile cues and audio, Ernst et al. [41] proposed deformation could potentially benefit blind users. Ernst and Girouard [40] developed a deformable device the size of an iPhone 6 able to recognize bend gestures. Similar to Girouard et al. [46], their prototype was also made of silicone but had grooves indicating the areas where users could apply bend gestures on. The prototype's purpose was to control VoiceOver for navigation and selection of items. Before running a study with the device, Ernst [39] pondered that the drawback of gesture interactions is that they require users to memorize sets of movements to effectively interact with the device. He stated that the situation is "even more problematic for visually impaired users who are unable to watch instructional videos, see coach marks or onscreen visual affordances to help guide and learn new patterns and interaction techniques."

However, in a preliminary evaluation with two vision-impaired participants, Ernst and Girouard [40] found that bend gestures might be "easier out of the box than touch [interactions]", supporting the findings from Schwesig et al. [84], who found deformation gestures are quick to learn. Additionally, they found participants considered bend gestures a more tactile form of interaction, which could improve the accessibility of smartphones [41], and might be more forgiving for those who also have physical disabilities and hand tremors [40].

2.3.3 Bend Passwords

Maqsood et al. [68] designed and investigated the use of a sequence of deformations (bend gestures) as a user authentication method called bend password. They developed a flexible prototype made of a PVC sheet, with dimensions similar to those of a tablet, with 4 2-inch

Flexpoint bidirectional bend sensors located at the corners of the device. Their prototype allowed for bend gestures in two directions (upwards or downwards) and gestures could be performed in one or two corners at a time, for a total of 20 possible gestures. In their user study, sighted participants created both a PIN on a touch-screen smartphone and a bend password on the flexible prototype, returning a week later to verify if they could still remember their passwords. The researchers chose to use PINs in the comparison “because they are the most commonly used authentication mechanism on mobile devices” [67]. The researchers found that bend passwords are as easy to memorize as PINs, as “they have an advantage over PINs because they require a repetition of movements, which becomes an automatic and unconscious action, or part of what is called muscle memory” [66].

However, participants were concerned about the vulnerability of the bend passwords against shoulder surfing attacks. To address this concern, the researchers ran another study in which participants acted as attackers and tried to steal the password entered by the researcher both by typing a PIN in a touch-screen device and by bending the corners of a flexible device [67]. The results show bend passwords are as hard to shoulder surf as PINs, but as participants entered PINs on a QWERTY virtual keyboard harder to see than a numeric keypad, bend gestures might be actually harder to guess than PINs when entered on a regular number keypad.

Considering bend passwords are as easy to memorize but potentially harder to shoulder surf than PINs, and as bend passwords support a more tactile interaction technique, this thesis aims to explore bend passwords for people with vision impairment.

3 Chapter: Online Survey[3]

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.

3.1 Research Questions

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:

Q1. How do people with vision impairment self-assess their ability to keep their digital data secure?

Q2. Which user authentication method people with vision impairment consider more secure and accessible?

Q3. 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

[3] This chapter appears almost verbatim in the following publication: *Briotto Faustino, D. and Girouard, A. 2018. Understanding Authentication Method Use on Mobile Devices by People with Vision Impairment. ACM SIGACCESS conference on Computers and accessibility (2018).*

contributions of our findings 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 with low vision regarding their digital security opinions and behaviours.

3.2 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:

H1. 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 [16] and the difficulty to assess if others are shoulder surfing their passwords [5].

H2. People with vision impairment will choose fingerprints as the most secure authentication method due to its broad use [81]. 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 [73].

H3. 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.

3.2.1 Survey Design

We applied the guidelines proposed by Kaczmirek and Wolff [54] 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 defined the survey questions in English and then translated them into Portuguese. We posted the survey in both languages using the platform Qualtrics [79], 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 organized choices within the same question by avoiding two consecutive alternative 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 the English version with two human-computer interaction specialists and with two people who are blind, to evaluate the appropriateness of the questions, their sequencing to avoid introducing bias and the overall survey accessibility. Each blind person tested it using a different device, smartphone and computer, to identify accessibility issues or other problems that could impact completion or ease of use. We also tested the Portuguese version by reviewing terms with two other Portuguese speakers, one from Portugal and another from Brazil. We distributed the survey in both languages by email to more than 400 organizations that support people with vision

impairment in 31 countries (e.g. Lighthouse for the Visually Impaired and Blind, or the Canadian Council of the Blind). We also posted the study on the Carleton's Research Participants page on Facebook.

The survey was open for two and half months from December 2017 to February 2018, to maximize data collection. Participants who declared being vision impaired and at least 18 years-old qualified to participate. As a token of appreciation, we drew a $50 Amazon gift card for one participant at random. We obtained ethical clearance from the Carleton University Research Ethics Board (CUREB-B # 102815).

3.2.2 Terminology

In our survey, we opted to use the term vision impaired or people with vision impairment, in accordance with the World Health Organization (WHO) [95], the Center for Disease Control and Prevention [45] and the Government of Canada [36]. For the Portuguese version of the survey, we consider the Brazilian Government recommendation on how to refer to people with vision impairment [49]. We also considered the suggestion from Cavender et al. [2] on clarifying if a person referred to as "blind" uses a screen reader, by adding a question on which assistive technologies participants use.

3.2.3 Analysis of Results

One researcher performed a quantitative analysis of the multiple-choice answers using R Studio [80] and qualitative analysis of the text-entry answers using NVivo [76]. Quantitative analysis included chi-square tests (χ^2) of categorical data and t-tests (t) of numerical data, both with Bonferroni corrections, but we only report statistically significant results. We conducted the qualitative analysis using grounded theory [37], coding answers and consolidating codes within different themes that emerged for each question. Whenever

necessary, we coded answers in more than one theme, but we did not code unclear answers.

3.3 Participants

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

3.3.1 Demographics

We collected 350 answers from adults with vision impairment, 329 in English and 21 in Portuguese. After our quality control checks, including the evaluation of text-entry answers and the identification of duplicate answers, we discarded all answers from 25 participants, keeping answers from 325 participants. We translated all Portuguese answers into English before consolidating them in a unique file for analysis.

From our 325 participants, 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 [102], to consolidate the analysis into 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 (*Md*) =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 [102]. Other participants reported using a wheelchair, having motor or mental or developmental disabilities. Considering participants with other impairments were equally spread among the two groups (blind and low vision), we choose not to analyze their answers separately. Participants took a median time of 24 minutes to answer the online survey.

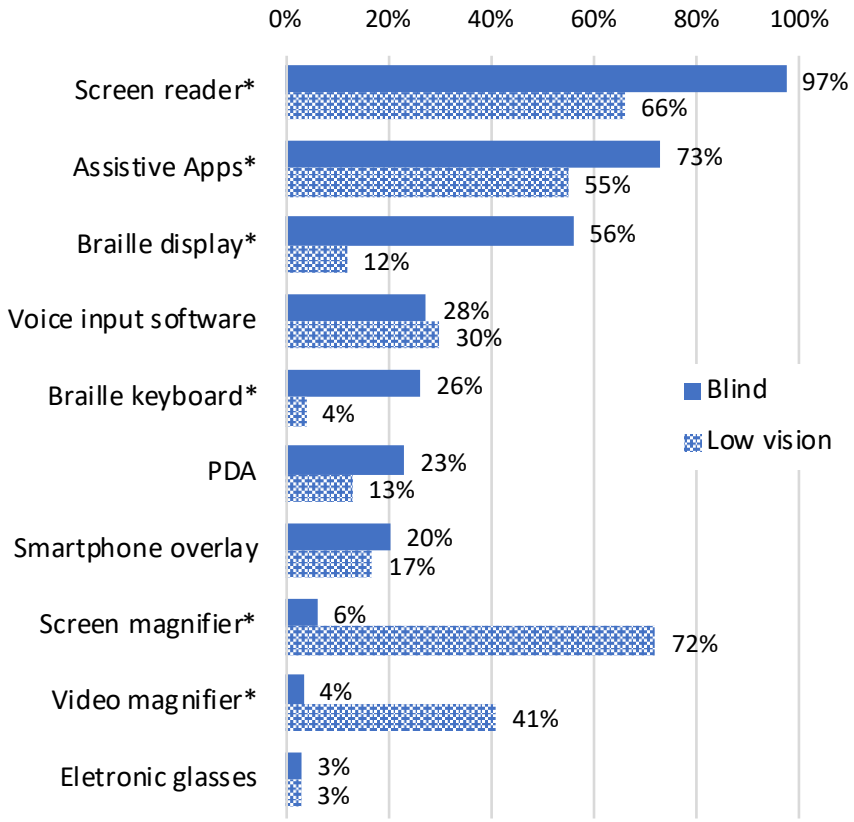

Figure 2: Blind and low vision participant's use of assistive technology. Significant differences marked with *.

3.3.2 Use of Assistive Technology

We asked participants to select assistive technologies they used from a list with 10 options. The most commonly used by participants in both groups (blind and low vision) were: screen readers (87.7%), assistive apps (67.4%) and Braille displays (42.5%). Figure 2 shows the assistive technology use. Only seven participants reported not using any of the devices listed in the question.

We compared the two groups of participants and found the use of the following assistive devices were significantly more common 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), and assistive smartphone applications (χ^2 (1, N=325) = 10.08, p < .005). On the other hand, the use of the following assistive devices was significantly more frequent 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 [8]. But our results also indicate people who are blind require the use of more assistive technologies (M=3.37) than people with low vision (M=1.41), except for devices that support the use of residual vision.

Participants who use Braille displays became vision impaired at younger age (M=3.9) than participants who do not use Braille displays (M=11.5) (t (321) = 2.81, p < .005). Considering participants' country did not influence their use of Braille displays, we believe our results might indicate that Braille education is more predominant among 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. [2], 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.

3.4 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.

3.4.1 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 [5]. Almost all participants (96%) said passwords are important or very important. Figure 3 illustrates the distribution of the results between the two groups (blind and low vision), although we did not find significant difference.

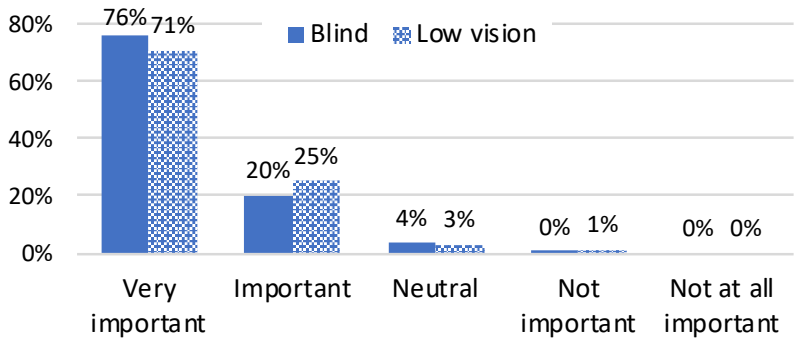

Figure 3: Blind and low vision participants' ratings for the importance of passwords.

We asked participants to explain their rating of password importance, illustrated in Figure 4. Among participants who rated passwords as very important, important or neutral, most mentioned acknowledging the importance of passwords for protecting personal information (57.6%) such as photos and contact lists, followed by assuring their privacy and security (26%). Answers grouped in the later included the words privacy or security in them.

Interestingly, 12 participants who 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 [38]: “[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 they secure (N=6).

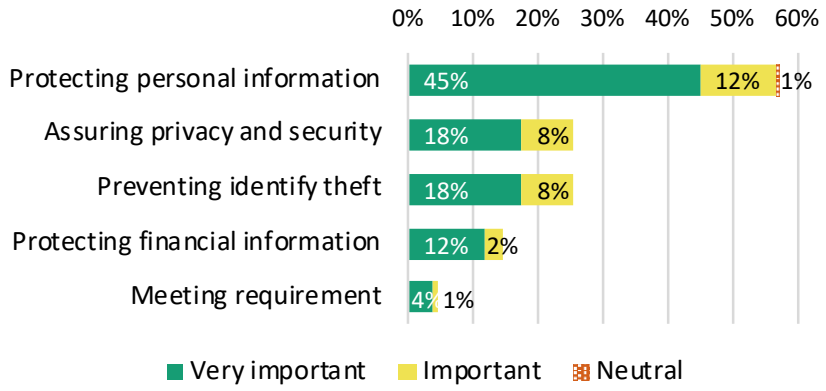

Figure 4: Participants’ top five reasons for rating passwords as Very Important (green), Important (yellow) or Neutral (red).

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 who 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."

3.4.2 Digital Presence

Participants' near unanimous evaluation of passwords as important is in line with their extensive password-protected digital presence (Figure 5). Only two participants declared not using passwords for any of the items we asked them about. We compared items participants reported protecting with passwords between the two groups and found no significant differences between the two groups of participants (*n.s.*).

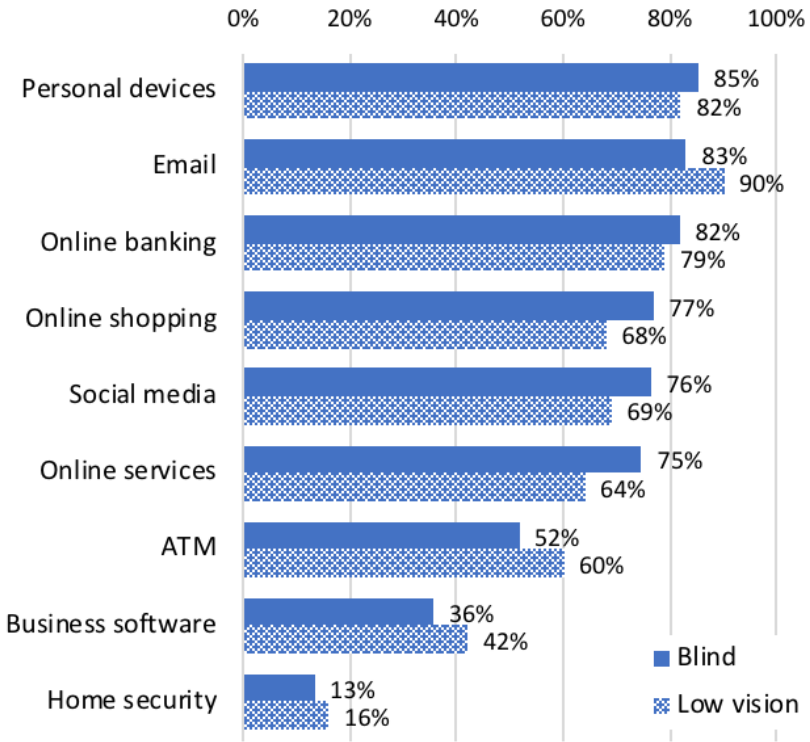

Figure 5: Blind and low vision participants' items protected with passwords.

Participants' digital presence significantly differed by age. Email users were significantly younger (M=44.3) than non-email users (M=54.2) (t (323) = 4.13, p < .001).

Similarly, social media users were significantly younger (*M*=44.1) than non-social media users (*M*=*M*=50.5) (t (323) = 3.26, $p < .005$), and users of password-protect personal devices were younger (*M*=44.8) than users of non-password protect devices (*M*=50.8) (t (323) = 2.53, $p < .05$). On the other hand, users of home security system were significantly older (*M*=50.3) than non-home security system users (*M*=44.8) (t (323) = 2.14, $p < .05$), and online shopping users were significantly older (*M*=47) than non-online shoppers (*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 (*M*=5.0) and low vision participants (*M*=4.7). It is also similar to the sighted population, which reported having 5 passwords on average [86].

3.4.3 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. [5]. Wash et al. [98], 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 the strategies used by sighted people a larger proportion reuse passwords (96%), use password managers (81%), and keep written records (78%) [86].

3.4.4 Ability to Keep Digital Information Safe

We asked participants to rate their ability to keep their digital information safe. Almost half of our participants (47.4%) believed they were able to secure their digital information, followed by very able (33.8%) and neutral (14.8%) (Figure 6). 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 (χ^2 (1, N=325) = 8.14, p <.005).

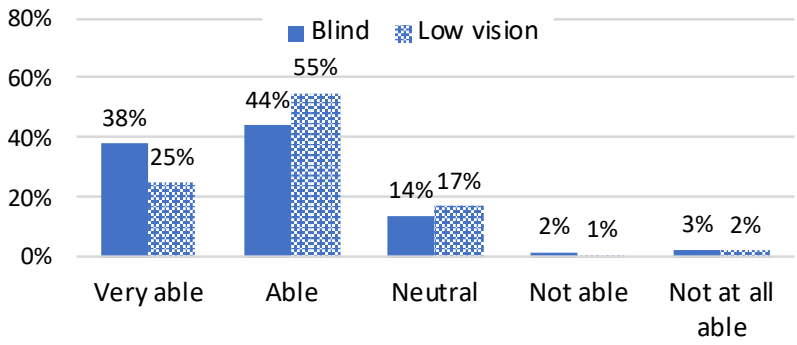

Figure 6: Blind and low vision participants self-assessed ability to protect their digital information.

We asked participants to explain their rating (Figure 7). 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%).

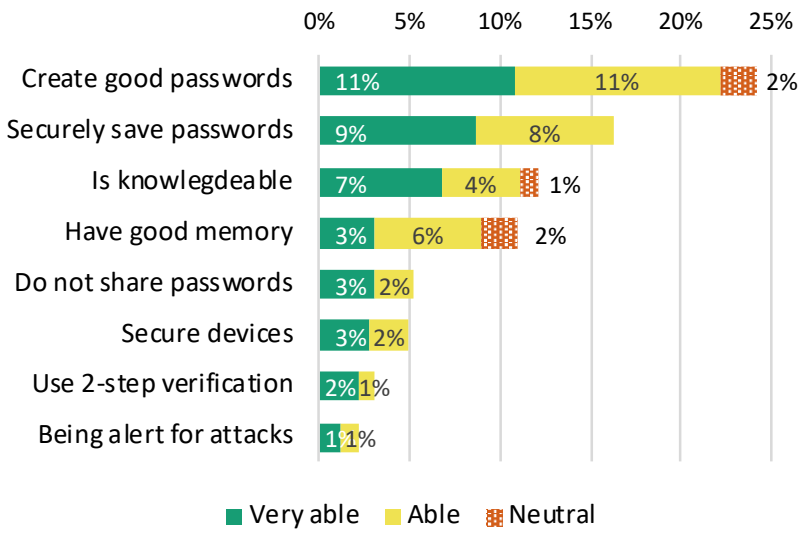

Figure 7: Participants' top five reasons to self-assess Very able (green), Able (yellow) or Neutral (red).

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 they could improve (5.1%). A few other participants attributed their ability to accessibility issues (N=6), e.g. with websites that have moving numbers for passwords. Others, to their 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 from protecting 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 touch screen 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) expressed felling patronized with our enquiry about rating their ability of protecting their digital information, answering their vision impairment does not influence their ability.

3.4.5 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 8).

Blind participants were more concerned with aural eavesdropping than participants with low vision (χ^2 (1, N=226) = 7.66, p =.006). 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 [5], 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 touch screens.

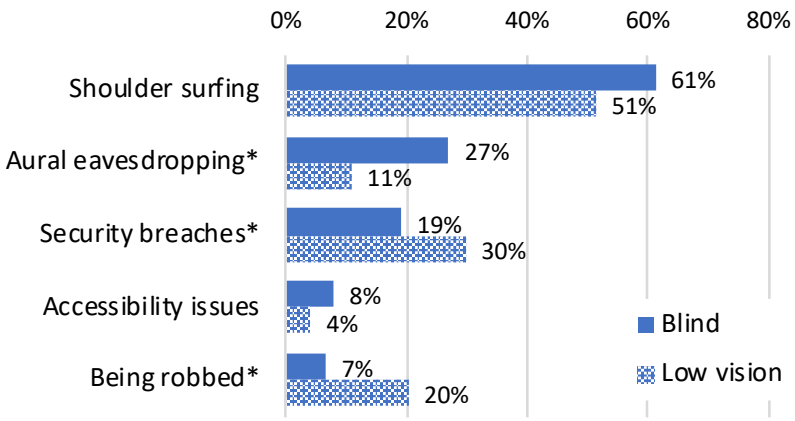

Figure 8: Blind and low vision participant's concerns with using passwords in public spaces, among those who had concerns (N=226). Significant differences marked with *.

3.4.6 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.

3.5 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 the least secure method, which came second.

3.5.1 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 readers as the most secure, followed by alphanumeric passwords, and facial recognition (Figure 9). 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).

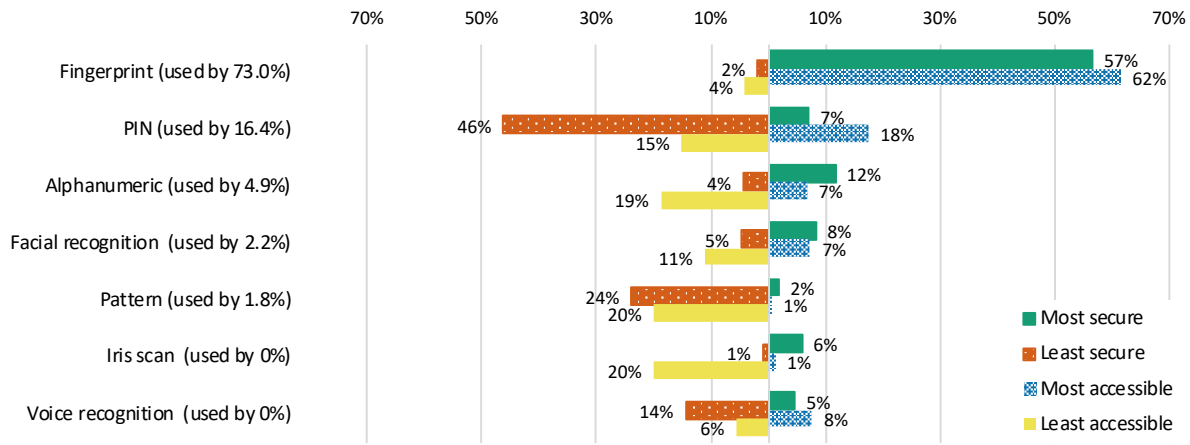

Figure 9: Participants most used selections of most secure (green), most accessible (blue), least secure (red), and least accessible (yellow) user authentication methods.

Interestingly, some participants (14.1%) said they chose fingerprint readers 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. [60]), 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 fingerprints as the most accessible method (Figure 9). 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 has 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).

3.5.2 PINs: Least Secure Method

As the least secure method, most participants chose PINs (N=149), followed by patterns drawn on the screen and voice recognition (Figure 9). 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. [50]). 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.

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.

3.5.3 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 9). 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 (χ^2 (1, N=325) = 5.78, p =.02). 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 (χ^2 (1, N=325) = 7.08, p =.008). 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).

3.5.4 Ideas for a New Method

We asked participants to share their thoughts on what they would like to have in a new user authentication method. Most participants mentioned the improvement or continuation of existing user authentication methods, such as biometrics (31.7%) or 2-factor authentication (6.5%), or were unsure (24.9%). Even though 7% of participants said there was no need for a new user authentication method, a lot of others did not present an idea per se, but commented on characteristics a new method should have, including being secure (10.8%), simple and with good usability (8.3%), accessible (4.6%), quick (4.0%), and accurate (3.7%). 11 participants suggested having the use of gestures. For example, P10 suggested a new

method with “some sort of code you can do with your hands”, while P144 suggested a “device prompt you in a tactile way and you respond with a gesture”. The lack of tactile feedback was one of the reasons mentioned by participants who choose not use smartphones, such as P258 who said “I am a very visual learner, and having no tactile overlay or physical buttons does not help me learn or use a smartphone or tablet.”

3.5.5 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. In a new user authentication method, most would value security, simplicity and accessibility.

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

	Blind		Low vision	
Method	**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%

3.6 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.

3.6.1 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 (M=43.2) were more likely to have a user authentication method in their smartphones than older ones (M=51.2) (t (294) = 3.87, p < .001).

Similarly to what was found by Leporini et al. [62] and Ye et al. [103], 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 differed 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.*)).

3.6.2 Choice of User Authentication Method

When selecting an authentication method, most smartphone users use fingerprints (73%) (Figure 9). 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 long (*M*=5.3) and the median alphanumeric password 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. [37]). 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).

3.6.3 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% [81]), 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.

3.6.4 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.”

3.6.5 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.

3.7 Discussion

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.

3.7.1 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 [26], almost 70% of our participants were blind, similar to an online survey by Azenkot and Lee [15], 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.

3.7.2 Broad Smartphone Use

More people with vision impairment owned a smartphone (91%) than sighted people (77%) [81]. 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.

3.7.3 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.

3.7.4 Ability to Keep Data Secure

Most participants felt able or very able to protect their digital information, so we reject our first hypothesis (**H1**). 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 [5].

However, we recognize that for 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.

3.7.5 Secure and Accessible Authentication Methods

The proportion of survey participants who declared the use of user authentication methods to protect their personal devices was higher than in previous research (75.3% vs 33.3% and 0%) [16, 37]. 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 (**H2**). 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.”

3.7.6 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 (**H3**): Blind people considered patterns and iris scans the least accessible methods, potentially because they require some level of visual interaction; while people with low vision selected alphanumeric passwords and PINs, possibly due to the difficulty of typing using a screen magnifier.

3.7.7 Limitations

This was a self-conducted survey so participants' answers may not necessarily reflect their real behaviours. Additionally, our 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.

3.8 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.

4 Chapter: Prototype Development

This section covers the development of a new device for password input, and a password recognition program, besides from a smartphone app to simulate PIN entry. We also present the development of a website to collect and verify password entries.

4.1 BendyPass Prototype

Informed by our online survey results, and to help people with vision impairment to better protect their smartphones from unauthorized access, we propose the use of deformable user interactions (DUIs) [72, 87], specifically bend passwords [68]. We developed BendyPass, a deformable flexible device implementing bend passwords as a more tactile password-input method (Figure 10) for people with vision impairment.

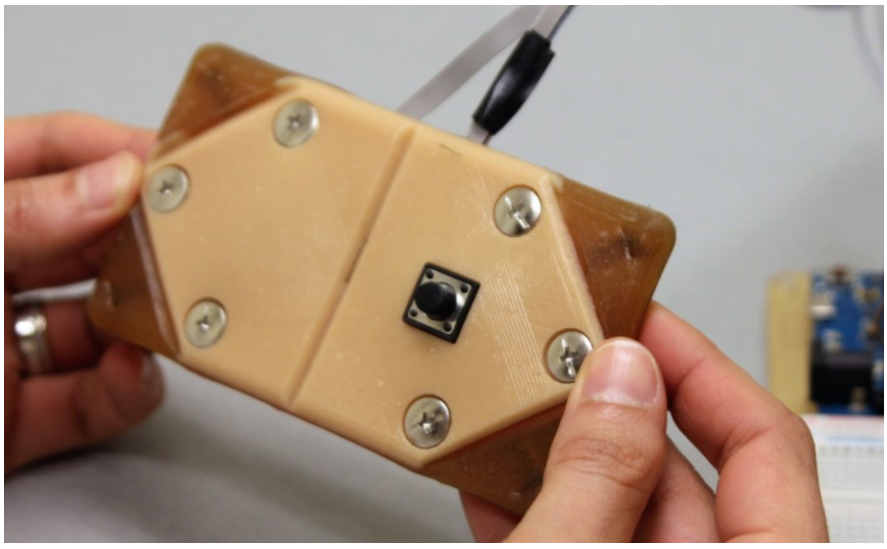

Figure 10: BendyPass prototype, where users can enter bend and fold gestures to form a password.

4.1.1 BendyPass Overview

From our online survey [29], we found that most people with vision impairment consider PINs the least secure user authentication method for smartphones and people who have low vision consider it one of the most inaccessible methods; although PIN is the most common method, required even when biometrics methods are available. We also found that the complexity of existing user authentication is one of the reasons for some people not to use any of them, leaving their smartphones completely unprotected. Additionally, we found the biggest concern on entering passwords in public amongst people with vision impairment is the risk of shoulder surfing attacks.

We looked into a simple user authentication alternative for people with vision impairment, which would better protect them against shoulder surfing and could replace PINs. Based on previous research, we decided to design a new flexible device for people with vision impairment, similar to Typhlex [41], for bend password input, as done by Maqsood et al. [68].

Our prototype called BendyPass is made of silicone and has the dimensions of an iPod touch. It has grooves close to its corners and at the centre, to facilitate bend and fold gestures, and it contains embedded flex sensors to recognize bend gestures. BendyPass is able to recognize 10 simple bend gestures (Figure 11), including bending each corner upwards or downwards (8 gestures) and folding it in half upwards or downwards (2 gestures). A series of bend gestures performed in BendyPass is called a bend password. When a user performs a gesture, BendyPass vibrates, while a computer provides audio feedback informing the name of the gesture recognized, such as “Top right corner up.”. We included audio feedback to help users learn the name of the gestures but believe it could be turned off by the user on a real device. The names of BendyPass gestures are composed by

both location and direction, as those are characteristics easy to recognize, based on findings from Warren et al. [97].

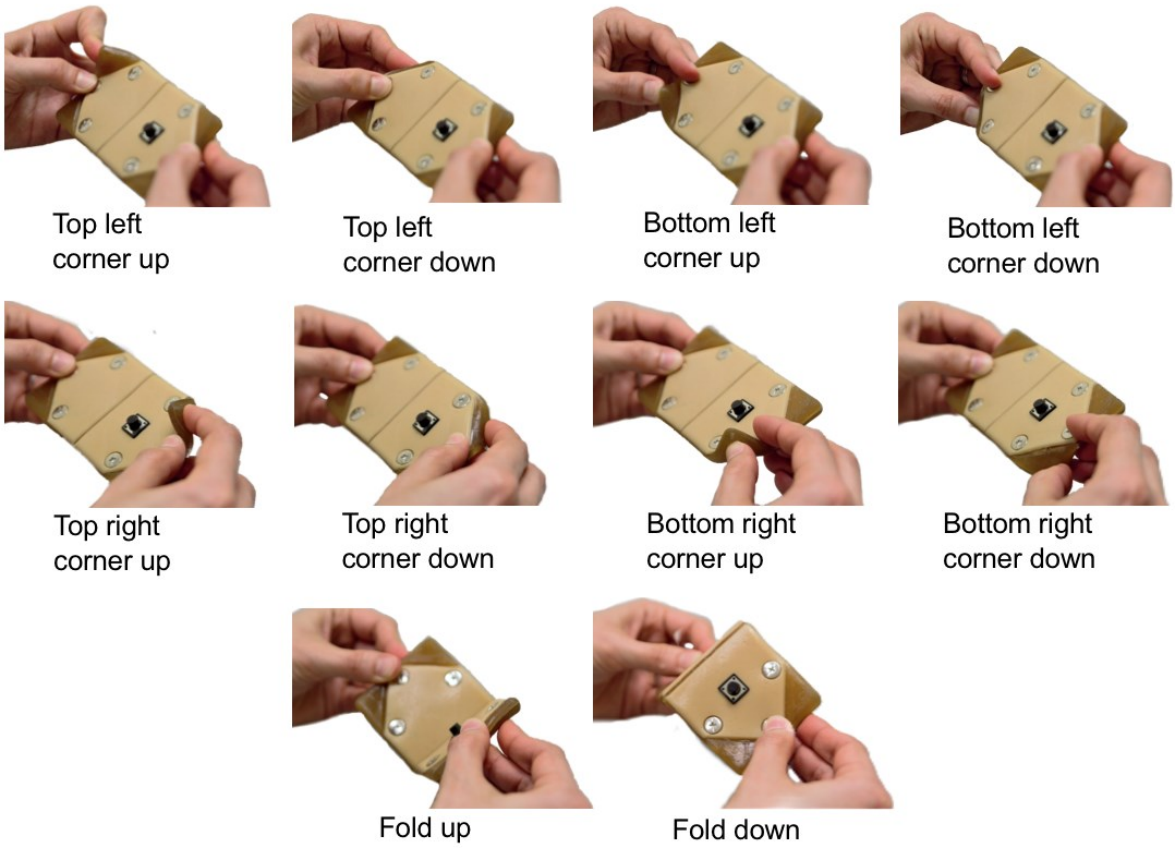

Figure 11: Set of bend gestures available on BendyPass.

4.1.2 Prototype Design

We designed BendyPass considering findings from previous research. With regard to size, we learned from Typhlex that the device should fit a small size to avoid re-gripping [40], a general conclusion found by other DUI researchers [58, 61, 63]. We also learned that grooves work as a tactile indication of bendable areas, guiding blind users to locate bendable areas [39], in addition to providing strain release for easier bending [41].

We started the design by defining the dimensions of the device as 11.5 x 6 x 1 cm, similar to those of Typhlex. Then, we used Blender [22] to design silicone moulds for the

prototype (Figure 12), for testing different groove positions and shapes to indicate bendable areas. We used the moulds to pour different silicone types. The various prototype versions allowed us to evaluate variations of material hardness and design and positions of grooves (Figure 13). We tested different prototype versions with specialists in flexible devices and two experts at the Canadian Council of the Blind.

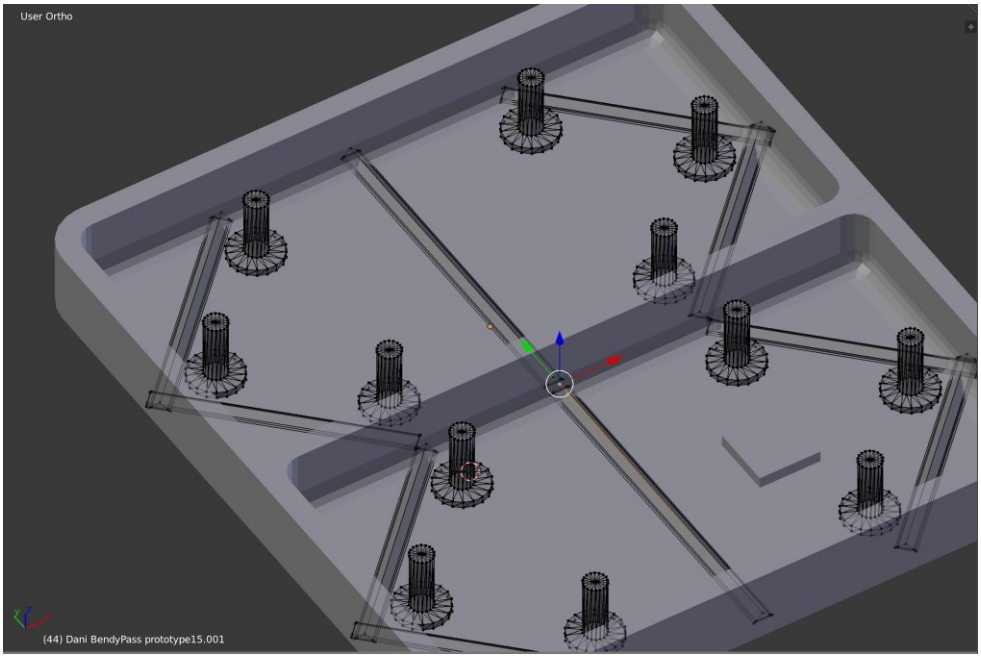

Figure 12: 3D model of the final BendyPass prototype mould in Blender.

We also learned from Ernst et al. [39] that using a rectangular prototype in portrait orientation requires participants to re-grip it to perform gestures in opposite poles (top and bottom). Considering that and after initial prototype evaluations, we decided to design our prototype for use in landscape orientation, to facilitate the user's access to all four corners of the prototype while holding it with both hands.

Our final design includes grooves that create triangular areas around each of its four corners, a vertical groove in its centre, and a lowered part to insert a squared push button, as shown in Figure 14. We extended the grooves to make them span from side to side for an

effortless bend gesture. We also angled them, so fingers can sense the grooves clearly but are not pinched when the device is bent.

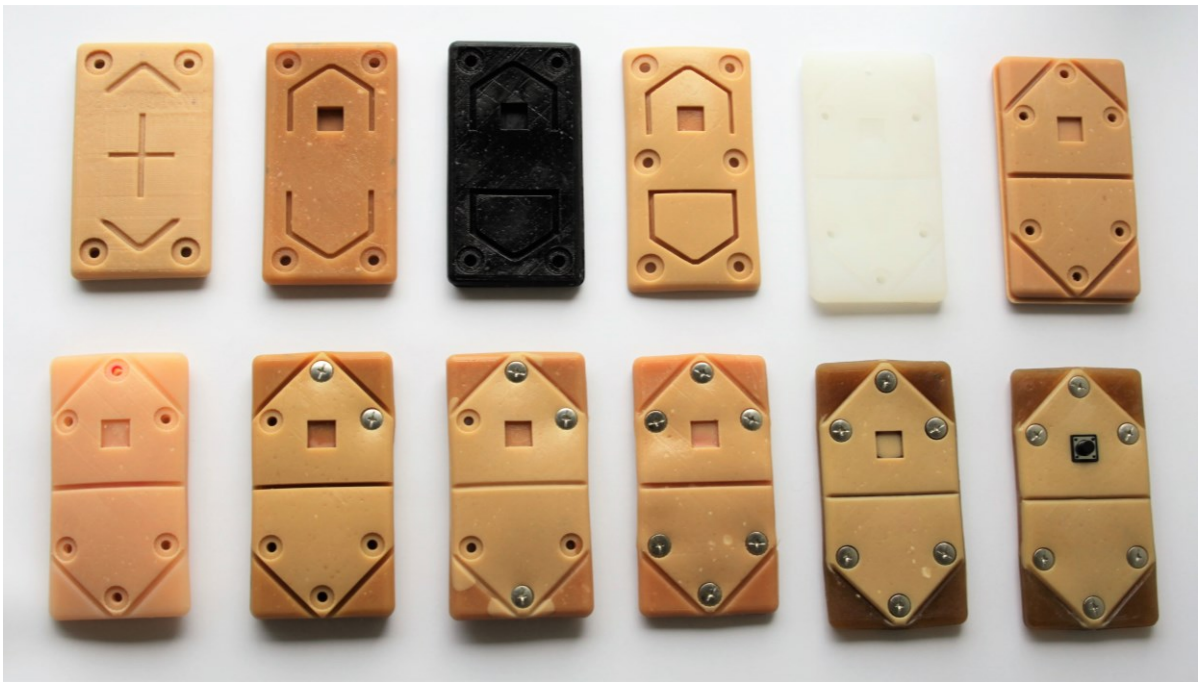

Figure 13: Initial prototype versions.

To provide users with indication of how much to bend, as recommended by Ernst et al. [41], we decided to include haptic feedback, as done by Strohmeier et al. [88], so the device vibrates when a gesture is recognized. Additionally, to help the user confirm the correctness of the input [6], we designed BendyPass to provide audio feedback indicating the name of the gesture recognized or the function activated. While designing BendyPass, we also considered the importance of avoiding accidental activation of gestures [103], and minimizing the use of “dwell time”, because it can negatively affect usability [56]. For that reason, we decided not to use 20 possible gestures as done in prior research by Maqsood et al. [68] (including single corners and double corners bent at once). By keeping the total number of possible gestures at 10, we were able to minimize the number of accidental activations that we observed during sessions of prototype evaluation with experts at the

Canadian Council of the Blind and eliminated the need for a “dwell time” to help identify whether users were bending one or two corners at a time.

Furthermore, we considered previous work recommending the design of devices for a discreet use, and with a good appearance not to look weird [5]. BendyPass’ size, the use of good quality 3D printing and silicone allowed us to present a nice-looking device, while the landscape orientation permits users to reach all corners and perform gestures discreetly.

The final version of BendyPass is composed of two silicone layers that enclose electronic components, including flex sensors to capture bend gestures, a vibration motor to give feedback when a gesture is recognized, and a button (Figure 10). The button allows the user to both delete the last gesture entered and confirm the password, depending on how long the user presses it before releasing it. A long button press (more than half a second) triggers the confirm function, while a shorter button press triggers the delete function.

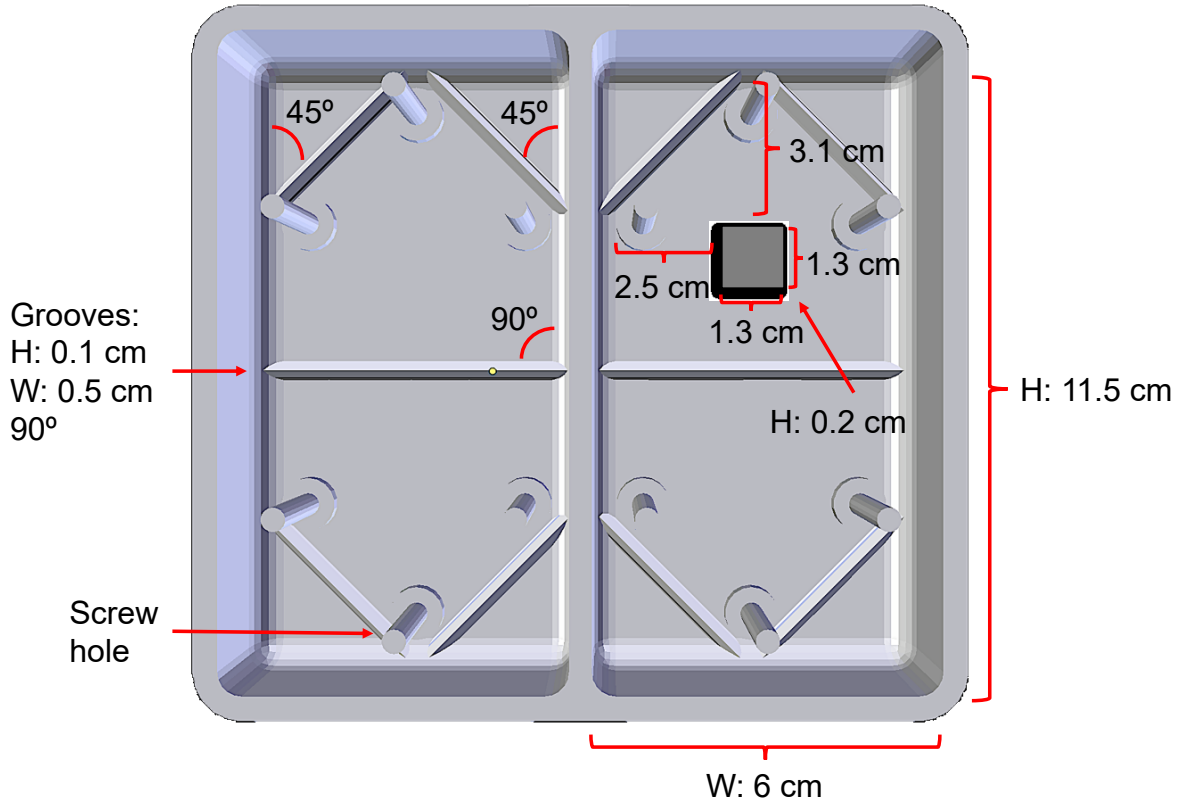

Figure 14: Final BendyPass prototype design.

4.1.3 Prototype Fabrication

To fabricate BendyPass, we used the 3D mould printed from the model presented in Figure 14. In this 3D printed mould, we used two different types of silicone to make the bendable areas more flexible than the central area, where we placed the rigid components. This emphasizes the areas that could be bent while better protecting the electronic components that should remain flat. We combined two silicone types by first pouring mixed Alumilite A80 in the central diamond-shaped area of the mould, and pouring mixed Alumilite A30 in the corners and over the A80 rubber immediately after (Figure 15). This is in line with the recommendation from Ernst [39, 41] of having pronounced grooves, clear physical affordances and different material stiffness to help identify bend locations.

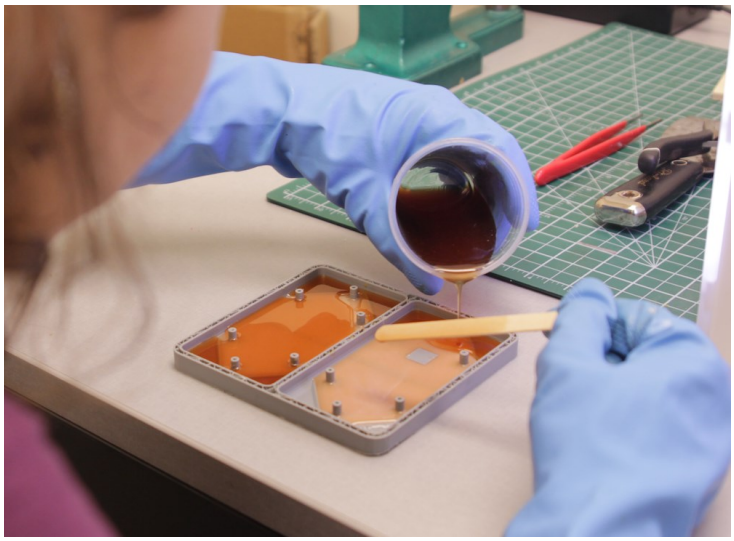

Figure 15: Researcher pouring mixed silicone Aluminite A30 on top of layer of silicone Aluminite A80.

BendyPass has 5 1” Flexpoint bidirectional bend sensors, placed in the centre, top-left, top-right, bottom-left and bottom-right corners. It also has a vibration motor positioned inside its left side, to give haptic feedback for the user that a gesture was recognized by the

system and a push-button on its right side, to allow the user to delete the previous gesture entered or confirm the password (Figure 16). Our prototype has a button embedded, because Maqsood et al. [66] reported challenges with having it decoupled from the flexible prototype, which required users to shift their attention from the device to the control panel where the buttons were.

We chose to not cast the electronic components within the silicone mould so we could easily replace mal-functioning components. Thus, to keep the electronic components in place, we cut a sheet of foam (0.2 mm thick) in the same dimensions of BendyPass, and cut holes on it to fit each of the five bend sensors and the vibration motor (Figure 16). We close BendyPass and keep all its layers together (silicone, foam with components and silicone) with Chicago screws, positioned in a diamond shape to leave the prototype corners free. To keep all bend sensors in position and facilitate bending the corners, each corner was stitched once using fishing line.

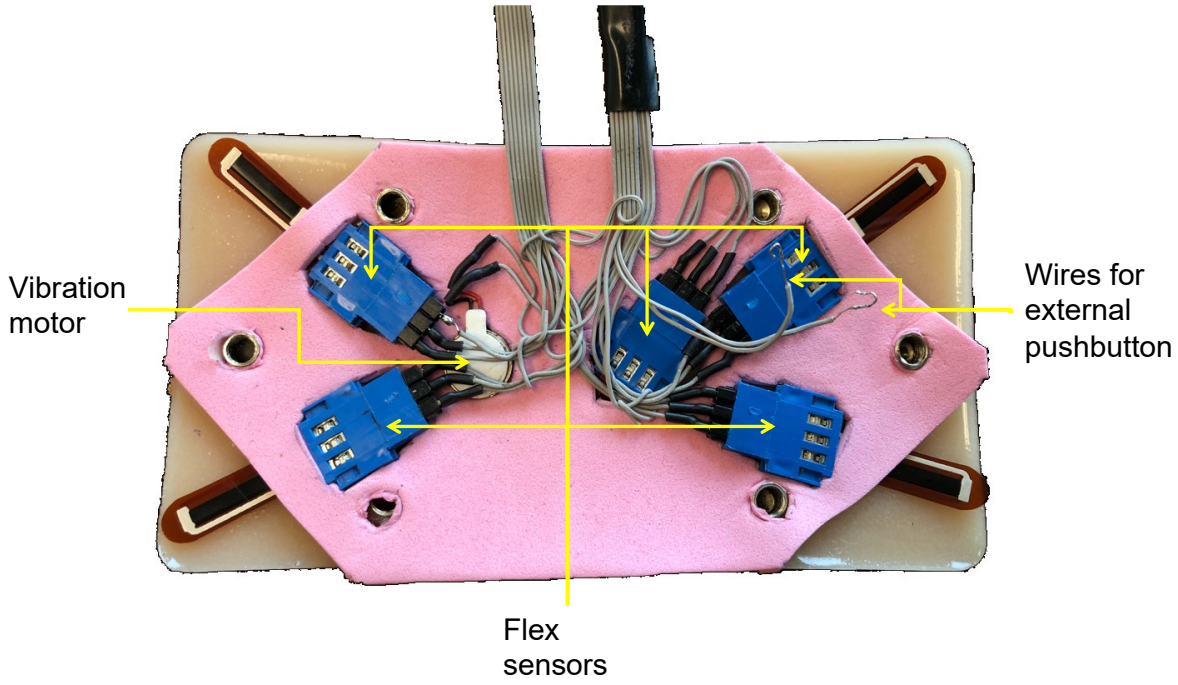

Figure 16: Electronic components of BendyPass, housed in a thin foam layer (pink).

Lastly, we connected all electronic components of the prototype to an Arduino Leonardo micro-controller, which transforms the gestures and button presses into keyboard entries on a connected computer, by using a bend password recognition program.

4.1.4 Bend Password Recognition Program

We developed an algorithm for recognizing bend gestures on BendyPass in Arduino [10], considering the position of the flex sensor and the direction of the gesture (up or down). When each of the five flex sensors are bent, their resistance value registered by the Arduino micro-controller changes, and is mapped to an integer value between 0 and 1023. Our algorithm reads the values of each flex sensor and considers the sensors stationary if their resistance value is within a particular range and if they have not changed more than 5 integer points since the previous readings.

In case a corner is intentionally bent up or down or the centre is folded up or down, the resistance value becomes higher or lower than the specified range by more than 5 points. In that case, our Arduino program maps the corner bent and the direction of the bend to a letter. Considering the flex sensors are extremely sensitive and are tightly attached to the silicone pieces of the prototype, we used a range from 250 to 750 for a stationary position, to account for potential flexion after bend gestures. As our algorithm considers not only the thresholds mentioned, but also requires a difference of more than 5 points between the current reading and the previous one, we do not need to calibrate the prototype between uses, as done in previous studies [68].

The final version of the bend password recognition program reads each corner being bent, and the centre being folded as bend password characters. We chose to describe folding gestures based on the direction of the movement made with the device's sides, after a brief survey with interaction specialists and considering the easiness of describing the

gesture performed by the user. For example, Fold up is a gesture in which the user brings the sides of the prototype up, moving its centre down. When a sensor is bent up or down, the Arduino program presses the corresponding key on the laptop keyboard, and the vibration motor on the prototype vibrates for 200ms. After that, the program waits for 300ms before reading again the values of the flex sensors, for a total interval of 500ms between gestures.

Each gesture performed in BendyPass becomes a letter on the computer, as mapping shown in Table 2. This key mapping is invisible to the user, who only needed to define and replicate a sequence of bend gestures. For example, participants will memorize a password including Top right corner up, Fold up, Bottom left corner down, not the letters C-T-F. Additionally, the user can delete a previous gesture by pressing and releasing the button in less than half a second, and confirm the password, by pressing the button and holding it down for at least half a second. Activating the deletion in the BendyPass triggers Backspace on the computer, while confirming a password in BendyPass activates the Enter key on the computer.

Table 2: Letters mapped to each bend gesture available on BendyPass.

Gesture	Letter
Top Left Corner Up	A
Top Left Corner Down	B
Top Right Corner Up	C
Top Right Corner Down	D
Bottom Left Corner Up	E
Bottom Left Corner Down	F
Bottom Right Corner Up	G
Bottom Right Corner Down	H
Fold Up	T
Fold Down	U

4.2 PIN Entry Prototype

Considering PINs are the main user authentication method in most smartphones, even though people with vision impairment consider it one of the least secure user authentication methods [29], we opted to compare PINs to bend passwords in our user study. This way we also follow the methodology used by Maqsood et al. [68], and compare two user authentication methods of the same type (knowledge-based).

4.2.1 Smartphone

In order to compare bend passwords to PINs, and considering most people with vision impairment use iPhones [29], we used an iPhone 6S to receive PINs (Figure 17). As an iOS smartphone, the iPhone has standard accessibility features including screen magnifier and screen reader VoiceOver. We kept the smartphone in a protective case, but without screen protection, maintaining the default responsiveness of the touch screen.

4.2.2 PIN Entry App

After testing various apps intended to turn the smartphone into a Bluetooth keyboard for a computer, we decided to use Unified Remote [93], which is available at the Apple App Store. Unified Remote has a keypad screen similar to a calculator or the keypad on a large external keyboard, as shown in Figure 17.

Although not perfect, we chose Unified Remote because it had large buttons and worked relatively well with VoiceOver, as all numeric keys and the Enter key were labelled and properly read. The Backspace key was not properly labelled but was identifiable while using VoiceOver because it was the only button on the screen to be read as “Button”. In the

preliminary tests running Unified Remote with VoiceOver, we identified it worked with the Standard Typing style available in iOS accessibility features. In this typing mode, the user can move the finger around the screen to explore it, and after hearing to the desired button or link read aloud, the user has to lift up the finger from the screen and then double tap the screen, in order to trigger the key or link. Another way to use this typing method is by keeping the finger on the screen after finding the desired key, and using another finger to double tap the screen, what is commonly called “split tapping”.

By using Unified Remote, all key presses are sent to a MacBook Pro laptop, where our password website receives the key presses and saves them.

Figure 17: iPhone 6S Smartphone used in the user study, with Unified Remote app open.

4.3 Password Website

We also developed a PHP website to receive and store passwords and verify if passwords are correct. The website was connected to a mySQL database and hosted in the researcher's computer using XAMPP.

4.3.1 Website Structure

We structured our website to support the user study, by having an initial screen to input the participant number, the session and the device used. The website then presents all steps of the study in sequence, starting with a training screen, moving to password creation, confirmation, and rehearsal screens for session 1. For session 2, it opens in the login screen. In each step, our mySQL database save participants' numbers, password entries, and the time the input started and ended.

4.3.2 Website Feedback

Our website provides audio cues to help the user to navigate the process of creating a password, by saying, for example, "Create your password using the gestures learned" or "Wrong password, please try again". We recorded the screen reader VoiceOver reading all messages on a MacBook Pro, using the default speed of 45. We also prepared our website to provide audio feedback when the user presses the button or performs a bend gesture, by recording VoiceOver reading the name of the keys and bend gestures.

With all the audio files prepared, we used JavaScript to open the appropriate audio files for each situation. For bend gestures, we assigned each audio snippet to be triggered by the respective letter entered. For example, we assigned the letter A to the audio snippet

that says, “Top Left Corner Up”, and we assigned the audio file that says “Enter” to the action of pressing and holding BendyPass button.

An example of a bend password created on BendyPass can be found here.

4.4 Password Strength

The theoretical password space, or the total number of possible passwords, is a measurement used to evaluate the security of passwords [20]. According to Maqsood et al. [68], the theoretical password space can be calculated by using the formula log (c^n), where c = number of available digits or gestures and n = the password length, and the result is represented in the unit bits.

For Florencio & Coskun [44], a 20 bit password, such as 6-digit numeric PIN suffices for protecting the user from a force-brute attack to the account, from guessing and from shoulder-surfing. Although it does not indicate resistance to more elaborate attacks such as phishing, key-logging or bulk guessing attacks. Considering both our prototypes will have 10 possible characters, passwords with a minimum length of 6 digits or gestures would be considered secure. For example, a password like 5-3-7-4-5-7 has the same security of a bend password as Top left corner down - Fold up - Bottom left corner up - Bottom right corner up - Fold up - Top right corner down.

5 Chapter: User Study

We designed and conducted a user study with participants who were blind or had low vision, to evaluate the potential of bend passwords as a password input method for them, and to collect their perceptions about our prototype BendyPass.

5.1 Research Questions

We ran a user study with vision-impaired participants to answer the following research questions:

Q1. How easy to create are bend passwords for people with vision impairment?

Q2. How does the learnability of bend passwords differ between people who are blind and people who have low vision?

Q3. How memorable are bend passwords for people with vision impairment?

Q4. How easy to enter are bend passwords for people with vision impairment?

This study is the first to explore the potential of bend passwords for people with vision impairment. Through an analysis of the data collected in study sessions with 16 participants, the contributions of this study are: (1) insights on how easy to learn and how easy to memorize bend passwords are for people with vision impairment; (2) suggestions on potential applications for bend passwords; (3) design recommendations for new deformable devices.

5.2 User Study Methodology

We designed a user study following the methodology proposed by Maqsood et al. [68] for their study on user-generated passwords, including two study sessions: the first for participants to create new passwords, and the second, a week after the first, when participants try and use their passwords to unlock the devices. Our hypotheses for the user study were:

H1. We expect people with vision impairment will create PINs faster than bend passwords, due to their familiarity with PINs, based on Maqsood et al. [68].

H2. We expect bend password will be easier to learn by people who are blind, because they will not be impacted by the lack of visual feedback on BendyPass when compared to the touch-screen smartphone.

H3. We hypothesize people with vision impairment will memorize bend passwords as easily as PINs, because of the use of their “muscle memory”.

H4. We expect people with vision impairment will take longer to enter bend passwords than PINs, based on Maqsood et al. [68].

5.2.1 User Study Overview

We structured our user study following the main tasks proposed by Maqsood et al. [68], as shown in Figure 18.

Our study was composed of two 60-minute sessions with participants who are either blind or have low vision. In the first session, we asked participants to create, confirm, and rehearse a bend password on BendyPass and a new PIN on a touch-screen smartphone. In the second session, about a week after the first session, we asked participants to use the passwords created in the first session to complete five successful logins on each device.

While in the first session we evaluated the learnability of bend passwords, in the second session we evaluated the memorability of bend passwords and the level of effort required to enter passwords using BendyPass.

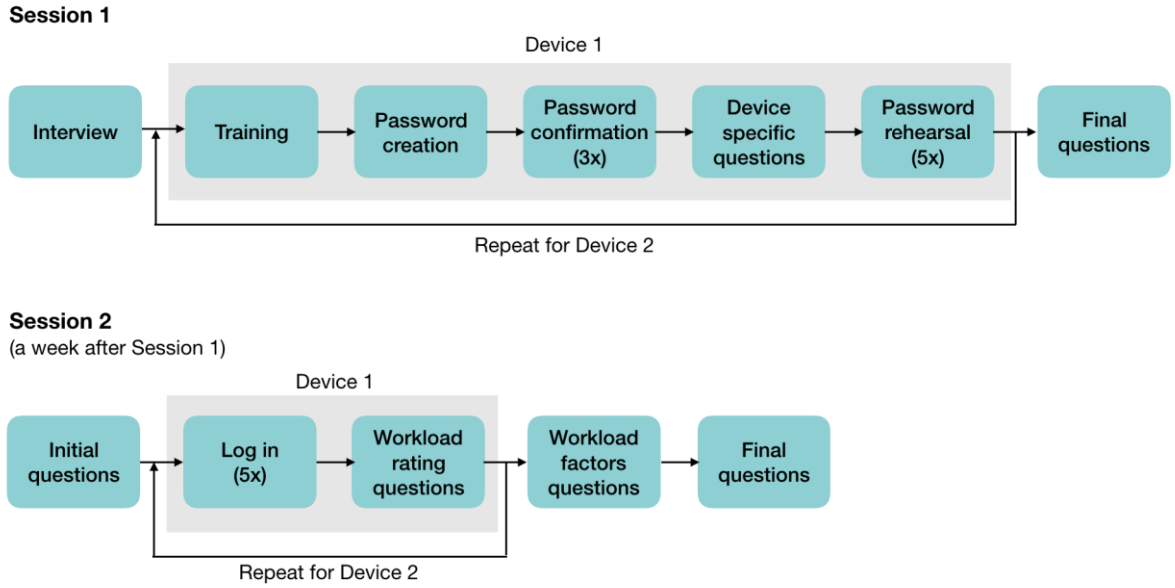

Figure 18: User Study Structure.

We hosted our user study protocol and questionnaires in two online surveys in Qualtrics [79], one for each session. The study setting for both sessions included a rectangular table and three chairs, a camera with a tripod beside the participant, BendyPass prototype, an iPhone 6S smartphone, and a MacBook Pro laptop connected to both devices and turned to the researcher. We requested participants to sit at the longer side of the table, while the researcher sat at the adjacent corner. A research assistant sat behind the camera, to operate it during the sessions.

We presented the devices (BendyPass and smartphone) to participants in a counterbalanced order, both among participants and between sessions with the same participant, as shown in Table 3. In both sessions, after interacting with each of the devices, participants answered specific questions related to their interaction with the device.

Table 3: Counterbalanced order used in the presentation of devices during the user study.

Participant	Session 1		Session 2	
	First device	Second device	First device	Second device
P01	BendyPass	Smartphone	Smartphone	BendyPass
P02	Smartphone	BendyPass	BendyPass	Smartphone
P03	BendyPass	Smartphone	Smartphone	BendyPass
P04	Smartphone	BendyPass	BendyPass	Smartphone
…	…	…	…	…

Before starting the study, we ran three pilot studies of the first session with sighted participants not familiar with the project, to evaluate the length of the session and technical aspects, including prototypes, website and the online protocol on Qualtrics. We also ran one pilot study of the second session with a sighted participant.

We recruited participants for the user study by contacting the Carleton University's Centre for Students with Disabilities (Paul Menton Centre), the Canadian Council of the Blind, an accessibility expert and by posting the study on the Carleton Research Participants page on Facebook. Participants who were vision impaired and at least 18 years-old qualified to participate.

The study sessions took place from May 21 to June 25, 2018, either at Carleton University or at the Canadian Council of the Blind's office in Ottawa. As a token of appreciation, we gave participants $10 after the end of the first session, even if they withdrew from the study, and another $30 after the end of the second session. We also covered reasonable transportation costs for participants. We obtained ethical clearance from the Carleton University Research Ethics Board (CUREB-B # 102815).

5.2.2 User Study Session 1

The first session started with the researcher asking if the participant agreed with the consent form, which the researcher either sent by email or read out loud, and with being video and audio recorded. Then, we interviewed the participant using the questions from the online survey.

Then, we presented one device at a time to participants, teaching them how to use the device for about 2 or 3 minutes [84], we allowed them to train to use it and then asked them to create a password and confirm it 3 times. We asked for 3 confirmations from participants to follow the protocol used by Maqsood et al. [68].

For the smartphone, we asked participants whether they preferred to use it with a screen reader or a screen magnifier on. After turning on the preferred assistive feature, we explained that the smartphone had an app open that connected the phone to the computer. As the keypad contained additional buttons, we instructed participants to ignore the keys we would not use during the user study.

For BendyPass, we started by handing the device to participants in landscape orientation, asking them to hold it that way. Then, we explained the device's characteristics and functionalities, and that it was connected to the researcher's computer. Then, we explained how to activate the 10 possible gestures and what feedback they would receive whenever a gesture was recognized.

After introducing either device to the participant, we opened the website in the training mode and encouraged participants to try each of the bend gestures and button presses on BendyPass at least twice, and at least some key presses on the smartphone. As soon as participants said they were ready to create a password, we asked them to create a memorable and secure password, with at least 6 gestures/digits. In the case of the smartphone, the researcher also asked participants not to use pre-existing PINs they had, in

order to avoid skewing the memorability results, as suggested by Maqsood et al. [68]. Then, the researcher loaded the next website page, where the participant created a password, which was saved into the database, associated with both the participant number and the device.

Participants then followed the audio cues from the computer to create and confirm their passwords. Once the password was confirmed, we posed questions to participants about the password created, before they rehearsed their passwords by having as many attempts as they needed to complete 5 successful logins.

At any moment, if participants forgot their password, we reopened the creation website page for them so they could create a new one. If participants forgot their password during the rehearsal step, the researcher did not ask questions again about the password created.

Once the rehearsal was completed with one of the devices, we presented the next one, following the same steps. At the end of the session, we asked final questions regarding participants' perceptions on the bend password system and BendyPass.

5.2.3 User Study Session 2

The second session started with the researcher asking the participant's opinion on the easiness and confidence to remember the passwords created during the first session. Then, we presented one of the devices, in counterbalanced order, and requested the participant to try to log in 5 times, using the password created in the first session. Participants could use as many attempts as they needed to do that. After interacting with the device, we asked rating questions from the NASA Task Load Index (TLX) [75].

We then presented the second device to the participant and repeated the process. After participants interacted with both devices, we followed the NASA TLX procedure by

verbally explaining the workload factors from the NASA TLX, to ask the participant's source-of-workload evaluation. The evaluation included we verbally presenting pairs of the workload factors in randomized order (automatically generated by Qualtrics) and asking participants to choose, for each pair, the most important contributor for their workload while logging into the two devices in the second session.

We then asked final questions to participants, on how they perceived the usability of BendyPass, and where bend passwords could be applied, before finishing the session.

5.2.4 Analysis of Results

One research assistant transcribed participants' comments and answers to open-ended questions using Inqscribe [51]. One researcher performed qualitative analysis of open-ended questions in Microsoft Excel [71] and quantitative analysis of the multiple-choice answers and coded open-ended questions using R Studio [80]. Quantitative analysis included Wilcoxon Signed-Rank (Z) of numerical data, and chi-square tests (χ^2) of independence between variables with categorical data, but we focus on reporting significant results. We conducted the qualitative analysis using themes from the online survey results for online survey questions, and grounded theory [37] to code different themes that emerged for each new question. Whenever necessary, we coded answers in more than one theme, but we did not code unclear answers.

5.3 Interview Results

This section presents participants' demographics and their answer to the online survey questions. Overall, the results are similar to those of the online survey, and we will thus only point out relevant results.

5.3.1 Demographics

We recruited 18 adults with vision impairment. After running the two sessions with participant P1, we decided to consider him as a pilot participant, because of technical issues we had in both of his sessions, not previously identified in the pilot studies with sighted participants. Similarly, we had to discard data from participant P3, who had a condition in the nervous system, preventing pressure control in the hands, and consequently, the creation of a password on BendyPass.

From the other 16 participants, 10 declared they were blind, 5 declared they had low vision, and one declared to have another condition. As the participant who declared (P7) having another condition could not see the smartphone screen, we grouped him with the blind for our analysis. This resulted in 11 blind participants (68.7%) and 5 with low vision (31.2%), a distribution similar to the one from the online survey.

Most participants self-declared as males (N=10, 62.5%) and ages ranged from 22 to 76 years-old (*M*=54.31, SD=15.38). Besides being vision impaired, 3 participants reported having another impairment, related to hearing loss (N=2), attention (N=1) or psycho-motor system (N=1), according to the WHO classification [102].

Almost all participants said they use assistive apps on their smartphones (N=15, 93.8%). Only 5 participants said they use a Braille display, a smaller proportion than the one

found in the online survey (31.3% vs 42.5%). 3 participants had previous experience in user studies exploring deformable flexible devices, though never for user authentication.

5.3.2 Password Use

Interestingly, proportionally fewer participants of the user study rated passwords as important or very important (N=12, 75%) than participants of the online survey (96%). Proportionally more study participants than survey participants said they use password managers (N=6, 37.5% vs. 11.1%) and reuse of passwords (N=5, 31.3% vs. 9.2%), although the sample used in the user study is much smaller, possibly skewing the results.

Most participants said they were able (N=10) to protect their personal information, similarly to what we found in the online survey. However, different than survey participants, the second most commonly chosen answer was neutral (N=4), followed by very able (N=2).

As found in the online survey, almost two thirds of participants reported having concerns with entering passwords in public (N=11). From those, 3 said the reason was accessibility issues, not identified in the online survey (N=3). For example, P9 has concerns with debit card use, because “it is not clear how many times I have to press OK or when it is time to type the PIN. Sometimes, I have to ask people when […] to put the PIN in and then I can just hope that they look away.”

5.3.3 Perceptions on User Authentication Methods in Mobile Devices

As found in our online survey, most participants selected fingerprint as the most secure (N=9) and most accessible (N=13) user authentication method (Figure 19). However, PIN and voice recognition tied as the least secure method (N=5). PIN was chosen because of the small number of possible combinations and easiness to hack it (N=3), while voice recognition was chosen because of the easiness to mimic someone else’s voice (N=3).

5.3.4 Use of Smartphones and Authentication

All participants reported owning a smartphone, for an average of 8 years (*SD*=5.14). 12 participants reported using an iPhone. Also, 12 participants said they protect their smartphones with a user authentication method, for a percentage almost identical to the one found in the online survey (75% vs. 75.3%). Most said fingerprint is the method they most frequently used to unlock their mobile devices (N=10) (Figure 19). From the 4 participants who said they do not use a method to avoid unauthorized access to their smartphone, 2 said they want to allow their relatives to have easy access to their phones.

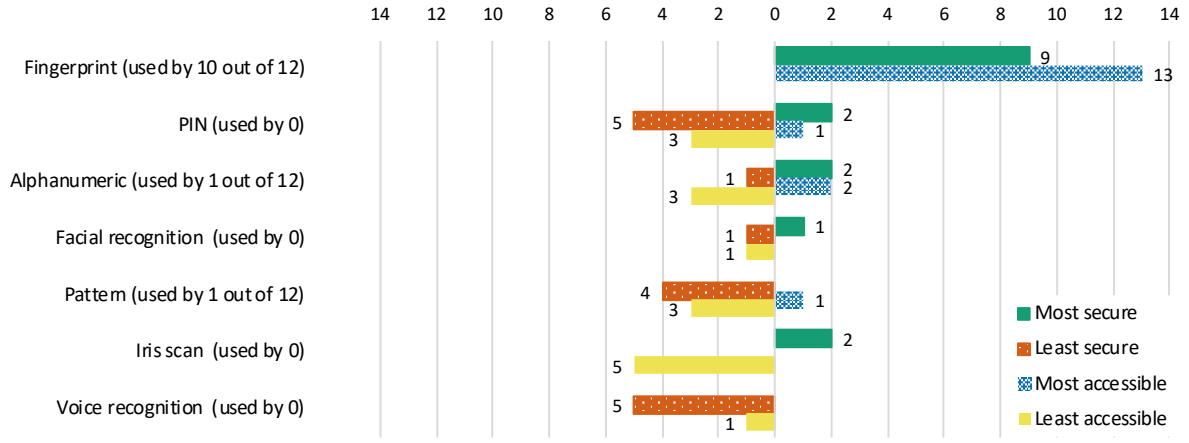

Figure 19: Study participants most used selections of most secure (green), most accessible (blue), least secure (red), and least accessible (yellow) user authentication methods.

5.3.5 Summary

Most results to the interview were similar to the answers collected in the online survey, confirming the participants of the user study represent well the group of people with vision impairment who have access to internet and mobile devices.

5.4 Password Results

We analyzed data from both sessions regarding the learnability and memorability of bend passwords when compared to PINs. Following the methodology used by Maqsood et al. [68], for session 1 we evaluated the composition of passwords, password creation time and number of trials required to create a memorable password. For session 2, we assessed success rates, login time and number of login trials.

All blind participants used the smartphone with the screen reader VoiceOver on. Only one participant with low vision used Screen Magnifier in both sessions of the study.

5.4.1 Session 1: Training

Before creating their passwords, participants trained to use the smartphone for an average time of 90s and trained bend gestures for an average time of 165s (Figure 20). A Wilcoxon Signed-Rank test found significant difference between the training time of bend passwords (*Md*=143.5s, *SD*=63.94s) and PINs (*Md*=91.5s, *SD*=30.92s) (Z= -2.97, $p < .005$). We also did not find significant differences between participants who were blind and participants who had low vision in their time training how to use bend passwords (not significant (*n.s.*)).

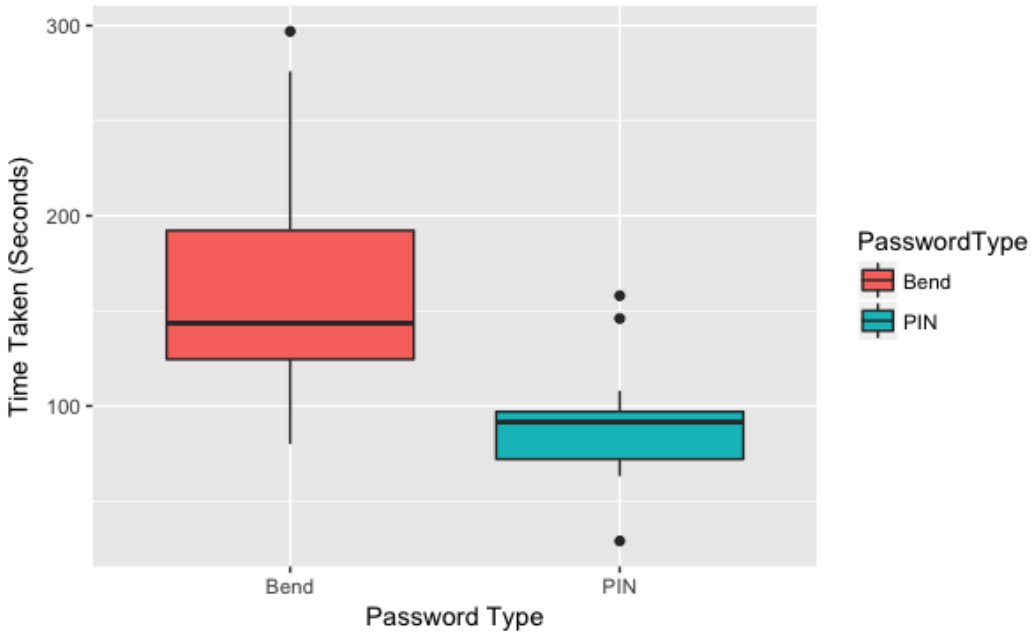

Figure 20: Training time, in seconds. Difference is statistically significant.

5.4.2 Session 1: Password Creation

When participants said they were ready to create their password, we asked them to create a new password both memorable, so we could use it in the session 2, and secure, with at least 6 gestures/digits. Participants took an average time of 59.6s to create their first bend password, and an average time of 48.8s to create their new PIN (Figure 21). Creation time includes time participants spent thinking about the passwords added to the time they took to enter their passwords. Compared to results from previous study [68] with sighted participants, time to create PINs was almost the same (48.8s vs 49s), while time to create bend passwords was longer (59.s vs 52s). We found no significant difference between the creation time of bend passwords and PINs (*n.s.*). We also did not find significant differences between participants who were blind and participants who had low vision in their time creating bend passwords on BendyPass (*n.s.*).

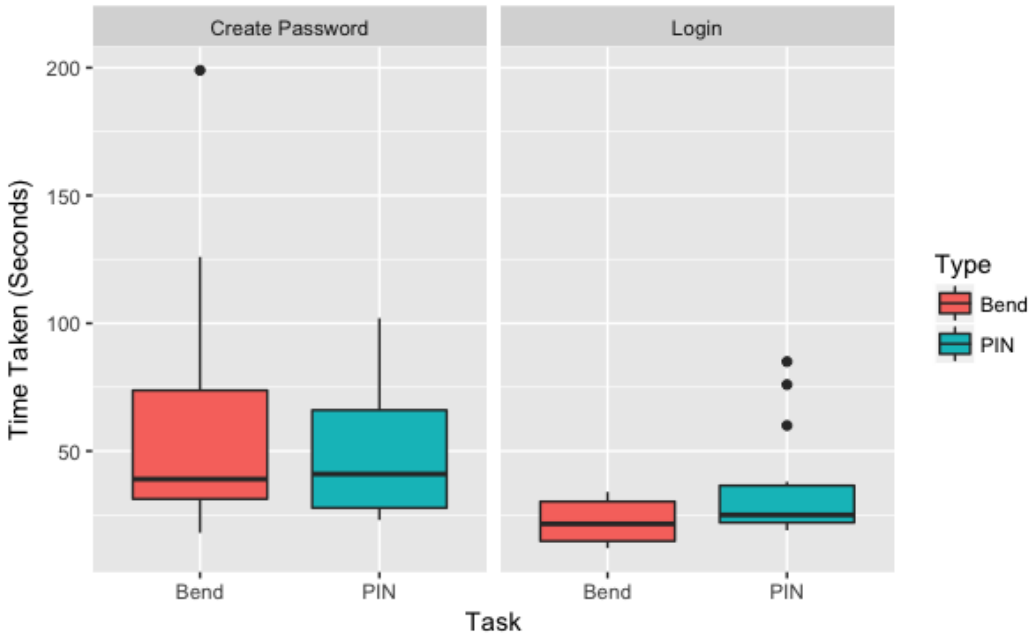

Figure 21: Creation and Login time in the first trial, in seconds. Differences are not statistically significant.

Similarly to what was found by Maqsood et al. [68], although participants in our study quickly created their first bend password, most did not remember their initial bend password. Whenever participants demonstrated being unsure about their passwords, while confirming or rehearsing them, we asked if they wanted to create a new one. 11 participants had to re-create their bend passwords, while only 2 had to re-create their PINs. We found a significant difference between the number of trials to create memorable bend passwords (M=1.94, Md=2, SD=1) and PINs (M=1.12, Md=1, SD=0.34) (Z= -2.36, p < .01).

From the 11 participants who forgot their initial bend password, 9 forgot it at the confirmation step (81.8%), and just 2 forgot it at the rehearsal step (18.2%). Technical issues with the prototype required 3 participants to recreate their bend passwords, but those trials were not considered in the results reported above, as they were not related to participants' memorability.

5.4.3 Session 1: Password Creation Strategies

We observed how participants created their passwords and analyzed the final passwords created. We also analyzed participants' answers on how they would rate the easiness to remember their passwords. Here we present a comparison between our observations and participants' answers. Table 4 shows the main strategies used.

Table 4: Strategies participants reported using to create memorable passwords. Numbers in parentheses express the number of observations of each strategy.

Strategies to create passwords	Bend passwords	PINs
Pattern	5 (9)	4 (9)
Simple	5 (3)	0 (2)
Repetition	0 (3)	2 (6)
Association	1	7
Good memory	1	2

For bend passwords, we observed more than half of the participants used some sort of pattern (N=9), including mirroring gestures from one side of the device to the other (N=5), shapes (N=2) and sequence of gestures in counterclockwise order (N=2). However, only 5 participants mentioned the use of patterns. We also observed that some participants reused the same gestures in their passwords (N=6), even consecutively repeating the same gesture more than once (N=3), but no participant mentioned the repetition as an attribute related to the memorability of their bend passwords. Some participants said they chose simple bend passwords (N=5), some said bend passwords are hard to remember (N=5) and some said bend passwords require more time for learning (N=5). Only one participant used good memory as a reason to be able to remember their bend password. The results we observed in our study are similar to those from the previous study with sighted participants, where patterns were the main strategy used by participants to remember their passwords (44%), followed by repeating gestures (16%) [68].

For PINs, we observed more than half of the participants used a pattern (N=9), although only 4 mentioned it. We also observed 8 participants used consecutive repetition of digits, but only 2 mentioned it. Additionally, 2 PINs created were simple, including only 2 or 3 different digits, but no participant mentioned the use of a simple PIN to make it memorable. Almost half of the participants mentioned using series of numbers they are familiar with in order to create their PINs, an association strategy for memorization (N=7).

5.4.4 Session 1: Password Characteristics

We analyzed the composition of passwords created by our participants. Table 5 shows the average length of passwords and the number of unique gestures or digits used, as well as their respective standard deviations. Both bend passwords and PINs ranged from 6 to 8 gestures/digits, but most were equal to the minimum length of 6 required from participants. We found no significant difference between the length of bend passwords and PINs (*n.s.*). Different than what was found by Maqsood et al. [68], our study participants used significantly more unique gestures in their passwords than unique digits in their PINs (Z= -1.95, p = .03).

Table 5: Password Characteristics. Unique entries are the number of unique digits and gestures in the bend password and PINs.

Password Type	Average Length M (SD)	Unique Entries M (SD)
Bend	6.44 (0.81)	5.81 (1.05)
PIN	6.19 (0.54)	4.69 (1.14)

Every bend gesture was used at least once by at least one participant to compose a bend password. However, some gestures were more frequently used than others. The top three most frequently used gestures were: top right corner up (17%), top left corner up (14%), bottom left corner up (12%), exactly the same top three single gestures for sighted

participants [66]. The least used gestures were top right corner down (6%), fold down (7%) and fold up (8%). Participants tended to prefer upward gestures (60.2%) than downward gestures (39.8%), even though the difference was not significant (*n.s.*), similar to what Maqsood [68] found. Our results confirm previous findings that gestures in the top area tend to be more preferable than those in the bottom area of the device [59, 64]. After analyzing the movements performed by participants, we believe the preference for up gestures is related to the fact that they can be activated by simply moving the index finger against the back of the corner to raise it. In contrast, down gestures tend to require not only the use of the index finger but also the thumb, which pressed the corner down.

5.4.5 Session 1: Password Confirmation

We requested participants to confirm their passwords 3 times after creating them, having as many attempts as they needed to complete the confirmation step. Whenever participants said they had forgotten their passwords or demonstrated being unsure about trying to confirm it, we asked whether they wanted to create their passwords again. Participants who created a new password had to go through the confirmation process again.

Following Maqsood's methodology [68], we selected the fastest confirmation time for each participant. Different than what was previously found [68], bend passwords were faster to confirm (M=15.6s, Md=14s, SD=4.19s) than PINs (M=20.6s, Md=17.5s, SD=9.43s) (Z= -2.27, p = .01). Bend passwords were faster to confirm than in prior work with sighted participants (15.6s vs 19s), while PINs were slower to confirm (20.6s vs 6s) [66]. However, participants had more incorrect attempts to confirm their bend passwords than to confirm their PINs for the three times. Not considering failed confirmation attempts due to either prototype errors or forgotten password that had to be re-created, participants made more

incorrect confirmation attempts for bend passwords (*M*=2.81, *Md*=2, *SD*=3.15) than for PINs (*M*=0.94, *Md*=0, *SD*=1.65), although the difference was not significant (*n.s.*).

Interestingly, P13 said that having to go through three confirmations probably makes passwords easier for people to remember, “engraving them into memory”, and suggested that this should be used more broadly.

5.4.6 Session 1: Password Rehearsal

Once participants completed the confirmation, participants had a pause when they answered questions about their perceptions on the memorability and security of their passwords. Then, we asked participants to rehearse their passwords by using as many attempts as they needed to complete 5 successful logins. In case participants forgot their passwords during the rehearsal step, we offered them the opportunity to create their passwords again. Participants who chose to create a new password during the rehearsal step had to immediately go through both the confirmation and rehearsal steps, without a pause for questions. As our pause only lasted a few minutes, we do not expect the lack of a pause caused any effect on our participants’ performance.

Following Maqsood’s methodology [68], we selected the fastest rehearsal time for each participant. Similar to what happened during confirmation, and different to what was found by Maqsood [68], bend passwords were faster to rehearse than PINs. We found significant difference between the rehearsal time of bend passwords (*M*=12.8s, *Md*=12s, *SD*=4.46s) and PINs (*M*=16.8s, *Md*=15s, *SD*=6.84s) (Z= -2.70, p = .003). Bend passwords were faster to rehearse than in prior work with sighted participants (12.8s vs 16s), while PINs were slower to confirm (16.8s vs 5s) [66]. Not considering failed confirmation attempts due to prototype errors, participants made slightly more incorrect rehearsal attempts for bend passwords than for PINs, but the difference was not significant (*n.s.*). All participants

remembered their PINs during the rehearsal step, and only 2 did not remember their bend passwords and had to create a new one.

We compared participants' fastest confirmation and rehearsal times to evaluate whether their performance improved with practice. Participants took less time to rehearse their passwords than to confirm them. Participants took significantly less time to rehearse their PINs than to confirm them (Z= -2.97, p = .001), as found by Maqsood [66]. Nonetheless, even though participants took less time to rehearse their bend passwords than to confirm them, the difference was not significant (*n.s.*), different to what Maqsood [66] found.

5.4.7 Session 2: Login

All participants returned about a week later for session 2. The number of days between the two sessions ranged from 7 to 10 (M=7.28, Md=7, SD=0.87). In the second session of our study, participants had as many attempts as they needed to complete 5 successful logins using the passwords created in the first session. Although 13 participants remembered their bend passwords, 1 participant (P14) was not able to enter it, due to prototype errors. Thus, participants' login success rate was 75% (N=12) for bend passwords and 93.8% for PINs (N=15). A McNemar test with the continuity correction found no significant difference between the success rate of bend passwords and PINs (*n.s.*). We also did not find significant difference between the number of days between sessions and the success rate of logging in with bend passwords (*n.s.*). The participant who forgot her PIN used a pattern, as well as 2 out of the 4 who could not log in with their bend passwords used a pattern, 1 used association to create the bend password and the remaining did not explain the strategy used to remember their passwords.

Not considering the trials in which participants could not log in due to prototype errors, most participants successfully entered their bend passwords (*M*=1.58, *Md*=1, *SD*=1.16) and PINs (*M*=1.27, *Md*=1, *SD*=0.8) in the first trial. A Wilcoxon Signed-Rank test found no significant difference between the number of tries participants took to successfully re-enter their bend passwords and PINs (*n.s.*). Participants took less time to complete a first log in with their bend passwords (*M*=22.4s, *Md*=21.5s, *SD*=8.48s) than with their PINs (*M*=35s, *Md*=25s, *SD*=21.25s), but a Wilcoxon Signed-Rank test found no significant difference between the first login time with bend passwords and PINs (*n.s.*), as shown in Figure 21. Bend passwords were faster to login than in prior work with sighted participants (22.4s vs 37s), while PINs were slower to confirm (35s vs 12s) [68].

We selected the fastest login time from each participant who was able to successfully login. As observed in the previous steps of the study, participants took significantly less time to log in using their bend passwords (*M*=13s, *Md*=12s, *SD*=3.1s) than using their PINs (*M*=18.27s, *Md*=16s, *SD*=7.71s) (*Z*= -2.20, *p* = .01).

We asked participants whether they used any strategies to remember their bend passwords. 4 out of 16 participants (25%) said they rehearsed their bend passwords in their heads throughout the week. While 11 participants (68.8%) said they thought about their passwords between sessions to fixate them in their memories, 7 (43.7%) said their methods to create their passwords were the main strategy used to memorize them and 2 (12.5%) said they did not use any strategy to memorize their passwords. Both participants who reported not using a strategy forgot their bend passwords and could not log in during session 2. The participants who forgot her PIN also reported not using a strategy to remember it.

Interestingly, one of the participants mentioned being concerned with how to store a bend password in case she used it in the future, because differently than alphanumeric and numeric passwords, it is not easy to write bend passwords down.

5.4.8 Summary

Due to their familiarity with PINs, participants used less time to train using the smartphone than BendyPass. However, bend passwords were significantly faster to confirm, rehearse and log in than PINs, a different result than what Maqsood [66] found in her study, although most of our participants used VoiceOver and the standard typing method, slower than how a sighted person uses a smartphone. Although participants significantly improved their performance with PINs between confirmation and rehearsal, we found that they did not improve as much with bend passwords, maybe due to their already quick times when confirming their bend passwords.

We found that the most common strategy participants used to try and remember passwords, for both PIN and bend, was creating a pattern, used by 9 participants each. 7 participants used association to create their PINs, while only 1 used it for bend passwords, possibly because the difficulty in creating an association between bend gestures and daily life things. We also found that all participants who did not use a strategy to remember their passwords forgot them for session 2. Finally, we observed participants made more mistakes entering bend passwords than PINs, but the difference was not significant.

5.5 Questionnaires Results

We asked participants to answer device-specific questions after interacting with them in both sessions, their workload while logging in to the devices and opinions about bend passwords.

5.5.1 Device Specific Questions

Participants verbally answered questions about each device used in the study, regarding the easiness to create passwords, the perceived security of both password schemes and their opinions about BendyPass and bend passwords, as shown in Figure 22. All questions were 10-point Likert scales, where 1 was the least favourable to bend passwords and 10 was the most favourable.

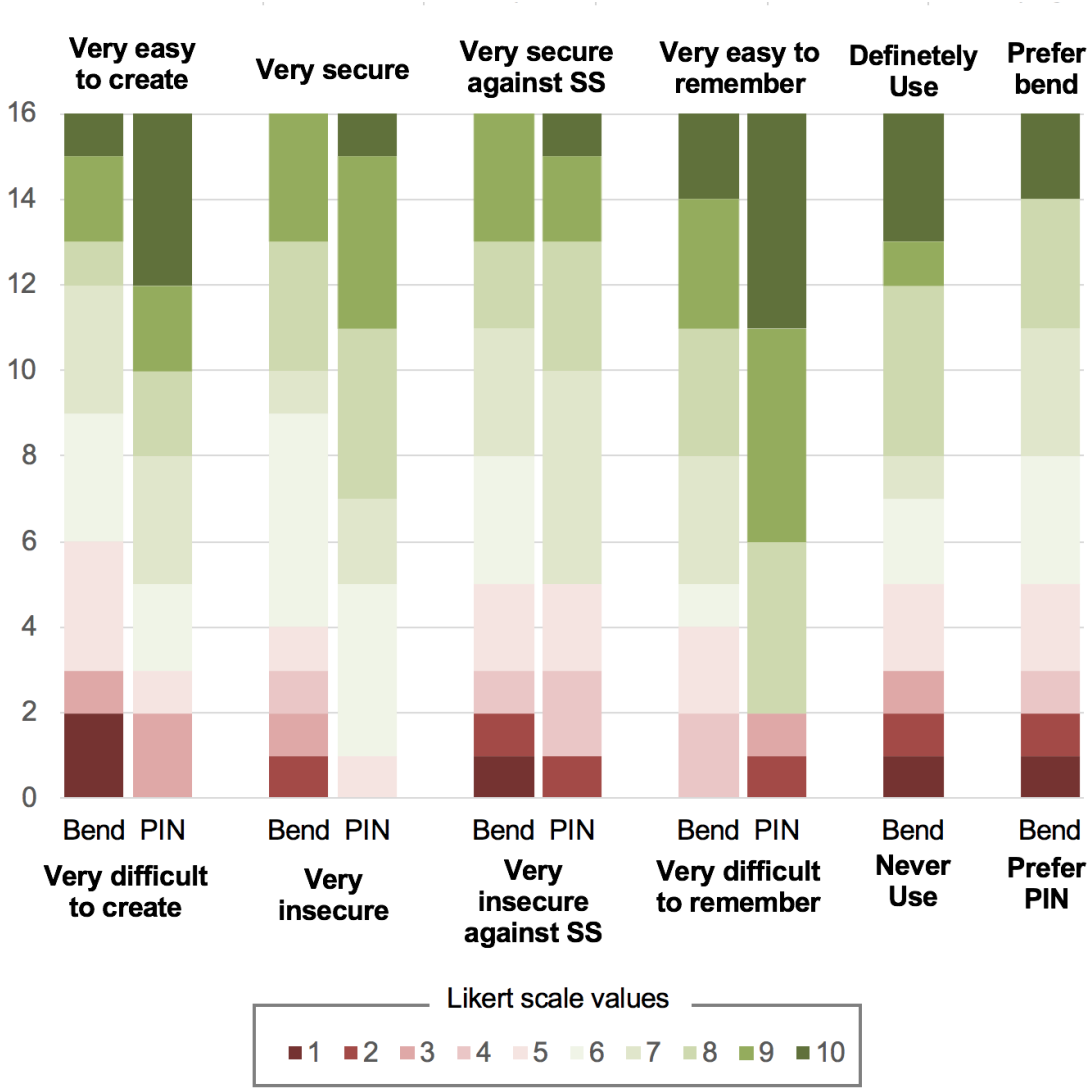

Figure 22: Distribution of Likert scale responses (*n.s.*) regarding easiness to create, easiness to remember, perceived security and likelihood of using bend passwords. First three distributions are from session 1, while the other three are from session 2.

Table 6 and Table 7 present the statistical analysis we generated with the responses collected. In session 1, participants rated bend passwords significantly harder to remember (*M*=6, *Md*=5.5, *SD*=2.66) than PINs (*M*=8.19, *Md*=8, *SD*=1.68) (*Z*= -1.88, *p* = .03). Nonetheless, their ratings for the same questions in session 2 for bend passwords and PINs were not significantly different (*n.s.*). P5 commented on that saying "It's fun but you have to suspend anything you know about passwords. You have to think in a new way."

Similarly, participants who were blind rated the easiness to remember bend passwords significantly lower (*M*=5.1, *Md*=5.0, *SD*=2.51) than participants who had low vision (*M*=8.0, *Md*=8, *SD*=1.87) (*Z*= -1.70, *p* = .04) in session 1 of our study. However, their ratings for bend passwords and PINs were not significantly different in session 2. We did not find other significant differences between participants who were blind and participants who had low vision.

Table 6: Likert scale responses for device-specific questions regarding easiness of use, easiness to remember and perceived security. Significant differences marked with *.

Question	Session	Bend Md (SD)	PIN Md (SD)	Stats
Ease of password creation	1	6.0 (2.62)	7.5 (2.33)	*Z*= -0.95, *p* = .17
Ease of remembering	1	5.5 (2.66)	8.0 (1.68)	***Z*= -1.88, *p* = .03***
	2	7.5 (1.98)	9.0 (2.38)	*Z*= -0.97, *p* = .17
Confidence in remembering	1	7.0 (2.47)	8.0 (1.89)	*Z*= -1.56, *p* = .06
	2	8.0 (1.89)	9.5 (2.68)	*Z*= -0.86, *p* = .20
Perceived overall security	1	6.0 (2.13)	8.0 (1.46)	*Z*= -1.40, *p* = .08
Security against shoulder surfing	1	6.5 (2.37)	7.0 (2.15)	*Z*= 0.68, *p* = .75

Comparing our results to those from Maqsood et al. [68], we observed a better perceived usability for bend passwords among vision-impaired participants than the researchers found among sighted participants, as sighted participants rated bend passwords significantly harder to create and significantly less secure than PINs. In our study, we found

no significant difference between the easiness to create and in the perceived security of bend passwords and PINs. However, we observed participants had difficulty understanding the difference between the questions about easiness to remember and their confidence to remember their passwords.

Participants' confidence to remember their passwords was affected by the number of errors made in session 1 during the rehearsal step of the study. Those who had fewer incorrect trials during rehearsal rated their confidence to remember significantly higher for bend passwords (χ^2 (24, N=16) = 36.98, p = .04) than for PINs (χ^2 (10, N=16) = 23.43, p = .009). Participants who were more confident in remembering their passwords before logging in during session 2 were significantly more likely to remember their bend passwords (χ^2 (6, N=16) = 85, p = .01) and their PINs (χ^2 (5, N=16) = 85, p = .007).

Interestingly, participants reported a slightly higher likelihood to use bend passwords in the first session than in the second session, although the results were not statistically significant either for the likelihood to use bend passwords if they were available (Z= -1.01, p = .35), or for using bend passwords versus PINs on flexible devices (Z= -1.01, p = .33).

When asked about their rating for easiness to create PINs on the smartphone, 10 participants mentioned their familiarity with creating PINs. With respect to their bend passwords, while 6 participants said bend passwords were hard to remember, 5 said they were easy to remember. A total of 5 participants pointed out that bend passwords require additional learning time.

The most common reasons for ratings regarding the easiness to remember their PINs were the use of association (N=7) and the use of patterns (N=4). On the other hand, no participants mentioned using association as a reason for their rated easiness to remember bend passwords, but 5 of them said they used patterns, while another 5 said they created easy bend passwords to increase their chances of remembering. Participants' methods to

create their PINs was the most common reason for their confidence level on remembering them (N=8), followed by having a good memory (N=4). Similarly, 4 participants said their methods to create their bend passwords were the reason for their confidence on remembering.

Interestingly, when we asked participants to justify their ratings for the overall security of their PINs, 5 said they chose hard to guess PINs, while another 5 said their PINs were easy to guess. The most common answer participants gave for their ratings on the security of PINs against shoulder surfing attacks related to PINs being easy to see by others (N=5). This was also one of the most common reasons participants gave for their ratings on the overall security of bend passwords (N=5), although other participants said bend passwords were difficult to see (N=4). The concern of bend passwords being easy for others to see was the most common reason for participants' ratings on the security of bend passwords against shoulder surfing attacks (N=7).

We also asked participants to explain their ratings for their likelihood to use bend passwords. The most common disadvantage participants mentioned was having to carry an additional device (N=6), while the most common advantage was considering bend passwords secure (N=4).

Table 7: Likert scale responses for device-specific questions regarding likelihood of using bend passwords.

Question	Session	Bend Md (SD)
Likelihood to use if available	1	7.5 (2.83)
Likelihood to use if available	2	6.5 (2.69)
Likelihood to use instead of PINs in flexible devices	1	6.5 (2.49)
Likelihood to use instead of PINs in flexible devices	2	5.5 (2.53)

At the end of session 2, we also asked participants to describe their experiences using BendyPass. After coding all answers, we found that 9 of them described positive

experiences, 4 described having a neutral experience and only 3 described a negative experience.

Participant P4, for example, said it was “fun, interesting, challenging, intriguing”, while P8 said, “it was easy, [there is] a little of learning curve to know how to do the bends right, but once you got that it’s easy to use, even easier than swiping the touch screen to find numbers.” P7, on the other hand, said, “if errors were removed, it would be OK. Primary reason for negative comments are the errors and the fact that the surface should be more rigid in some places to be more responsive.” The errors mentioned by the participants involved derecognition of gestures performed or the recognition of opposite gestures. For example, sometimes “Top right corner down” was recognized instead as “Top right corner up”. A possible reason for that is how flex sensors work. As their resistance is influenced not only by bending but also by pressure, when participants gripped a corner too firmly with their thumbs and indexes, the resistance rose as it would for an up gesture.

5.5.2 Typing Method Used on Smartphones

We asked participants what typing style they most commonly use in their smartphones. 5 said they use Standard Typing, the method used during the study, 7 said they use Touch Typing, where the user explores the screen and lifts up his/her finger to activate a key, and 2 said they use Direct Touch Typing, which works similarly to Touch Typing but also allows the user to activate keys by directly touching them. This might have impacted their timing typing PINs on the smartphone.

5.5.3 Workload Rating Questions

After participants interacted with each device in session 2, we verbally asked them Workload Rating questions from the NASA-TLX Rating Sheet [104]. Questions were 21-point Likert

scales (starting at 0), and the only question where we inverted the scale while posing the question to participants was the one related to Performance, a common practice according to Cain [32]. We asked participants to rate their performance in a scale from 0 to 20, where 0 was a failure and 20 was perfect, to be consistent with the scale of the other questions. Even though we made this change to facilitate participants to verbally answer, all answers were converted back to the original scale before we performed any further analysis.

Once participants interacted with both devices in session 2, we asked them to choose, from each random pair of factors, the most important contributors to their workload while completing the login in both the smartphone and BendyPass. We used this information to determine the Source of Load Weights.

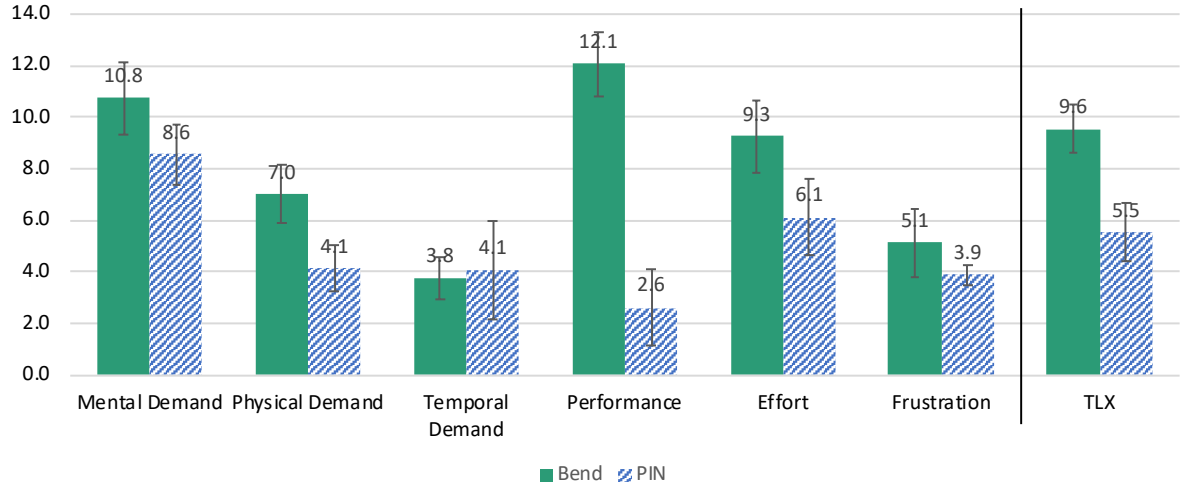

Figure 23: The mean results of the NASA-TLX Workload Ratings and the mean final TLX Score.

Figure 23 shows the workload ratings from all 16 participants, including the final TLX score. Overall, participants' task load during login was significantly higher with bend passwords (*M*=9.6, *Md*=8, *SD*=3.85) than with PINs (*M*=5.5, *Md*=5.2, *SD*=4.48) (*Z*= -3.01, *p* = .001). This result is a function of how participants felt about their performance while logging in, as their weighted performance was significantly worse with bend passwords

(*M*=12.1, *Md*=15, *SD*=7.68) than with PINs (*M*=2.6, *Md*=0.5, *SD*=5.02) (*Z*= -2.09, *p* = .02). All other weighted workload factors were not significantly different between the two conditions.

5.5.4 Applications Areas for Bend Passwords

We listed 7 places where bend passwords could be used, based on Maqsood et al. [68], and asked participants whether they thought bend passwords could be applied to those (Figure 24). Almost all participants agreed opening house doors was a good application for bend passwords (N=15), but 2 participants said opening a front door with bend passwords in the Canadian winter could be a problem, because of the exposure to the cold weather both of electronic components, and the user, who would take additional time to unlock the door. Similarly, 13 participants considered bend passwords appropriate for accessing social media and accessing email, but participant P4 said that accessing social media or email would not be interesting for him, as he uses a password management system in his computer. However, using password managers did not affect the likelihood of participants to use bend passwords to unlock their accounts (*Z*= 0.64, *p* = .74).

Additionally, 12 participants agreed bend passwords could be used in ATMs. P6 and P17 said that, even though BendyPass only had 10 possible bend gestures, they felt it was safer than a PIN. In contrast, P11 said it would be hard to cover your hand when using BendyPass so others could see your password, and participant P5 shared a concern with using BendyPass in ATMs, due to the risk of shoulder surfing attacks.

We also asked whether participants had other ideas of applications for bend passwords. 5 participants suggested using them in lockers, and 4 to use home security systems, for example (Figure 24).

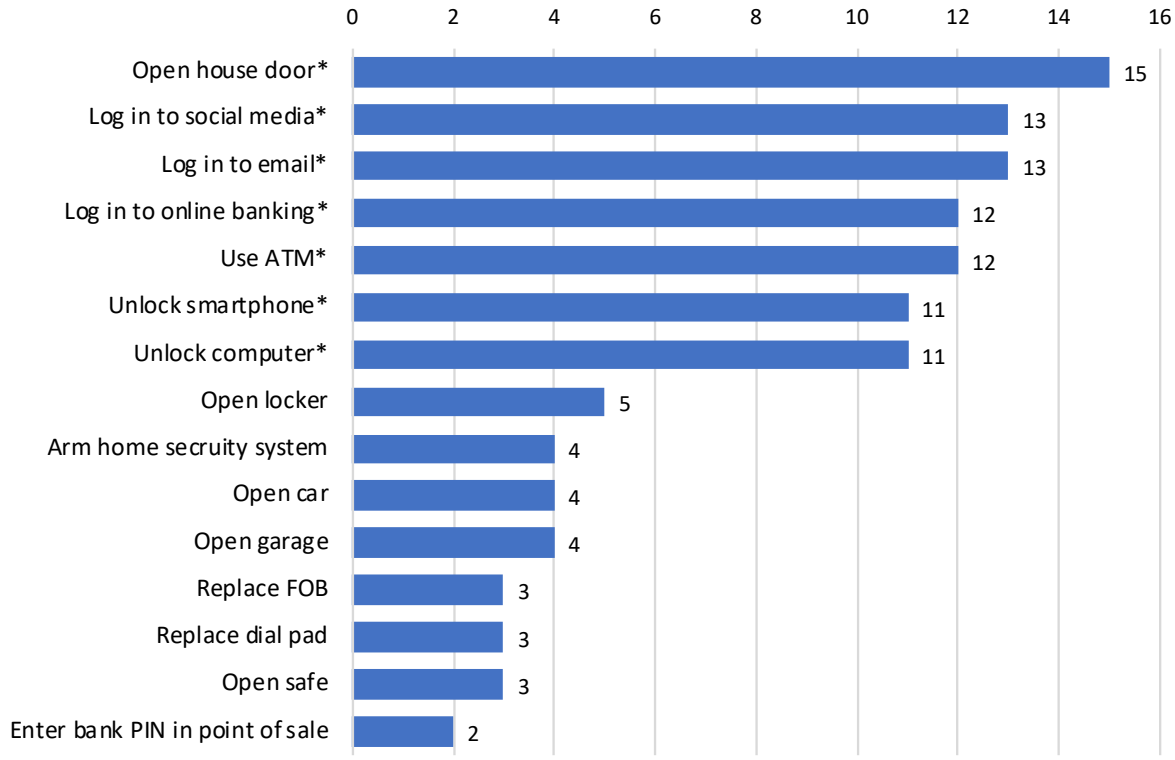

Figure 24: Potential application areas for bend passwords, ranked by the number of participants. Items suggested to participants are marked with *.

To have a better understanding of how likely participants would be to use bend passwords for different applications, we asked 10-point Likert scale questions for some of the possible application areas. The distribution of answers is shown in Figure 25. 10 participants would be somewhat likely to use bend passwords for unlocking accounts on their personal devices, and 10 for opening house doors. However, unlocking flexible devices would be the application participants would be more likely to use with bend passwords (N=12), for which 8 participants rated 9 or 10, where 10 meant very likely to use.

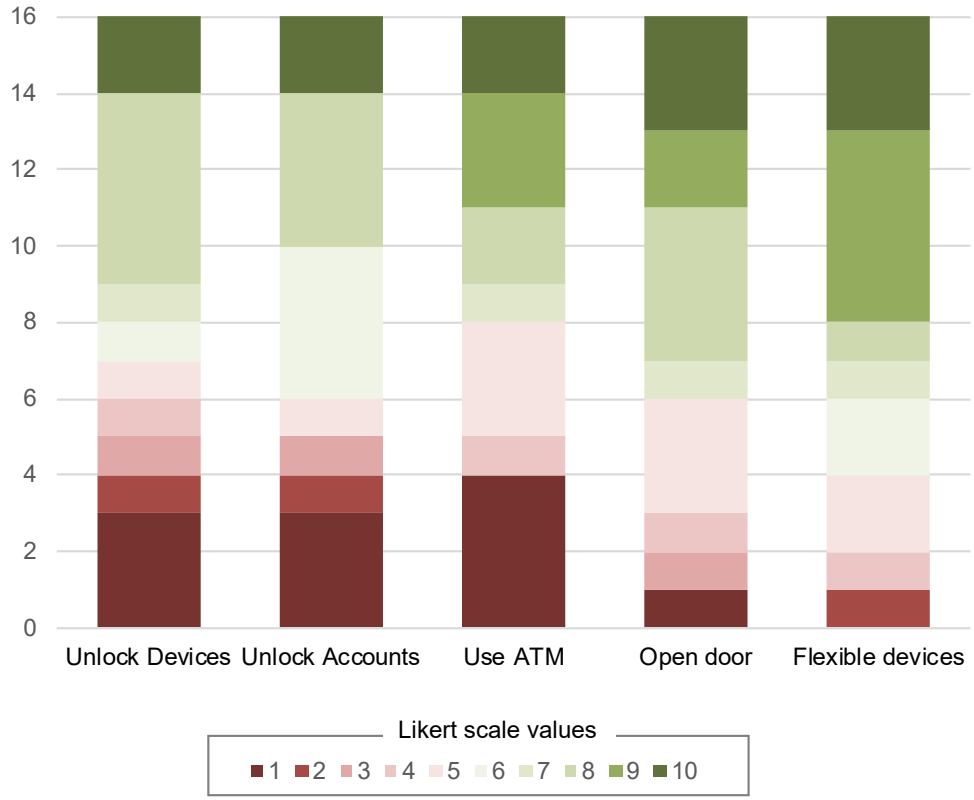

Figure 25: Distribution of Likert scale responses regarding likelihood of using bend passwords for specific applications.

5.5.5 Final Questions

At the end of both sessions, we asked participants to point out characteristics they liked or worked well in BendyPass and the bend password system, as well as aspects they consider should be improved. We coded participants' answers and combined the results from both sessions. Figure 26 shows the most commonly mentioned positive aspects of BendyPass and bend passwords, while Figure 27 shows the aspects for improvement most frequently suggested by participants.

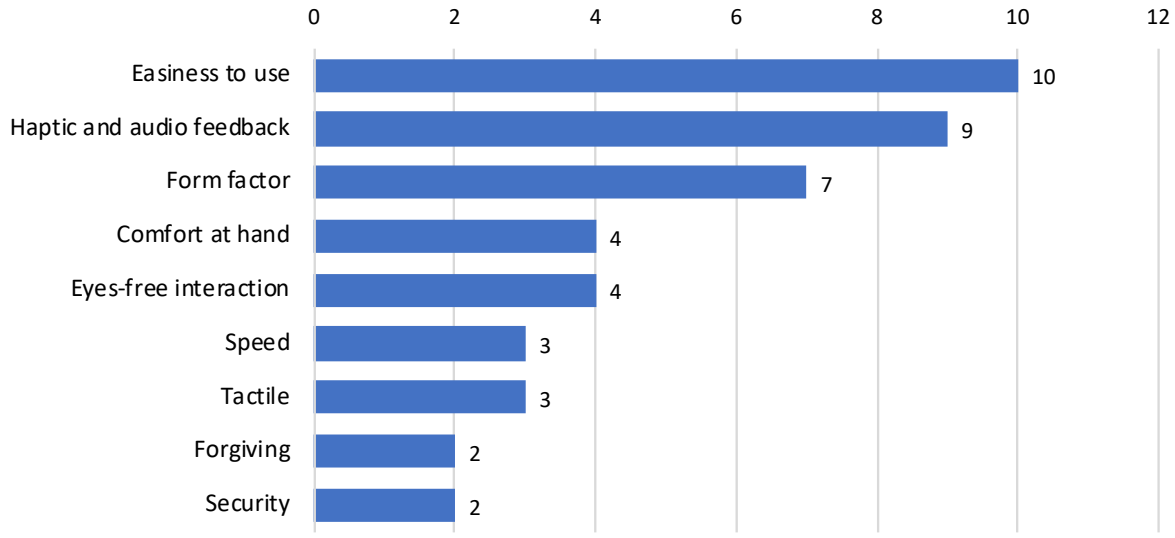

Figure 26: Most positive aspects of BendyPass and the bend password system, ranked by number of participants who mentioned them.

Although more than half of the participants liked the audio feedback provided by BendyPass, participant P17 suggested it could use tones, instead, because he "hate[s] numerical password because it speaks it out." Also, some participants were resolute in terms of not using bend passwords if that would require the use of an extra device. P7, for example, said, "I don't like carrying extra things, I barely remember my charging cable." P16 also mentioned that bend passwords could be to online banking and ATM "if the bank could give you a bendable card."

Interestingly, even though 7 participants liked the form factor of BendyPass, 8 suggested the reduction of the device size, even mentioning it would be nice to have it as a keychain. Participant P17, for example, said, "the smaller it is, more people would catch up with it [start using it]." During the course of the two sessions, at least 3 participants also mentioned the possibility of using BendyPass without audio feedback. P11, for example, said this would make the use of the device more discreet, as no one would hear it.

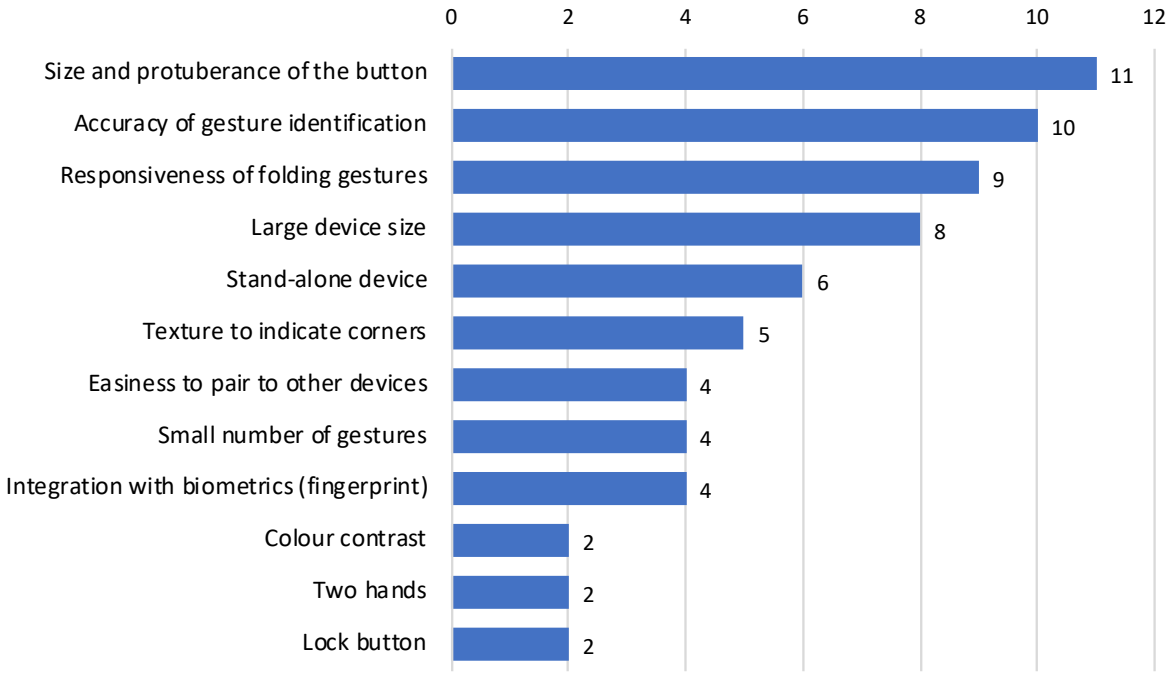

Figure 27: Aspects for improving BendyPass and the bend password system, ranked by number of participants who mentioned them.

When asked who might like to use bend passwords, 12 out of 16 participants said vision-impaired people in general. P5 said, “Certainly blind and low vision, or people with learning disabilities that make them have issues with numbers and seniors or people with learning issues.”

5.5.6 Summary

Bend passwords were perceived as easy to create and remember and as secure as PINs, indicating potential for bend passwords to be used in replacement of PINs. Additionally, more than half of our participants said they had a positive experience using BendyPass (N=9). Using BendyPass for login posed a significantly higher workload to participants than using the smartphone, exclusively due to participants’ perceived lower performance when logging in with BendyPass. The application where participants would be more likely to use

bend passwords is unlocking flexible devices (N=12), followed by opening the door of their houses and unlocking their accounts (N=10 each). However, 6 participants mentioned their likelihood to use bend passwords was influenced by the fact BendyPass would require them to carry an additional device.

Most participants considered BendyPass easy to use (N=10) and liked its haptic and audio feedback (N=9), while most suggested reducing the protuberance of the button (N=11) and improving the accuracy of the bend password recognition (N=10), especially for folding gestures (N=9).

5.6 Discussion

We presented the results of a user study on bend passwords compared to PINs with 16 participants who were blind or had low vision. We found that bend passwords were as easy to create as PINs, and participants assessed them as easy to remember as PINs. Participants reported being more likely to use bend passwords on a flexible device but would also be willing to use them as a separate device for opening the front door of a house or accessing accounts on their personal devices.

5.6.1 Learnability of Bend Passwords

Our results show PINs were not significantly faster to create than bend passwords, as found by Maqsood et al. [68]. Thus, we reject our first hypothesis **H1**, because PINs were as fast to create as bend passwords. Additionally, bend passwords were as hard to create as PINs.

We took around 2 minutes to explain to participants how to use BendyPass, confirming the findings of Schwesig et al. [84] that participants are able to quickly

understand how to interact with deformable devices. Participants took significantly more time training with BendyPass than with the smartphone, because of their previous familiarity with touch screens. But creating a password with BendyPass did not take significantly longer with the smartphone, showing how quickly participants learned how to use it.

5.6.2 Learnability for Blind vs Low Vision

We did not find significant differences between the time participants who were blind and participants who had low vision, neither to train how to use bend passwords nor to create a bend password. Thus, we reject our hypothesis **H2**, as participants with low vision were not impacted by the lack of vision feedback from BendyPass. This demonstrates that people with low vision can also benefit from a tactile password input method such as bend passwords on BendyPass, as much as people who are blind.

5.6.3 Memorability of Bend Passwords

Participants forgot their bend passwords significantly more often than their PINs, having to re-create their passwords on average 1.9 times. The fact participants forgot bend passwords relates to their potential unfamiliarity memorizing gestures compared to their experience memorizing the ubiquitous sequences of numbers. That is an indicative of the initial difficulty to memorize bend passwords, proven by participants' ratings during the first session on the easiness to remember bend passwords, significantly worse than PINs.

However, participants rated bend passwords as easy to remember as PINs in session 2. This finding is also supported by the success rates and the number of attempts participants took to complete the first successful login, which were not significantly different than those for PINs. Thus, we confirm our hypothesis **H3,** because bend passwords were as easy to memorize as PINs, potentially because of the use of the "muscle memory".

5.6.4 Easiness to Enter Bend Passwords

We found that entering bend passwords posed a significantly higher workload to participants than entering PINs, although this result was influenced by how participants perceived their performance when entering bend passwords, a novel user authentication method for them. We also found that bend passwords were significantly faster to login in session 2 than PINs. Thus, we reject our hypothesis **H4**, as PINs were not faster to enter than bend passwords, as found by Maqsood et al. [68]. Our findings are mainly due to the fact that our participants, who were blind or had low vision, used the smartphone with accessibility features, which slowed them down. In fact, being slow to enter is actually one of the things users dislike about PINs, as previously found [29].

5.6.5 Potential Applications for Bend Passwords

Most participants not only believed bend passwords have potential but also said they were likely to use bend passwords for: unlocking personal devices, unlocking accounts such as email and social media in personal devices, and opening the front door of houses. Interestingly, we found that half of our participants would be likely to use bend passwords in ATMs, and some suggested its use in points of sale and lockers, probably indicating accessibility issues in those contexts of use. Additionally, bend passwords were perceived as secure as PINs against shoulder surfing attacks, reinforcing its potential to replace PINs.

5.6.6 Study Participants

The answers our study participants gave for our interview questions were similar to those of our online survey participants. Considering that the Ottawa office of the Canadian Council of

the Blind helped us with the recruitment of the study as well as with the distribution of the online survey, the same participants may have answered both questionnaires. However, these may account for at most 5% of the online answers. As such, the similarities are mainly indicative that the group recruited for the user study well represented the group who answered the online survey.

Similar to our online survey, we recruited more blind than low vision participants. This might be a result of a higher interest of the blind community in novel assistive technologies but might also be an indicative of the difficulty in classifying some people as blind or low vision. For example, one of our participants self-declared as blind, but said he uses inverted colours on his smartphone to better see the screen.

Comparing the results from our online survey and our study, we found that proportionally more study participants reported using password managers as a strategy to remember their passwords. That could mean our study participants are more knowledgeable in digital security. However, as we also found more study participants admitted reusing passwords, we believe the differences in our results might be related to the way the questions were posed, as study participants were asked verbally and probably felt more comfortable and open to share their strategies with the researcher.

5.7 Limitations

Although we tested our prototypes before starting the study, including through 3 pilot sessions, we identified limitations on them along the course of the study sessions, which could limit our ability to compare bend passwords with PINs. We also had some limitations in the organization of our study.

5.7.1 BendyPass Limitations

Some bend gestures were not recognized in the first attempt, gestures that took too long to be released were recognized as two gestures in sequence, movements in the internal sensors caused bend gestures to be recognized in the wrong direction (up gesture recognized as down gesture), and issues with the button wiring caused Backspace to be triggered instead of Enter. On the first day of study sessions, we noticed participants were keeping the Enter pressed for longer than a second, triggering the Enter in the computer twice. That caused the following screen to be confirmed before the participant entered a password, returning an audio message saying, “Wrong password. Please try again.” We solved this issue by changing the gesture recognition program not to accept two Enter keys in a row. However, we acknowledge session 1 of 3 participants were impacted by this issue.

5.7.2 Smartphone App Limitations

Although we used a commercial app to simulate the PIN entry screen, we also found a number of limitations in it. First, the app did not work with any typing style other than the standard typing, used by only 5 of our participants in their own smartphones. That might have affected the time participants took to enter passwords on the smartphone.
Participant P9 said standard typing is the typing method new users commonly used, while participant P7 mentioned he would have been able to enter PINs two times faster in the smartphone if touch typing was available, although we were not able to test that. Although we acknowledge both the app keypad and the typing method in our study are not equal to those the majority of our participants use in their own smartphones, the process of learning how to use the app to create PINs simulated well what new users have to go through when using a new device.

The erase button was not labelled and was read as “button” by the screen reader VoiceOver. In the first session with participant P4, who is an accessibility instructor, he showed the researcher how to label buttons using VoiceOver, and he labelled the button to read “Backspace”. Consequently, participant P2 who had a session before that used the smartphone without the button label.

Additionally, app keys did not consistently blink to indicate activation, lacking a clear feedback for participants not using screen reader. Participant P5 who has low vision tried to use the smartphone without VoiceOver but decided to use VoiceOver after noticing the lack of proper visual feedback, added to the lack of audio feedback. Participant P7, on the other hand, wanted to use the smartphone with inverted colours, but the app did not present a good contrast ratio, as shown in Figure 28.

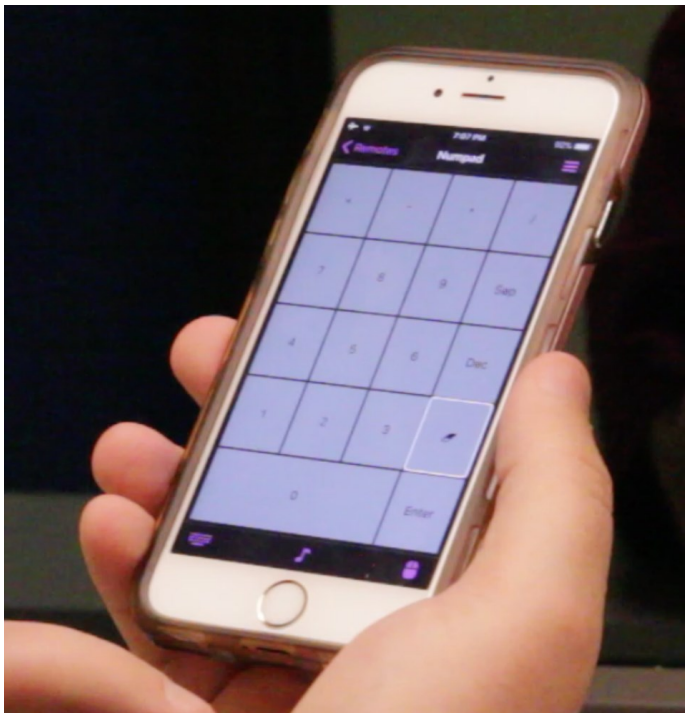

Figure 28: Smartphone with the accessibility feature of inverted colours on.

Another issue with the app mentioned by participant P14, who has low vision, was the font size and style. She said the keypad numbers should be bigger and bolder and their

colours should be brighter and have a better contrast. Also, participant P15 had initial difficulties while using the smartphone, because the 3D touch feature was active, allowing the activation of different controls when applying pressure to the screen. We changed the settings of the smartphone to disable 3D touch during the first session, and participants who tested after that used the smartphone without this function. Moreover, the size and proximity of the keys on the app proved to be an issue for participants P12 and P13, who mentioned having to stretch their fingers to be able to hit the digits.

We also found that the use of screen magnifier on the smartphone was not completely accessible. Although the screen magnifier on the iPhone enlarged a screen area, it requires the manipulation of a small handle, as shown in Figure 29. Participant P6, who used the smartphone with the screen magnifier on, mentioned how effortful was to find and move the handle around the screen.

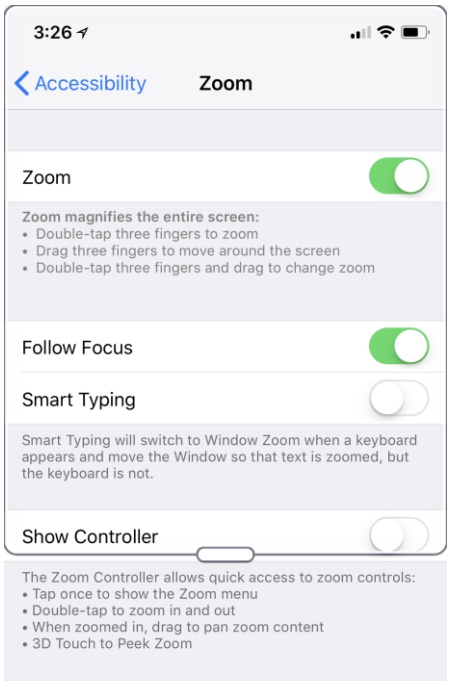

Figure 29: Screen magnifier box, with the handle in the bottom centre.

5.7.3 Study Limitations

We did plan to have an option to provide feedback in terms of the numbers of digits or characters already entered in a password, or whether the password field was empty or not after using the backspace button. This might have affected entering passwords with either the smartphone and BendyPass.

We used the NASA-TLX test to gather information about the workload imposed on participants when entering their passwords on the smartphone and the prototype. However, posing ratings questions with a large scale verbally showed to be far from ideal. We also integrated questions from the previous study which had 10-point Likert scales and questions from our online survey, which had 5-point Likert scales, potentially confusing participants. Additionally, only one researcher completed the data analysis and may therefore possess bias towards her single perspective.

5.8 Conclusion

We proposed the application of a tactile user authentication method [68] for people with vision impairment using bend passwords on a deformable flexible prototype called BendyPass. We conducted a user study with people who are blind or have low vision to evaluate the learnability and memorability of bend passwords on BendyPass when compared to PINs on a touch-screen smartphone. We found that bend passwords were as easy to learn and to memorize as PINs and were also rated as secure as PINs. We also found that bend passwords are significantly faster to enter than PINs on a touch screen using screen reader VoiceOver and the standard typing method of exploring the screen and double tapping the screen once the target is located. Our findings indicate potential for bend

passwords not only on mobile devices, but also for logging into personal accounts personal devices and for using ATMs.

We envision BendyPass can be paired via Bluetooth to personal devices or can be connected via USB cable to public computers or to ATMs, to allow users to have a unique point of entry for passwords. Additionally, when flexible smartphones are available in the future, bend passwords can even be entered directly in the smartphones. Even though we designed BendyPass for people with vision impairment, we believe it can also be used by people with dexterity impairments, as it does not require precise selection of items. It can also be useful for people with learning disabilities because it allows users to use their "muscle memory" to remember passwords. Additionally, it can be even used by people without disabilities, as an eyes-free method to unlock devices and access accounts without having to look at the device when holding it with both hands, similarly to what was previously proposed [68].

6 Design Recommendations

Considering the results of our study, we suggest design recommendations for new user authentication methods and deformable flexible devices for people with vision impairment.

6.1 Use Simple Interaction

Complexity in user authentication methods is one of the reasons some people with vision impairment decide not to protect their mobile devices against unauthorized access. Thus, we recommend the design of simple interactions, that can be easily taught verbally and experimented with in a safe environment. For example, our folding gestures were not as successful as our corner gestures, potentially because they were not as simple and clear as the corner gestures. A good guideline for designing simple interactions is evaluating how easy to explain a gesture is. Gestures that require additional clarification or are ambiguous might cause confusion and make learnability and memorability more difficult, so designers should thrive for the design of gestures that easily become intuitive.

6.2 Use Discreet Interaction

Considering people with vision impairment are concerned with the risk of shoulder surfing attacks, we recommend interactions to be designed to be discreet, to avoid others to easily see the gestures performed and to make vision-impaired users more confident with the security of the user authentication method. For example, folding gestures require more effort

to be executed and can be more easily seen than bending corners, so we recommend the design of devices that could register smaller bend gestures to be both easier to perform and most secure against shoulder surfing attacks.

6.3 Guide the Learning Process

During our user study, we noticed participants quickly learned how to use BendyPass and create bend passwords. We attribute this not only to the simplicity of the device and the interactions we designed, but also to the training we gave participants and to the audio feedback we provided them. This combination allowed users to learn what to expect after each gesture was performed, as recommended by Fares et al. [43]. Thus, we suggest that designers create a guiding system to support the learning of new interactions, via an audio or video guide that:

1. Says where the bendable areas are and how to recognize them (by relying on tactile indicators embedded on device's surface).
2. Indicates how to interact with bendable areas.
3. Provides audio feedback when a bend gesture is recognized, textually informing the name of the gesture.

Additionally, we suggest considering the use of training modes where users can try gestures and get audio feedback, without committing to creating passwords yet.

6.4 Provide Non-Visual Feedback

Both for helping users to learn how to perform gestures and notice when gestures are recognized by the recognition program, it is essential to provide users with feedback, preferably through more than one channel, such as audio and haptic feedback. Additionally, provide users with the option to turn on or off each feedback type, so they can choose, for example, to stop the audio feedback to make bend passwords more discreet. Thus, we recommend new deformable flexible devices to provide non-visual feedback on multiple channels and allow their individual activation.

6.5 Provide Clear Information About the System State

We recommend new user authentication methods to allow for a non-visual identification of the system state (if the user is in the password field, whether the field is empty or how many characters are inputted). One alternative is having a button or gesture to receive audio feedback, either in the form of a textual message or a sound tone. For example, squeezing the device could trigger the system state function, which would play a message saying “Password field: empty” or “Password field: 5 characters entered” or a sequence of tones, one per character entered. Another option is having raised dots on the deformable flexible device, one for each character entered, so users can feel how many characters they have already entered for a password.

6.6 Integrate to Existing Devices

People who are blind and even those who have low vision usually navigate the physical space by using white canes or holding guide dog leashes [6]. Additionally, most use smartphones as an aggregating assistive device, so it is common for them to carry their smartphones in their hands when walking around. Thus, a new user authentication device method would be more convenient for them if it is integrated in their existing devices, such as a deformable phone case with flexible corners or a keychain attached to their smartphone or white cane.

6.7 Make Set Up Easy

In addition to designing easy interaction, we believe the easiness to set up a user authentication might also influence users' motivation to use it. Thus, we recommend user authentication to be easily accessible in setting menus and simple to set up.

7 Conclusion and Future Work

This thesis explored the intersection of usability, security and accessibility for people with vision impairment, by running an online survey and a user study with vision-impaired participants regarding user authentication methods on mobile devices. In this chapter, we present our conclusion and suggest future work in the area.

7.1 Conclusion

We found from our online survey that most people with vision impairment are concerned with entering their passwords in public due to the risk of shoulder surfing attacks, most consider passwords important for protecting their personal information, but about a third do not use a user authentication method to avoid unauthorized access to their smartphones. We also found PIN is considered the least secure and one of the least accessible user authentication methods for mobile devices, although it is the most commonly used in smartphones. Our conclusion with our online survey is that 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 [29].

We designed a new deformable flexible device called BendyPass for people with vision impairment to enter bend passwords based on the survey conclusion and on prior work [41, 68]. In our user study, we compared bend passwords on BendyPass with PINs on a touch-screen smartphone. We found the learnability and memorability of bend passwords is comparable to those of PINs. Bend passwords are also perceived as secure as PINs. Bend passwords were significantly faster to enter than PINs on a touch screen, although we

recognized the typing method used in our study is slower than more advanced typing methods. Our findings indicate potential for bend passwords not only for mobile devices, but also for logging into personal accounts in personal devices and for using ATMs.

We attribute the success of our project to involving vision-impaired experts to pilot the online survey and provide early feedback on the suggested designs before starting the study. Also, we recruited participants with vision impairment, both for our online survey and for our user study, instead of collecting data from sighted people or using blindfolded participants to evaluate our prototype. This way, we were able to get more realistic results on how people with vision impairment deal with passwords on mobile devices, and how usable bend passwords are for them.

Thus, our research project answered the overarching question regarding how usable bend passwords are for people with vision impairment by finding that bend passwords are as easy to create and to remember as PINs, but are faster to enter than PINs for people with vision impairment.

Our work was the first to extensively explore the relationship people with vision impairment have with passwords and user authentication methods on mobile devices. Through our online survey, we contribute to the body of knowledge by providing: 1) the main challenges faced by people with vision impairment when dealing with passwords, including accessibility issues they have with existing user authentication methods; 2) insights on how people with vision impairment perceive different user authentication methods, for example the methods they feel are more secure and least secure; 3) a comparison between people who are blind and people who have low vision regarding digital security, which resulted in very similar results except the least accessible user authentication method for them.

Additionally, our user study was the first to explore the use of bend gestures on deformable devices as a password input method, contributing with: 1) The design and fabrication of a new deformable prototype for password input; explained in Chapter 4; 2)

insights on bend passwords including that they are as easy to learn and as easy to memorize as PINs for people with vision impairment when; 3) potential applications for bend passwords, such as a universal password entry device for unlocking personal accounts; 4) design recommendations for new deformable devices described in Chapter 6.

7.2 Future Work

Future work will include improvements on the prototype, investigation of other application areas for BendyPass, and user studies on different contexts of use for people with vision impairment. We intend to improve the prototype by increasing the accuracy of the bend password recognition program, developing a method to provide clear feedback on the system status, defining sounds to be used as an alternate audio feedback, improving or replacing folding gestures, and experimenting with new device shapes and sizes, such as smartphone cases or keychains. We plan to evaluate other application areas for BendyPass, for example in ATMs, points of sales and bank tellers, by running user studies on different contexts of use. Finally, we plan to evaluate the usability of BendyPass for other groups of people, with different abilities.

Appendices

Appendix A: Online Survey

A.1 Consent Form for Online Survey

Research Title: Exploring the learnability and usability of bend gestures for the visually impaired.

Funding Source: National Sciences and Engineering Research Council of Canada (NSERC) through a Discovery Grant (RGPIN-2017-06300).

Date of ethics clearance: November 8, 2017.

Ethics Clearance for the Collection of Data Expires: November 30, 2018.

Please provide your consent to participate in this online survey.

This survey aims to explore the use of passwords in personal devices by visually impaired users. The researcher for this study is Daniella Briotto Faustino in the Carleton University Human-Computer Interaction program. She is working under the supervision of Dr. Audrey Girouard in the School of Information Technology.

This online survey includes around 30 questions, either multiple choice or text entry, and you can complete it all at once or leave it and come back to finish it within a week. With your consent, your answers will be anonymously recorded so you will be referred to as participant number 1, for example. There are no known risks associated with taking part in this survey. You have the right to end your participation in the study at any time, for any reason, until the end of the survey. If you withdraw from the survey, all information you have provided will be discarded.

As a token of appreciation, you will participate in a prize draw of an Amazon gift card in the value of 50 Canadian dollars. To assure your anonymity, at the end of the survey please follow the instructions to access another webpage to inform your email address. This will prevent any association between your email address and your answers to the survey.

All research data will be encrypted and will only be accessible by the researcher and the research supervisor. Once the project is completed, all research data will be kept for five years and potentially used for other research projects on this same topic. However, when completing the survey please note that Qualtrics servers for Carleton are located in the United States, hence subject to the US Patriot Act.

If you would like a copy of the finished research project, please contact the researcher to request an electronic copy, which will be provided to you.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-A (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

A.2 Online Survey Questions

S3 Section 1 of 4: General questions

Q1 Are you visually impaired? (Choose one)

- ○ Yes
- ○ No

Q2 What is your age? (Write your answer in years) _____

Q3 In which country do you live? (Choose one)

- ○ Canada
- ○ Australia
- ○ India
- ○ The United Stated
- ○ United Kingdom
- ○ Other

Display This Question:
If Q3 = Other

Q3a Please write the name of the country:

_____

Q4 What is your gender? (Choose one)

- ○ Female
- ○ Male
- ○ Other
- ○ Prefer not to answer

Q5 What best describes your visual impairment, with the best correction in your better eye? (Choose one)

- ○ Blind
- ○ Low vision
- ○ Other

Display This Question:
If Q5 = Other

Q5a Please describe your visual impairment:

_____

Q6 How old were you when you became visually impaired? (Write age) _____

Q7 Which assistive devices do you use? (Choose all that apply)

- ☐ Screen magnifier
- ☐ Video magnifier
- ☐ Personal digital assistant (PDA)
- ☐ Electronic glasses
- ☐ Voice input software
- ☐ Screen reader
- ☐ Refreshable Braille display
- ☐ Braille keyboard
- ☐ Smartphone overlay
- ☐ Assistive apps
- ☐ None of the above

Q8 Please comment in case you have any other physical or cognitive impairment (Write your answer) _____

S5 Section 2 of 4: Use of Passwords

Q9 How would you rate the importance of using passwords to secure your personal data? (Choose one)

- ○ Not at all important
- ○ Not important
- ○ Neutral

- ○ Important
- ○ Very important

Q10 Why? (Write your answer) _____

Q11 Usually, how many different passwords you use per day? (Write number) _____

Q12 Where do you commonly use your passwords? (Choose all that apply)

- ☐ ATM machine
- ☐ Online banking
- ☐ Home security system
- ☐ Personal devices
- ☐ Email
- ☐ Social media
- ☐ Business software
- ☐ Shopping websites
- ☐ Online services
- ☐ None of the above

Q13 What are the strategies you use to remember passwords? (Write your answer)

_____

Q14 How able you feel to keep your digital information secure? (Choose one)

- ○ Not at all able
- ○ Not able
- ○ Neutral
- ○ Able
- ○ Very able

Q15 Why? (Write your answer)

_____

Q16 Do you have any concerns about entering passwords in public spaces? (Choose one)

- ○ Yes
- ○ No

Display This Question:
If Q16 = Yes

Q16a What are your concerns? (Write your answer)

_____

S4 Section 3 of 4: Methods to avoid unauthorized access to mobile devices, such as smartphones and iPods

Q17 In your opinion, which method to unlock mobile devices is the most secure? (Choose one)

- ○ PIN (numeric password)
- ○ Alphanumeric password
- ○ Pattern (gesture draw on the screen)
- ○ Fingerprint
- ○ Voice recognition
- ○ Iris scan
- ○ Facial recognition
- ○ Other

Display This Question:
If Q17 = Other

Q17a Please specify what method you consider the most secure: (Write your answer)

_____

Q18 Why do you think this is the most secure method? (Write your answer)

_____

Q19 In your opinion, which method to unlock mobile devices is the least secure? (Choose one)

- ○ PIN (numeric password)
- ○ Alphanumeric password
- ○ Pattern (gesture draw on the screen)
- ○ Fingerprint
- ○ Voice recognition
- ○ Iris scan
- ○ Facial recognition
- ○ Other

Display This Question:
If Q19 = Other

Q19a Please specify what method you consider the least secure: (Write your answer)

_____

Q20 Why do you think this is the least secure method? (Write your answer)

_____

Q21 In your opinion, what is the most accessible method to unlock mobile devices? (Write your answer) _____

Q22 In your opinion, what is the least accessible method to unlock mobile devices? (Write your answer) _____

Q23 In a new method to unlock mobile devices, what would you like to see? (Write your answer)

_____

S6 Section 4 of 4: Use of mobile devices, such as smartphones and iPods

Q24 Which devices do you have? (Choose all that apply)

- ☐ Desktop computer
- ☐ Laptop computer
- ☐ Tablet
- ☐ Smartphone
- ☐ Mobile phone (but not a smartphone)
- ☐ iPod
- ☐ Smartwatch
- ☐ None of the above

Display This Question:
If Q24 != Smartphone
And Q24 != iPod

Q24a Why you do not use a smartphone or iPod? (Write your answer)

_____

Q25 What is the operation system of your smartphone? (Choose one)

- ○ iOS
- ○ Android
- ○ Windows
- ○ Blackberry
- ○ Other
- ○ I don't know

Q26 How many years have you been using smartphones? (Write number of years)

_____

Q27 Do you use any method to avoid unauthorized access to your smartphone? (Choose one)

- ○ Yes
- ○ No

Display This Question:
If Q27 = No

Q27a Why you do not use any method to secure your smartphone? (Write your answer)

_____

Display This Question:
If Q27 = Yes

Q28 Which method you use more frequently to unlock your smartphone? (Choose one)

- ○ PIN (numeric password)
- ○ Alphanumeric password
- ○ Pattern (gesture draw on the screen)
- ○ Fingerprint
- ○ Voice recognition
- ○ Iris scan
- ○ Facial recognition
- ○ Other

q26 How many years have you been using iPods? (Write number of years)

_____

q27 Do you use any method to avoid unauthorized access to your iPod? (Choose one)

- ○ Yes
- ○ No

Display This Question:
If q27 = No

q27a Why you do not use any method to secure your iPod? (Write your answer)

_____

Display This Question:
If q27 = Yes

q28 Which method you use more frequently to unlock your iPod? (Choose one)

- ○ PIN (numeric password)
- ○ Alphanumeric password
- ○ Pattern (gesture draw on the screen)
- ○ Fingerprint
- ○ Voice recognition
- ○ Iris scan
- ○ Facial recognition
- ○ Other

q26 How many years have you been using mobile phones? (Write number of years)

_____

q27 Do you use any method to avoid unauthorized access to your mobile phone? (Choose one)

- ○ Yes
- ○ No

Display This Question:
If q27 = No

q27a Why you do not use any method to secure your mobile phone? (Write your answer)

_____

Display This Question:
If q27 = Yes

q28 Which method you use more frequently to unlock your mobile phone? (Choose one)

- ○ PIN (numeric password)
- ○ Alphanumeric password
- ○ Other

Display This Question:
If Q28 = PIN (numeric password)
Or Q28 = Alphanumeric password
Or q28 = PIN (numeric password)
Or q28 = Alphanumeric password
Or q28 = PIN (numeric password)
Or q28 = Alphanumeric password

Q28a How many characters does your password have? (Write number)

_____

Display This Question:
If Q28 = Other
Or q28 = Other
Or q28 = Other

Q28b What is the method that you use more frequently? (Write your answer)

_____

Display This Question:
If Q27 = Yes
Or q27 = Yes
Or q27 = Yes

Q29 Why do you use this method to unlock your device? (Write your answer)

_____

Display This Question:
If If Why do you use this method to unlock your device? (Write your answer) Text Response Is Displayed

Q30 What do you dislike about this method? (Write your answer)

_____

Display This Question:
If If Why do you use this method to unlock your device? (Write your answer) Text Response Is Displayed

Q31 Please write any additional comments you may have about securing your mobile device

_____

Appendix B: User Study Protocol

B.1 Consent Form for User Study

Title: Exploring the learnability and effectiveness of bend gestures as a form of input when compared to other touch interaction patterns for visually impaired users

Funding Source: National Sciences and Engineering Research Council of Canada (NSERC) through a Discovery Grant (RGPIN-2017-06300).

Date of ethics clearance: May 17, 2017.

Ethics Clearance for the Collection of Data Expires: November 30, 2018.

I _____, choose to participate in a study on Bend Gestures. This study aims to explore the usability of a deformable device for password input for users with vision impairment. The researcher for this study is Daniella Briotto Faustino in the Carleton University Human-Computer Interaction program. She is working under the supervision of Dr. Audrey Girouard in the School of Information Technology.

This study involves two 60 minute sessions. In the first session, you will set-up a password in two different devices, a touchscreen smartphone and a bendable prototype.

The password will be entered multiple times to make sure you memorize them. In the second session, about a week after the first session, you will have five attempts to use the password defined in the first session to unlock each device.

With your consent, your hand gestures will be video-recorded and a brief interview will be audio-recorded. All the data collected will be anonymized so you will be referred to as participant number 1, for example. There are no known risks associated to taking part in this study.

You have the right to end your participation in the study at any time, for any reason, until the end of the session. If you withdraw from the study, all information you have provided will be immediately destroyed.

As a token of appreciation, in today's session you will receive $10. This is yours to keep, even if you withdraw from the study. In addition, after completing the second session of this study, you will receive other $30. Your reasonable transportation costs for attend each session will also be covered.

All research data, including video-recordings and any notes will be encrypted. Any hard copies of data (including any handwritten notes or USB keys) will be kept in a locked cabinet at Carleton University. Research data will only be accessible by the researcher and the research supervisor.

Once the project is completed, all research data will be kept for five years and potentially used for other research projects on this same topic. At the end of five years, hard copies will be securely destroyed.

If you would like a copy of the finished research project, you are invited to contact the researcher to request an electronic copy which will be provided to you.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board, which provided clearance to carry out the research. If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research

Ethics Board-A (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca).

B.2 Protocol Session 1

Consent form

I1 Participant number: _____

I3 First device to be tested:

(if odd participant number = flex, if even participant number = touch)

- ○ flex - BendyPass
- ○ touch - Smartphone

S1 Thank you for agreeing to participate in this study. This study is composed of two sessions, which should take around an hour, each.

S3 In today's session, I will first ask you a few questions. Then, I will present you two devices, one at a time. After training how to use each of them, I will ask you to create a new password. Then, I will also ask a few more some questions before we move to the next device.

Please remember that you are not being tested; in fact, you are testing the prototypes! So, if you have any issue, it is not your fault, it is because we are testing imperfect prototypes. Do you have any questions before we start? OK, let's start.

S4 Now, I am going to ask you some questions. If you do not feel comfortable answering any of the questions just let me know and we can move on to the next question.

Questions from the online survey

Q40 Have you ever participated in a study on flexible devices before?

- ○ Yes
- ○ No

Display This Question:
If Have you ever participated in a study on flexible devices before? = Yes

Q41 What was the study? _____

S5 Now, we are going to start testing the devices. For each device, I'll tell you how to use them, and you will have some time to train how to use them. Then, I'll ask you to create a new password with them and confirm the password created 3 times.

S8 Now, you are going to interact with a touch-screen smartphone. Do you prefer to use it with a screen reader or a screen magnifier? [set it up]

The smartphone is open in an application that has a keypad similar to the one of a calculator. You can try it to learn where the buttons are. The button labelled button can be used to delete the previous digit typed. Once you are done training the gestures, let me know so you can create a new password for you. [wait]

Now please create a strong and memorable password with at least 6 digits, following the audio cues. Please avoid using a password you already have.

Q60 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy it was for you to create a new PIN number on the smartphone? _____

Q61 Why? _____

Q62 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy do you think it will be to remember your PIN number? _____

Q63 Why? _____

Q64 On a scale from 1 to 10, where 1 is not at all confident and 10 is very confident, how confident do you feel to remember your PIN number in a week from now? _____

Q65 Why? _____

Q66 On a scale from 1 to 10, where 1 is not at all secure and 10 is very secure, how secure do you think your new PIN number is? _____

Q67 Why? _____

Q68 On a scale from 1 to 10, where 1 is not at all secure and 10 is very secure, how secure do you think your new PIN number is against a shoulder-surfing attack?

Q69 Why? _____

S9 As in our second session I will ask you to unlock the device without my help, by using the password memorized today, let's rehearse it a little more. You will have as many attempts as you need to complete five successful logins. Are you ready? So, please follow the audio cues from the testing website to proceed.

S6 This is a BendyPass, a flexible prototype for password input.
You can bend its corners up or down and fold it in half. It can recognize a total of 10 different bend gestures. Please try it to learn the possible gestures. Once you are done training the gestures, let me know so you can create a new password for you. [wait]
Now your task is to create a strong and memorable password with at least 6 gestures, following the audio cues.

Q50 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy it was for you to create a bend password on BendyPass? _____

Q51 Why? _____

Q52 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy do you think it will be to remember your bend password? _____

Q53 Why? _____

Q54 On a scale from 1 to 10, where 1 is not at all confident and 10 is very confident, how confident do you feel to remember your bend password in a week from now? _____

Q55 Why? _____

Q56 On a scale from 1 to 10, where 1 is not at all secure and 10 is very secure, how secure do you think your bend passwords is? _____

Q57 Why? _____

Q58 On a scale from 1 to 10, where 1 is not at all secure and 10 is very secure, how secure do you think your bend password is against a shoulder-surfing attack (someone looking over your shoulder and trying to get your password)? _____

Q59 Why? _____

S7 As in our second session I will ask you to unlock the device without my help, by using the password memorized today, let's rehearse it a little more. You will have as many attempts as you need to complete five successful logins. Are you ready? So, please follow the audio cues from the testing website to proceed.

Q70 On a scale from 1 to 10, where 1 is not at all likely and 10 is very likely, how likely would you be to use bend passwords if they were available? _____

Q71 Why? _____

Q72 On a scale from 1 to 10, where 1 is prefer PIN number or text and 10 is prefer bend password, how would you rate your preference for bend passwords on a flexible device? _____

Q73 Why? _____

Q74 What do you think worked well on BendyPass today?

_____

Q75 What do you think could be improved on BendyPass today?

_____

Q76 Do you have any final questions or comments?

_____

Q77 That's the end of today's session. Just to confirm, do you agree that I keep the anonymized data collected today as part of the study?

- ○ Yes
- ○ No

S10 Thank you for your participation in today's session. Please take $10 as a token of our appreciation [pay participant]. See you in the next session [confirm date and time].

B.3 Protocol Session 2

I1 Participant number: _____

BEND PASSWORDS FOR PEOPLE WITH VISION IMPAIRMENT

I3 First device to be tested:

(if odd participant number = smartphone, if even participant number = flex)

- ○ flex - BendyPass
- ○ touch - Smartphone

S1 Thank you for coming for the second session of our study. Today, we will be checking the passwords used in the first session.

S2 Before we start, I'd like to ask you a few questions about the passwords you created in the last session.

Q90 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy do you think it will be to remember your PIN number? _____

Q90a Why? _____

Q91 On a scale from 1 to 10, where 1 is not at all confident and 10 is very confident, how confident do you feel to remember your PIN number today? _____

Q91a Why? _____

Q92 What strategies have you used to remember your PIN number to unlock the smartphone in today's session?

_____

Q80 On a scale from 1 to 10, where 1 is not at all easy and 10 is very easy, how easy do you think it will be to remember your bend password? _____

Q81 Why? _____

Q82 On a scale from 1 to 10, where 1 is not at all confident and 10 is very confident, how confident do you feel to remember your bend password today?

Q83 Why? _____

Q83a What strategies have you used to remember your bend password to unlock BendyPass in today's session?

_____

S6 Here is the smartphone [handle device to the participant]. I would like to ask you to unlock it 5 times using the password rehearsed in the last session. Are you ready? So, please follow the audio cues from the testing website to proceed.

Q93 Which assistive feature you most commonly you use on your smartphone?

- ○ Screen reader
- ○ Screen magnifier
- ○ Both

Q93a [If use screen reader] what method do you most common use to type on your smartphone?

- ○ Standard typing
- ○ Touch typing
- ○ Direct touch typing

Q93b [If use screen magnifier] Do you use the feature to invert the screen colours?

- ○ Yes
- ○ No

S7 Now I will ask a few questions to measure the workload required to complete the login with the smartphone.

Q94 On a scale from 0 to 20, where 0 is very low and 20 is very high, how mentally demanding was the task? (How much thinking, deciding and remembering was required?) _____

Q95 On a scale from 0 to 20, where 0 is very low and 20 is very high, how physically demanding was the task? (How much pushing and pulling was required / how strenuous the task was?) _____

Q96 On a scale from 0 to 20, where 0 is very low and 20 is very high, how hurried or rushed was the pace of this task? _____

Q97 On a scale from 0 to 20, where 0 is failure and 20 is perfect, how successful were you in accomplishing what you were asked to do? _____

Q98 On a scale from 0 to 20, where 0 is very low and 20 is very high, how hard did you have to work to accomplish your level of performance? _____

Q99 On a scale from 0 to 20, where 0 is very low and 20 is very high, how insecure, discouraged, irritated, stressed, and annoyed were you? _____

S3 Here is BendyPass, the flexible device. I would like to ask you to unlock it 5 times using the password rehearsed in the last session. Are you ready? So, please follow the audio cues from the testing website to proceed.

S4 Now I will ask a few questions to measure the workload required to complete the login with BendyPass.

Q84 On a scale from 0 to 20, where 0 is very low and 20 is very high, how mentally demanding was the task? (How much thinking, deciding and remembering was required?) _____

Q85 On a scale from 0 to 20, where 0 is very low and 20 is very high, how physically demanding was the task? (How much pushing and pulling was required / how strenuous the task was?) _____

Q86 On a scale from 0 to 20, where 0 is very low and 20 is very high, how hurried or rushed was the pace of this task?

Q87 On a scale from 0 to 20, where 0 is failure and 20 is perfect, how successful were you in accomplishing what you were asked to do? _____

Q88 On a scale from 0 to 20, where 0 is very low and 20 is very high, how hard did you have to work to accomplish your level of performance? _____

Q89 On a scale from 0 to 20, where 0 is very low and 20 is very high, how insecure, discouraged, irritated, stressed, and annoyed were you? _____

S8 As Workload is perceived differently each person, I'll explain the factors we are considering, based on the NASA Task Load index. One is the Mental effort, related to how much thinking, deciding and remembering you applied. Another is the Physical demand, related to pushing and pulling, for example. Another is Temporal demand, associated to how you perceived the pace of the task. Performance is associated with how successful you were completing the task, Effort relates to how hard you had to work to complete the task, and Frustration is related to how insecure, stressed and annoyed you felt. I'll now tell you pairs of those factors and I'd like to ask you to choose the most important contributor to workload for the specific task you performed:

Q100 Choose one for each pair:

Effort	Performance
Temporal demand	Frustration
Temporal demand	Effort
Physical demand	Frustration
Performance	Frustration
Physical demand	Temporal demand
Physical demand	Performance
Temporal demand	Mental demand
Frustration	Effort
Performance	Mental demand
Performance	Temporal demand
Mental demand	Effort
Mental demand	Physical demand
Effort	Physical demand
Frustration	Mental demand

Q101 On a scale from 1 to 10, where 1 is not at all likely and 10 is very likely, how likely would you be to use bend passwords if they were available? _____

Q102 Why? _____

Q103 On a scale from 1 to 10, where 1 is prefer PIN number or text and 10 is prefer bend password, how would you rate your preference for bend passwords on flexible devices?

Q104 Why? _____

Q115 Do you prefer system-assigned passwords or do you like choosing your own?

_____

Q116 Do you think not choosing your own passwords had any effect on your ability to remember it?

_____

Q117 If you had a flexible device, would you use a bend password or a PIN?

_____

Q110 How was your experience using BendyPass, the flexible device?

_____

Q111 Where do you think bend passwords could be applied?

- ☐ Unlocking smartphones
- ☐ Unlocking personal computer
- ☐ Accessing social media
- ☐ Accessing email
- ☐ Accessing online banking
- ☐ Using ATM
- ☐ Open front door of the house
- ☐ Other _____

Q112 On a scale from 1 to 10, where 1 is not at all likely, and 10 is very likely, how likely would you be to use BendyPass to unlock your devices, if it could be paired via Bluetooth to your personal devices? _____

Q113 On a scale from 1 to 10, where 1 is not at all likely, and 10 is very likely, how likely would you be to use BendyPass to unlock your accounts, if it could connect via Bluetooth to your personal devices? _____

Q114 On a scale from 1 to 10, where 1 is not at all likely, and 10 is very likely, how likely would you be to use BendyPass to access your bank account, if it could be paired with ATM machines? _____

Q115 On a scale from 1 to 10, where 1 is not at all likely, and 10 is very likely, how likely would you be to use BendyPass to open your house, if it could be paired with your door? _____

Q116 On a scale from 1 to 10, where 1 is not at all likely, and 10 is very likely, how likely would you be to use bend passwords on a flexible smartphone?

Q117 What did you like the most about BendyPass, the flexible device?

_____

Q118 What did you dislike the most about BendyPass, the flexible device?

_____

Q119 How do you think we can improved with the Bend password system?

_____

Q120 What customization options would you like BendyPass to have, so you could personalize it to you?

_____

Q121 Who do you know that would like to use BendyPass, the flexible device? What are they like?

_____

S5 Thank you for your participation and please take $30 as a token of our appreciation. [Pay participants for their participation]

S6 If you know anyone else that is blind or have low vision, and would like to participate in the study, please let me know or forward my email to them.

References

[1] Accessibility: *https://www.apple.com/ca/accessibility/iphone/vision/*. Accessed: 2018-06-26.

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

[3] Ahmaniemi, T.T., Kildal, J. and Haveri, M. 2014. What is a device bend gesture really good for? *SIGCHI Conference on Human Factors in Computing Systems* (2014), 3503–3512.

[4] Ahmed, T., Hoyle, R., Connelly, K., Crandall, D. and Kapadia, A. 2015. Privacy Concerns and Behaviors of People with Visual Impairments. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*. (2015), 3523–3532. DOI:https://doi.org/10.1145/2702123.2702334.

[5] 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.

[6] Alnfiai, M. and Sampalli, S. 2016. An Evaluation of SingleTapBraille Keyboard: A Text Entry Method That Utilizes Braille Patterns on Touchscreen Devices. *Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility*. (2016), 161–169. DOI:https://doi.org/10.1145/2982142.2982161.

[7] Americans' Internet Access: 2000-2015: 2015. *http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/*. Accessed: 2018-06-20.

[8] 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.

[9] App Store: 2018. *https://www.apple.com/ca/ios/app-store/*. Accessed: 2018-06-19.

[10] Arduino: *https://www.arduino.cc/en/Main/Software*. Accessed: 2018-06-27.

[11] Assistive Technology Act of 2004: 2004. *https://www.gpo.gov/fdsys/pkg/STATUTE-*

118/pdf/STATUTE-118-Pg1707.pdf. Accessed: 2018-02-21.

[12] 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.

[13] 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.

[14] Aviv, A.J. and Fichter, D. 2014. Understanding visual perceptions of usability and security of Android's graphical password pattern. *Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14*. (2014), 286–295. DOI:https://doi.org/10.1145/2664243.2664253.

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] Biddle, R., Chiasson, S. and Oorschot, P.C. Van 2009. Graphical Passwords : Learning from the First Twelve Years. *Security*. V, (2009), 1–43. DOI:https://doi.org/10.1145/2333112.2333114.

[21] BlackBerry World: *https://appworld.blackberry.com/webstore/?countrycode=CA&lang=en*.

Accessed: 2018-06-19.

[22] Blender: *https://www.blender.org*. Accessed: 2017-07-02.

[23] Blindness Statistics - Statistical Facts about Blindness in the United States: .

[24] BlindSquare: 2017. *http://www.blindsquare.com/about/*. Accessed: 2018-06-19.

[25] 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.

[26] 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.

[27] Braille displays supported by iPhone, iPad, and iPod touch: 2017. *https://support.apple.com/en-ca/HT202514*. Accessed: 2018-06-20.

[28] Braille is spreading but who's using it? *http://www.bbc.com/news/magazine-16984742*. Accessed: 2016-12-15.

[29] Briotto Faustino, D. and Girouard, A. 2018. Understanding Authentication Method Use on Mobile Devices by People with Vision Impairment. *ACM SIGACCESS conference on Computers and accessibility* (2018), (to appear).

[30] Buzzi, M.C., Buzzi, M., Donini, F., Leporini, B. and Paratore, M.T. 2013. Haptic reference cues to support the exploration of touchscreen mobile devices by blind users. *Proceedings of the Biannual Conference of the Italian Chapter of SIGCHI*. (2013), 1–8. DOI:https://doi.org/10.1145/2499149.2499156.

[31] Buzzi, M.C., Buzzi, M., Leporini, B. and Trujillo, A. 2015. Exploring Visually Impaired People's Gesture Preferences for Smartphones. *Proceedings of the 11th Biannual Conference on Italian SIGCHI Chapter*. (2015), 94–101. DOI:https://doi.org/10.1145/2808435.2808448.

[32] Cain, B. 2007. *A Review of the Mental Workload Literature*.

[33] 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.

[34] 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.

[35] 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.

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

[37] 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.

[38] 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.

[39] Ernst, M. 2015. *Bending Blindly : Exploring the learnability and usability of bend gestures for the visually impaired*. Carleton University.

[40] Ernst, M. and Girouard, A. 2016. Bending Blindly : Exploring Bend Gestures for the Blind. *CHI'16 Extended Abstracts*. (2016), 2088–2096.

[41] Ernst, M., Swan, T., Cheung, V. and Girouard, A. 2017. Typhlex: Exploring Deformable Input for Blind Users Controlling a Mobile Screen Reader. *IEEE Pervasive Computing*. 16, 4 (Oct. 2017), 28–35. DOI:https://doi.org/10.1109/MPRV.2017.3971123.

[42] Eye Note: 2018. *https://www.eyenote.gov*. Accessed: 2018-06-19.

[43] Fares, E., Cheung, V. and Girouard, A. 2017. Effects of bend gesture training on learnability and memorability in a mobile game. *Interactive Surfaces and Spaces*. (2017), 240–245. DOI:https://doi.org/10.1145/3132272.3134142.

[44] Florêncio, D., Herley, C. and Coskun, B. 2007. Do strong web passwords accomplish anything? *Proceedings of the 2nd USENIX workshop on Hot topics in security (HOTSEC'07)*. (2007), 10.

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

[46] Girouard, A., Lo, J., Riyadh, M., Daliri, F., Eady, A.K. and Pasquero, J. 2015. One-Handed Bend Interactions with Deformable Smartphones. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*. 1, (2015), 1509–1518. DOI:https://doi.org/10.1145/2702123.2702513.

[47] GLOBAL AND REGIONAL ICT DATA: 2018. *https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*. Accessed: 2018-07-18.

[48] Gonzalo E . Perez 2015. *Analyzing Impaired-User Input Scenarios for Keystroke Biometric Authentication*. Pace University.

[49] Google Play: 2018. *https://play.google.com/store/apps/*. Accessed: 2018-06-19.

[50] 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.

[51] Inqscribe: *https://www.inqscribe.com*. Accessed: 2018-06-20.

[52] Install and enable BrailleBack: 2018. *https://support.google.com/accessibility/android/answer/3535226?hl=en*. Accessed: 2018-06-20.

[53] iOS accessibility: 2014. *http://www.cnib.ca/en/living/how-to-videos/tools-and-tech/Pages/iOS-accessibility.aspx*. Accessed: 2018-06-20.

[54] 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.

[55] Kane, S.K., Bigham, J.P. and Wobbrock, J.O. 2008. Slide rule: making mobile touch screens accessible to blind people using multi-touch interaction techniques. *Proceedings of the 10th International ACM SIGACCESS Conference on Computers and Accessibility* (New York, New York, USA, 2008), 73.

[56] Karrer, T., Wittenhagen, M., Lichtschlag, L., Heller, F. and Borchers, J. 2011. Pinstripe: Eyes-free Continuous Input on Interactive Clothing. *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*. (2011), 1313–1322. DOI:https://doi.org/10.1145/1978942.1979137.

[57] Kerber, F., Lessel, P. and Krüger, A. 2015. Same-side Hand Interactions with Arm-placed Devices Using EMG. *Chi 2015 Ea*. 2, (2015), 1367–1372.

DOI:https://doi.org/10.1145/2702613.2732895.

[58] Kildal, J. and Wilson, G. 2012. Feeling it: the roles of stiffness, deformation range and feedback in the control of deformable ui. *Proceedings of the 14th ACM international conference on Multimodal interaction - ICMI '12* (New York, New York, USA, 2012), 393.

[59] Lahey, B., Girouard, A., Burleson, W. and Vertegaal, R. 2011. PaperPhone: Understanding the Use of Bend Gestures in Mobile Devices with Flexible Electronic Paper Displays. *Proc. CHI*. Vancouver, (2011), 1303–1312. DOI:https://doi.org/10.1145/1978942.1979136.

[60] 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.

[61] Lee, S.-S., Maeng, S., Kim, D., Lee, K.-P., Lee, W., Kim, S. and Jung, S. 2011. FlexRemote: Exploring the Effectiveness of Deformable User Interface as an Input Device for TV. *HCI International - Poster's Extended Abstracts* (2011), 62–65.

[62] 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.

[63] Lo, J. and Girouard, A. 2017. Bendy: An exploration into gaming with mobile flexible devices. *International Conference on Tangible, Embedded, and Embodied Interaction* (2017), 163–172.

[64] Lo, J. and Girouard, A. 2017. Bendy. *Proceedings of the Tenth International Conference on Tangible, Embedded, and Embodied Interaction - TEI '17*. (2017), 163–172. DOI:https://doi.org/10.1145/3024969.3024970.

[65] 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.

[66] Maqsood, S. 2014. *Bend Passwords : Using Gestures To Authenticate on Flexible Devices*. Carleton University.

[67] Maqsood, S. 2014. Shoulder surfing susceptibility of bend passwords. *Proceedings of the extended abstracts of the 32nd annual ACM conference on Human factors in computing*

systems - CHI EA '14. (2014), 915–920. DOI:https://doi.org/10.1145/2559206.2579411.

[68] 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.

[69] 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.

[70] Maqsood, S., Chiasson, S. and Girouard, A. 2013. POSTER: Passwords on flexible display devices. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13*. (2013), 1469–1472. DOI:https://doi.org/10.1145/2508859.2512528.

[71] Microsoft Excel: *https://products.office.com/en-ca/excel*. Accessed: 2018-07-10.

[72] Mone, G. 2013. The Future Is Flexible Displays. *Communications of the ACM*. 56, 6 (2013), 16–17. DOI:https://doi.org/10.1145/2461256.2461263.

[73] 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.

[74] Napoli, D. 2018. *ACCESSIBLE AND USABLE SECURITY : EXPLORING VISUALLY IMPAIRED USERS' ONLINE SECURITY by*. Carleton University.

[75] NASA Ames Research Center *Task Load Index*.

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

[77] Oliveira, J., Guerreiro, T., Nicolau, H., Jorge, J. and Gonçalves, D. 2011. BrailleType: Unleashing Braille over Touch Screen Mobile Phones. *Human-Computer Interaction – INTERACT*. P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, and M. Winckler, eds. Springer Berlin Heidelberg. 100–107.

[78] Park, J., Jeong, B., Jeon, S., Han, S., Cho, J.-D. and Ko, J. 2015. Understanding Interactive Interface Design Requirements for the Visually Impaired. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '15*. (2015), 881–886. DOI:https://doi.org/10.1145/2702613.2732810.

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

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

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

[82] Samsung's extra-stretchable display can survive dents: 2017. *https://www.engadget.com/2017/05/22/samsung-stretchable-oled/?sr_source=Facebook*. Accessed: 2018-06-30.

[83] 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.

[84] Schwesig, C., Poupyrev, I. and Mori, E. 2004. Gummi: a bendable computer. *Proc. CHI*. 6, 1 (2004), 263–270. DOI:https://doi.org/10.1145/765891.766091.

[85] Seeing AI: 2018. *https://www.microsoft.com/en-us/seeing-ai*. Accessed: 2018-06-19.

[86] 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.

[87] Strohmeier, P., Burstyn, J., Carrascal, J.P., Levesque, V. and Vertegaal, R. 2016. ReFlex: A Flexible Smartphone with Active Haptic Feedback for Bend Input. *Proceedings of the TEI '16: Tenth International Conference on Tangible, Embedded, and Embodied Interaction - TEI '16*. (2016), 185–192. DOI:https://doi.org/10.1145/2839462.2839494.

[88] Strohmeier, P., Burstyn, J., Carrascal, J.P., Levesque, V. and Vertegaal, R. 2016. ReFlex: A Flexible Smartphone with Active Haptic Feedback for Bend Input. *International Conference on Tangible, Embedded, and Embodied Interaction* (2016), 185–192.

[89] TalkBack: 2018. *https://play.google.com/store/apps/details?id=com.google.android.marvin.talkback&hl=en*. Accessed: 2018-06-19.

[90] TapTapSee: *https://taptapseeapp.com*. Accessed: 2018-06-19.

[91] TextGrabber: 2018. *http://www.textgrabber.pro/en/?utm_source=abbyy-com-textgrabber*. Accessed: 2018-06-19.

[92] 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.

[93] Unified Remote: *https://www.unifiedremote.com*. Accessed: 2018-02-21.

[94] Visa Has A Plan That Would Allow You To Forget All Your Passwords: *https://www.forbes.com/sites/theodorecasey/2018/05/15/visa-has-a-plan-that-would-allow-you-to-forget-all-your-passwords/#5851ac2494fc*. Accessed: 2018-05-15.

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

[96] VoiceOver: 2018. *https://www.apple.com/ca/accessibility/osx/voiceover/*. Accessed: 2018-06-19.

[97] Warren, K., Lo, J., Vadgama, V. and Girouard, A. 2013. Bending the Rules: Bend Gesture Classification for Flexible Displays. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*. (2013), 607. DOI:https://doi.org/10.1145/2470654.2470740.

[98] 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.

[99] Windows phone apps: *https://www.microsoft.com/en-ca/store/apps/windows-phone?icid=CNavAppsWindowsPhoneApps*. Accessed: 2018-06-19.

[100] With new technology, few blind Canadians read braille: *http://www.ctvnews.ca/with-new-technology-few-blind-canadians-read-braille-1.503149*. Accessed: 2016-12-16.

[101] 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.

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

[103] 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.

[104] 1988. *NASA TLX*. Human Performance Research Group, NASA Ames Research Center.