5-2023

Survey of Input Modalities in the Western World

John Ezat Sadik
University of Tennessee, Knoxville, jsadik@vols.utk.edu

To the Graduate Council:

I am submitting herewith a thesis written by John Ezat Sadik entitled "Survey of Input Modalities in the Western World." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Computer Science.

Scott I. Ruoti, Major Professor

We have read this thesis and recommend its acceptance:

Scott I. Ruoti, Doowon Kim, Jinyuan Sun

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:
I am submitting herewith a thesis written by John Ezat Sadik entitled "Survey of Input Modalities in the Western World." I have examined the final paper copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Computer Science.

_____
Dr. Scott Ruoti, Major Professor

We have read this thesis
and recommend its acceptance:

_____
Dr. Scott Ruoti

_____
Dr. Doowon Kim

_____
Dr. Jinyuan Sun

Accepted for the Council:

_____
Dixie L. Thompson
Vice Provost and Dean of the Graduate School

To the Graduate Council:
I am submitting herewith a thesis written by John Ezat Sadik entitled "Survey of Input Modalities in the Western World." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Computer Science.

Dr. Scott Ruoti, Major Professor

We have read this thesis
and recommend its acceptance:

Dr. Scott Ruoti

Dr. Doowon Kim

Dr. Jinyuan Sun

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Survey of Input Modalities in the Western World

A Thesis Presented for the

Master of Science

Degree

The University of Tennessee, Knoxville

John Ezat Sadik

May 2023

To my parents, for their countless sacrifices and unyielding support, thank you. Soli Deo gloria.

Acknowledgements

I would like to sincerely thank my advisor, Dr. Scott Ruoti, who made this all possible. His guidance throughout all the stages of conducting the research and writing this thesis was instrumental to the completed work.

I would like to thank my family and close friends who encouraged me often throughout the process of completing this thesis. It was their prayers and support that sustained me throughout the research and writing.

Most importantly, I would like to thank God. By His grace alone and for His glory alone, I am here.

Abstract

Having your account compromised can lead to serious complications in your life. One way accounts become compromised is through the security risks associated with weak passwords and reused passwords [22,23]. In this thesis, we seek to understand how entering passwords on non-PC devices contributes to the problems of weak and reused passwords. To do so, we conducted a survey that was distributed to people in the the Western World. In our survey results, we found that users commented about how the current password model was not created with a variety of device types in mind, which created frustrations and complexity in the authentication process. We also found that users will try to prioritize using the devices that are fast and the ones they are familiar with. While users are most frequently authenticating using keyboards and mice, and generally had a strong preference for physical devices, we also found that touchscreen and mobile devices were the next most frequent device used to authenticate. When authenticating on other devices, users listed a number of frustrations like not having access to password managers and having to use arrow keys to input passwords, which made the whole process slower and more complex. Ultimately, these frustrations caused a majority of users to create intentionally weak passwords so they could authenticate faster and it caused other users to simply refuse to use the device or service. This shows that there are specific user needs that are not being met when it comes to the current authentication scheme, and to rectify this, we suggest a preliminary model for how password managers might better meet these needs in the conclusion of this paper.

Table of Contents

Chapter 1

Introduction

Passwords continue to be the dominant form of authentication even though they face many, well-documented problems [6,4,3,17,23]. One of the main reasons for this is that other forms of authentication are not meeting users' needs [2]. Furthermore, there is a significant gap in the knowledge about the system designs and principles that can address these needs [21]. For example, users are regularly asked to create passwords for accounts that they make. These passwords need to be strong so that attackers do not guess them, but not so strong that users have difficulty remembering them. Not only that but, users who make many accounts need to create multiple strong passwords because reusing passwords can cause them to be less secure [22,23]. This causes a problem for the user and often leads to some kind of compromise where either the user creates a weaker password that is easy to remember, but is also more easily compromised by attackers [4, 20], or the user reuses a previous password, which is also bad [22,23].

One way users can shed some of the burdens with password creation is through the use of password managers [5,18,19]. Password managers can create strong and unique passwords for the user, they can store these passwords, and they can fill the passwords in automatically whenever the user needs to authenticate [18]. This allows

users to enjoy the benefits of strong passwords without the work of creating them or remembering them.

However, users often are not using password managers to their full potential, leaving behind some of the features that help secure user passwords [14,16], causing user's passwords to remain vulnerable or weak [14,16]. Though it is not completely clear why users are underutilizing security-critical functionality or how to address this issue. Work by Oesch et al. [16] suggests that a potential reason for underutilization of password generation is the difficulty of entering the generated passwords on non-desktop devices, but details about this specific problem or how to address it are lacking in the research literature.

To address this knowledge gap, this thesis sets out to understand more about the user experience when authenticating, especially as it relates to the mindset users have when using different devices and the frustration that comes along with needing to authenticate on multiple devices. To better understand users and how they authenticate, we survey 1,003 people cross the United States, the United Kingdom, and other parts of Europe. In this survey, we ask users what devices they authenticate on, with what frequency they authenticate on some devices, and what specific challenges they face. After cataloging the different devices users use, specific points, such as the relative prevalence of these devices, the list of their input modalities, and the common challenges that users face when authenticating, we examine the data to draw worthwhile conclusions about users' experiences with passwords. This helps fill in parts of the knowledge gap by providing data on actual user experience with authentication, which will hopefully improve not only the user's experience but also the user's security when authenticating.

Our contributions to the literature include the following takeaways:

- We produce a list of devices that users are using to authenticate, a list of their relative frequency for authentication, and a list of the most frequently used devices for authentication. This helps us understand what devices users are

using that have password managers available and what devices do not. It also helps us understand where users might like to have the functionality of password managers.

- We confirm that users are complaining that password managers are not available on all devices. Furthermore, we confirm users wish to use password managers and are sometimes forced to go without them.

- When users are forced to enter passwords on devices they do not prefer, either because the input modality is not favorable for them or because they prefer some augmented form of authentication like password managers or biometrics, users readily admit that they change their passwords. This means that users are freely admitting to making weaker passwords to lessen the burden of authenticating on some devices.

- In fact, users seem to care greatly about the speed of authentication and ease of use, even more than they care about security. Meaning that users work with a mental model that prioritizes usability above most other things.

- This mental model is also seen when users are admitting to avoiding using certain devices, websites, or services because the authentication process can be slow or complex. This includes when their preferred method of authentication is not present. This shows that the usability of these services is not just a preference for users. For some, it is a requirement.

Although some of these findings may seem like common sense, we now have the data to substantiate our intuition. This is the first study to produce a list of devices used for authentication and the challenges in using such devices across multiple device groups (such as game consoles and touchscreen devices). This allows this research to look at common trends across device groups and produce conclusions that are device-agnostic and conclusions that are device-specific.

Chapter 2

Related Works

Here, we survey the current literature surrounding the topic of passwords and input modalities in order to get a fuller view of the existing knowledge base. We begin by looking at work by Oesch et al. describing the problem of users straying away from password managers, and then we continue by looking at research examining different where users authenticate. Importantly, we are focused on both the devices users are using and their input modalities.

2.1 Cross-Device Authentication

Lyastani et al. [14] conducted the first large-scale study of a password manager's impact on the passwords that users use. In their study, the combined qualitative data on how users use password managers to create and manage passwords with quantitative data on password metrics and entry methods. This data showed that users were using their password managers to store and autofill passwords for many websites. Alongside this, they found that users were not using the password managers to generate passwords.

Pearman et al. [18] conducted a series of interviews with users to understand how they view password managers. In their interviews, they find that many users who use built-in managers enjoy the convenience of password managers while those who

use separately installed tools were interested more in the security that it brought. Also, in these interviews, they also found that users were avoiding using password managers to generate passwords. This is consistent with the work of Lyastani et al., but neither group gives a reason for why this behavior is prevalent among users.

Oesch et al. [16], following up on the work of Lyastani et al. and Pearman et al., conducted a survey of 32 password manager users to find out how password managers are used in the wild. Through this survey, they found that users are avoiding generated passwords because of concerns that these passwords would be challenging to remember and enter on devices when the password manager is not available, especially those devices without physical keyboards. In this work, Oesch et al. suggests that there needs to be more research about generating easy-to-enter passwords based on the device in use or easy-to-remember passwords. They especially note that the current research literature does not address the variety of devices users might need the generated passwords. Our research aims to directly follow-up on the work of Oesch et al. by surveying the variety of devices users authenticate on and by gaining a better understand of users' use of these devices.

2.2 Mobile /Touchscreen On-Screen Authentication and Text Entry

When it comes to mobile devices and touchscreen devices, the work of Greene et al. [7] indicates the effect of password entry as affected by the number of keystrokes needed to enter the password. Greene et al. point out that switching back and forth between the different screen layouts on mobile makes password entry more difficult. This conclusion was based on previous work by Greene et al. [8] where a study was conducted to analyze entering complex passwords on different devices with participants across different age groups. Participants were asked to memorize and then enter a set of system-generated passwords. Mistakes and failures were recorded

as the participants entered the passwords. One conclusion reached in this prior work by Greene was that switching between virtual keyboard layouts increased the time it took for participants to input the passwords and it caused a higher error rate in entering the passwords. In the later work by Greene et al., the goal was to minimize the number of keystrokes in order to decrease the cognitive load users had to endure when entering a password on their mobile devices. To make up for minimizing the keystrokes, they had to make the passwords longer to retain the same amount of security in the passwords. In their conclusion, they note that there is a fundamental difference between entering passwords on desktops and mobile platforms, and this difference should be taken into account by password generators, which is in line with the conclusions drawn by Oesch et al. Our research aims to continue bridging this knowledge gap by providing a better understanding of not only mobile input but all kinds of input modalities.

Whereas the later work by Greene et al. tried to minimize keystrokes to make entering passwords a better experience for the user, the work of Jakobsson et al. [9] proposes a way to improve the user experience when entering passwords through the use of so-called "fastwords". One of the main reasons they propose this heuristic in place of traditional passwords is because traditional passwords run counter to useful features like autocorrect. Users are familiar with and expect the helpful functionality of autocorrect when they use a mobile or touchscreen device. However, passwords run counter to this by not using words from the dictionary, so users are left without the help they are so used to. Fastwords proposes a remedy to this and might fit into a model of password generation that is easy for users to remember. Furthermore, this work highlights that users are making errors at higher rates on mobile devices and touchscreen devices compared to other devices. This implies there must be something about the actual input modality of touchscreen devices that is impacting the user experience.

This is further highlighted by Karat et al. [11] who found that users could transcribe text using keyboards and mice at faster rates than when using voice.

Keyboards and mice had a transcription rate of about 33 words per minute. In the same study, they found that transcribing the same text using voice was done at a rate of only about 14 words per minute. Both rates account for corrections needed throughout the input. Furthermore, they found that users using their voice had to make around 11 corrections per task whereas users using a keyboard and mouse only had to make about 8 corrections per task. We compare this to the work of Mackenzie et al. [15] which found that text entry on on-screen keyboards, such as those for mobile devices and touchscreen devices, was in the range of 15 to 30 words per minute. However, this rate did not include any error correction. This information should be taken with the work of Lee et al. [13] which indicates that the rate of errors on soft buttons without using a stylus was 8% higher than the error rate for hard buttons. Therefore, the rate of accurate or correct words per minute is lower than this presented range because the on-screen keyboard users are potentially making mistakes at a rate higher than those on a physical keyboard, though we do not have enough data to certainly say how much lower the input rate would be. This analysis, however, is enough to simply show that the rate of entry on mobile devices is lower than that of physical keyboard entry. This continues to highlight frustrations users can experience when they are entering passwords on mobile devices. It should also be noted that these metrics are related to text transcription and not to password entry. We believe that password entry would be done at a higher error rate because of the nature of passwords, in that they are not simple or common words.

2.3 Virtual Reality Authentication

Kürtünlüoğlu et al. [12] researched different forms of authentication in virtual reality. They studied the following forms of inputting authentication: input using the controller to trace a pin or pattern, reading biometrics, and gaze tracking. There were also authentication methods that used some combination of those input types, such as reading biometrics while a user traced a pattern. This tells us that on virtual reality

headsets, users are able to use controllers like a stylus on an on-screen keyboard, users are able to have their biometric information read, and they are able to use eye tracking to input information.

Jones et al. in [10] do a literature review on the material concerning VR authentication. This review only reviewed up to October 2020, which means that the work by Kürtünlüoğlu et al. was written after this review. In their review, Jones et al. find the same input modalities discussed by Kürtünlüoğlu et al..

While this research literature does talk a little about the security aspect of each of these authentication methods, it does not talk much about the user experience with the authentication methods. Our research hopes to add to the existing literature by presenting the user's side of authenticating and the mindset they have when they are asked to authenticate on a wide array of devices.

2.4 TV Entry

Bobeth et al. [1] conduct a study that compares standard remote controller entry, gesture-based entry (which was a wizard-of-Oz type entry), and a screen-mirrored tablet for entry as different ways to enter text on a TV. In their study, they look at how different age groups use each input modality and what the impact on that age group's user experience is. Bobeth et al. found that older users had worse motor skills, and therefore it took longer for them to complete the tasks in the user studies. However, the more interesting result is that neither the application used nor the age of the participant had an impact on usability. The only thing that had an impact on usability in this study was the input modalities. This work also found that avoiding display switching seemed to be advantageous in this context. Similarly to part of the research literature on password entry for mobile devices and touchscreen devices, this literature for TV entry does not center around authentication. Instead, this research was done to gauge the different input modalities as a way of navigating the TV and opening different apps to complete specific tasks. The nature of password entry is

different than just opening an app to complete a specific task, so we expect that our research will also contribute to the literature here, providing user insight into the usability and experience of text entry on TVs.

Chapter 3

Methodology

For this research, we used a survey to gather real-world data in order to understand the user's perspective when authenticating. We then analyzed the data we gathered in order to form conclusion about the users and the authentication process, especially as it related to using multiple device types and input modalities. This survey was conducted in October 2022 and all responses were gathered on October 10th, 2022. The platform we used to distribute this survey was Prolific, with the actual survey being administered on Qualtrics. Prolific allowed us to access to people mostly in the United States and Europe. Each participant could only take the survey once, and they were given $1.50 USD as compensation when they completed the survey. We gathered 1003 completed responses from the survey. The survey was approved by our Institutional Review Board and is contained in Appendix A.

3.1 Survey Content

Before the survey, the only information we wanted respondents to have was that we wanted them to know the process of logging into an account is referred to as authentication. In the survey, we asked respondents a mixture of close-ended and open-ended questions. These questions were intended to not only understand what devices the users were authenticating on in the first place, but they also aimed to

understand the user's mindset and experience when authenticating on these devices. For the close-ended questions, we asked respondents what types of devices they authenticated on.

We first asked the respondents about what devices they have entered a password or pin on. We asked about 20 specific devices across four questions and then left space for respondents to list other devices they have authenticated on.

- The first set of devices were general devices users were likely familiar with: desktop, laptop, phone, touchscreen tablet, smartwatch , smart speaker (e.g. Amazon Alexa).

- Next, we asked about devices related gaming: Nintendo Switch , Xbox, PlayStation, Steam Deck, VR headset, other game device, where other was a box where respondents could input text.

- Then, we we asked about smart devices and their non-smart variants: TV / smart TV, thermostat / smart thermostat, lock / smart lock, safe / smart safe, security alarm.

- Finally, we asked about other devices that didn't fit in previous categories: kiosk computer or tablet, printer, physical keypad (such as when entering a building), ATM, other device.

Next, respondents are asked to list the three to five devices that they authenticate on the most frequently. This means that they had to at least list three devices, but they could list as many as five devices.

The next question asked the respondents directly about six different input modalities with the added option of listing another input modality. Respondents are asked to identify how frequently they use each input modality to enter a password or pin.

After this, we asked respondents sets of three key questions. In the first set, we asked respondents three close-ended questions related to their experience inputting

passwords and pins and their experience creating accounts. Here, respondents were instructed to indicate to what degree they agreed with the individual statements using a 5 point likert scale. In the second set, we asked three open-ended questions where respondents were given the chance to talk more freely about their experience using different devices to authenticate.

We then wanted to ask a series of 11 questions mirroring the previous questions about authenticating using a password or pin, but this time about authenticating in other ways. This included using biometrics or multi-factor authentication. However, due to an unfortunate error made by the researchers, these questions were created but never published in the final study, so they were never answered in the survey. This leads to the last set of questions asked which were four questions about demographics.

3.2 Survey Development

In developing our survey, we first crafted a list of questions that we thought were relevant to input modalities and authentication. When we were reviewing these questions, we decided that we wanted to split the survey into a part that asked specifically about passwords and pins and a part that asked about other forms of authentication. However, as mentioned earlier, this second part was unfortunately never sent to the respondents. After creating our final set of questions, we got it IRB approved. After it was IRB approved, we decided to do a pilot survey with a convenience sample to ensure that the survey was understood properly and that there were no technical problems with the survey. After this pilot survey, we deleted the responses we got to make sure that their responses were not included in the actual results we got and then we sent out the survey to the intended population.

3.3 Quantitative Data Analysis

To get a well-rounded understanding of the devices that users are using to authenticate and how frequently they use them, we asked close-ended questions specifically targeting these domains. After collecting all the data, we assigned each respondent a unique ID so that we could track their responses across all questions without using personally identifiable information.

To understand the answers to these questions, we decided to group some questions together and analyze the answers together. We grouped together the five questions asking about what devices users used in order to get an overview of these devices and frequencies. We coded the most frequently used devices in such a way that each respondent would only be able to indicate each specific device once. For example, this means that respondents that listed a mobile phone twice, even if it was a personal phone and a work phone, would only have a phone listed once in their list. Each of the other devices listed would then be moved up in frequency to make up for a device being removed from the list. The rest of the close-ended questions were analyzed in a straightforward way, based on their response type. The input modality question asking about frequency of used was analyzed on its own, and the questions using the likert scale were also analyzed individually.

Also, we looked at the demographic breakdown of the data. We ran a chi-squared test on the data to determine if there was a statistical difference between the data from each region. Although statistically significant differences were found between the EU, US, and UK, the effect size of these differences was not practically meaningful. As such, we report on our aggregate results in the body of the paper, but we provide the data with a breakdown by country in Appendix B for interested readers.

3.4 Qualitative Data Analysis

To better understand our respondents' experiences and feelings towards authentication and input modalities, we offered open-ended questions where they were allowed to enter whatever text answer they wanted. Before diving into the responses we got, there are a few comments we must make about the dataset. First, in regards to the first question about authentication, some respondents clearly interpreted the question to be asking about the authentication process in general, and not about the devices they were using. Such respondents had answers like the following:

> *"I don't like having to use Passwords/PINS, but I know they are a necessity"* (R902)

> *"I don't want them on a device only I use"* (R815)

Next, some respondents mention some variations of desktops, laptops, and physical keyboards. In our coding, we combined all of these into a single category because the underlying input modality is the same. In the same way, we combined comments about mobile phones and touchscreens into the same category. Finally, it is worth saying that users were given open-response questions, so we expect that the specifics mentioned in their response are actually often representative of a lot more people sharing this sentiment, and if questions related to these specifics were asked, we would expect to see even more users indicating that they agree with the general sentiment being expressed.

In analyzing the responses, we used a method based on grounded theory to code the data. Two researchers sat down in a room together and analyzed the data. We read through all the individual responses and applied open coding. In open coding, we assigned any number of codes to each response based on what it said. When there was disagreement about what codes to use, we discussed the disagreements until agreement was achieved. We also applied the constant comparative method, meaning that we revisited the codes and combined or split them as needed.

This coding was done over the course of multiple days, so research notes were created to ensure consistent coding of the data. After the codes were assigned, we reviewed the data and applied axial coding. In axial coding, we examined all the codes we initially created and discussed the ones we thought were actually the same and could be grouped together. This created concepts. Finally, we conducted thematic analysis by grouping related concepts together into themes. It is these themes that we discuss in this paper.

3.5 Quality Control

To ensure that we were only using valid data, we reviewed all of the answers that we received, both to the close-ended questions and the open-ended questions. This was done to ensure that the responses given were valid human responses. In this process, we found one response that simply copied a portion of the question as their answer for one of the questions. We also found three responses in the open-ended questions that were also unfit for our results. Two of which had not answered any of the open-ended questions, and the third had clearly auto-generated the responses or copied some text which only loosely related to the question for their answer. Therefore, we discarded these four results (0.4%). The remaining 999 responses comprise the results of our survey, and these are the only responses considered in the analysis of the data.

3.6 Demographics

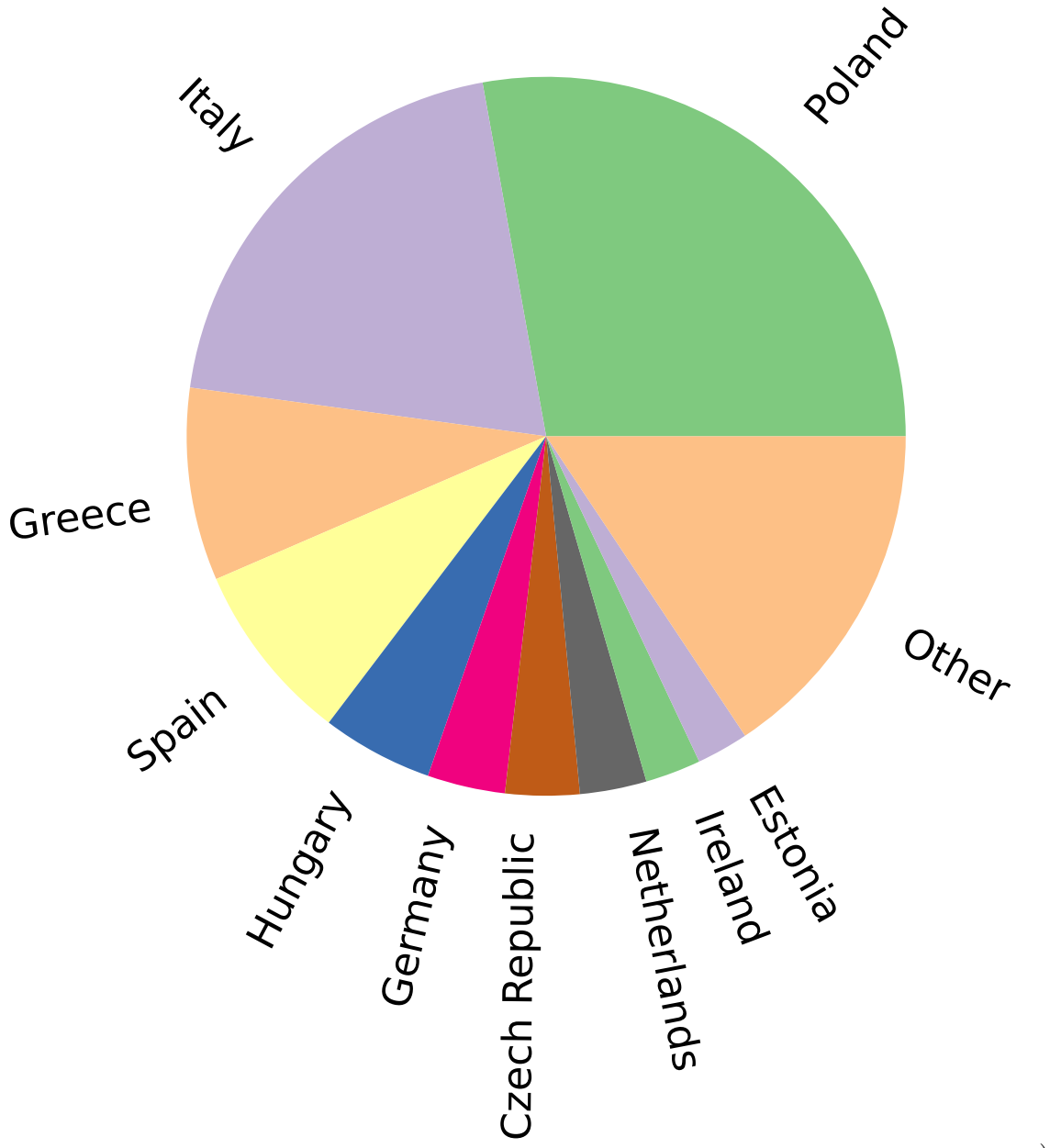
We wanted our results to represent as many users as possible. To accomplish this, we split up our survey to target a specific number of people in three key demographics, the United States, the United Kingdom, and the rest of Europe. We made this split based on how the population of each demographic in our survey compares to the others in terms of actual population numbers. 60% of our data came from Europe, not including the United Kingdom, 10% came from the United Kingdom, and 30% came

from the United States. Figure 3.1 shows part of the breakdown of the nationalities represented in the Europe (other) category. Overall, 47 nationalities were represented in the Europe (other) category.

Table 3.1 shows the breakdown of the demographics of our survey. We had almost an even mix of males and females with 495 males and 486 females, plus 18 respondents who preferred not to answer the question. The ages were mostly in the ranges 18 to 25 and 26 to 25. Combined, roughly 72% of the respondents being in these two age ranges. As far as education was concerned, 597 (60%) respondents said that they had completed college with a degree, 972 (97%) said that they had at least completed high school or some equivalent, and the remaining respondents (27, 27%) either had not completed high school or its equivalents or they preferred not to respond.

3.7 Limitations

In focusing on the western world in this research, we limited where our respondents are from. Additional work could be done to fill in this gap and to see how these results generalize globally. Of course, with the expansion of countries included in these studies, there would be an expansion of languages needed to engage these countries on a proper level, therefore researchers would need a way to send out the survey in the native tongues of the respondents and they would need an understanding of the respondents' culture and perceptions. While we did not specifically ask about biometrics or multi-factor authentication, many respondents did explicitly mention these themes in their responses. We think this suggests that even more users are engaging with these themes than represented in our data because respondent's were not directly prompted on these topics, so it might be worthwhile to have questions related specifically to those topics. Of course, we would also like to see another study asking the questions that we were not able to publish in this study about authentication not using password and pins. While there certainly were limitations that we had to accept to conduct this research, we still decided to continue with



)

Figure 3.1: Europe (other) Composition.

Table 3.1: Demographics for the participants taking the study, less those that were removed for quality reasons.

		Overall		EU		USA		UK	
		999	(100%)	601	(60%)	299	(30%)	99	(10%)
Gender	Male	495	(50%)	300	(50%)	149	(50%)	46	(46%)
	Female	486	(49%)	292	(49%)	144	(48%)	50	(51%)
	I prefer not to answer	18	(2%)	9	(1%)	6	(2%)	3	(3%)
Age	18-25	373	(37%)	282	(47%)	70	(23%)	21	(21%)
	26-35	343	(34%)	205	(34%)	103	(34%)	35	(35%)
	36-45	161	(16%)	83	(14%)	67	(22%)	11	(11%)
	46-55	72	(7%)	22	(4%)	34	(11%)	16	(16%)
	55+	47	(5%)	9	(1%)	24	(8%)	14	(14%)
	I prefer not to answer	3	(0%)	0	(0%)	1	(0%)	2	(2%)
Education	Less than high school degree	19	(2%)	12	(2%)	3	(1%)	4	(4%)
	High school graduate	184	(18%)	130	(22%)	41	(14%)	13	(13%)
	Some college but no degree	191	(19%)	94	(16%)	73	(24%)	24	(24%)
	Associate's degree in college	55	(6%)	30	(5%)	20	(7%)	5	(5%)
	Bachelor's degree in college	337	(34%)	192	(32%)	109	(36%)	36	(36%)
	Master's degree	172	(17%)	117	(19%)	41	(14%)	14	(14%)
	Doctoral degree	15	(2%)	11	(2%)	3	(1%)	1	(1%)
	Professional degree (JD, MD)	18	(2%)	9	(1%)	8	(3%)	1	(1%)
	I prefer not to answer	8	(1%)	6	(1%)	1	(0%)	1	(1%)

the research in order to begin laying the groundwork for future research about input modalities and similar topics with the hope that this future research will find ways to gather even more data with even fewer limitations.

Chapter 4

Quantitative Results

In this section, we will discuss the quantitative results of our survey.

4.1 Device Authentication

In this research, we defined authentication as the process of logging into an account. First, we asked users to recall times when they authenticated on a device using either a password or PIN. Figure 4.1 shows how often users were authenticating with different input modalities. The figure is ordered in an ascending order based on the selection of never.

It should be noted that in this question, a touchscreen represents any device that uses a touchscreen for its main input modes, such as a phone or a tablet. From the figure, it is easy to see that users were most commonly authenticating using a keyboard and a touchscreen. Conversely, users were authenticating least on TV remotes and game controllers.

In Table 4.1, the devices that respondents authenticated on are presented. Furthermore, this table also shows the count for how many respondents indicated each device in order of most used to least used. Finally, the table also shows the difference in these counts based on the region where the data was collected from.

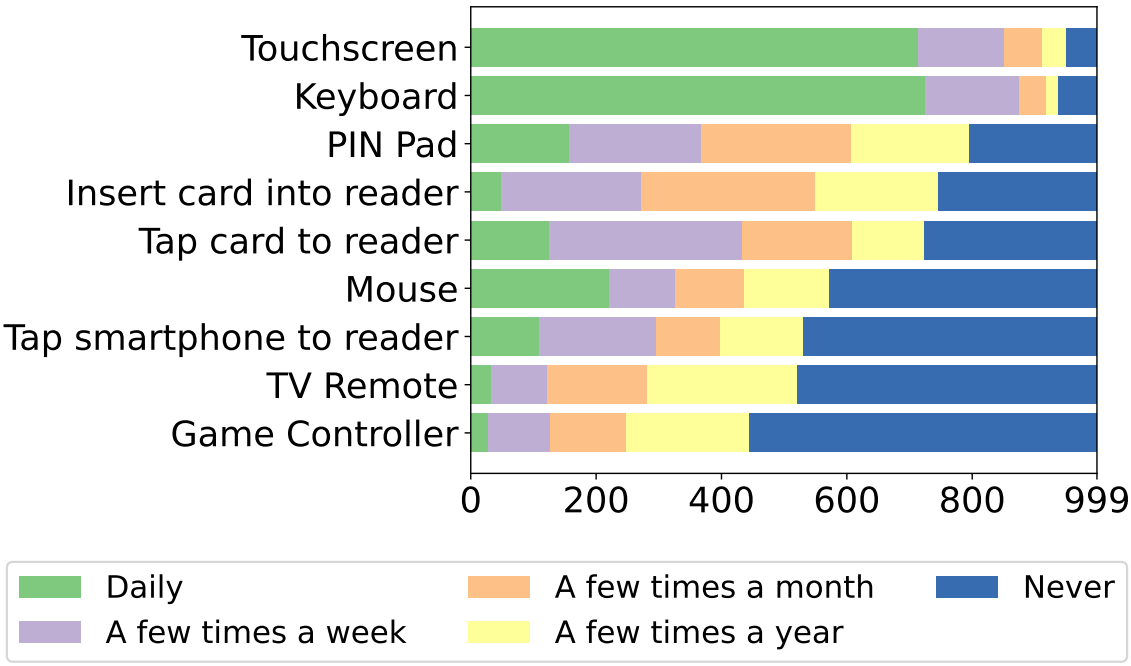


Figure 4.1: Device Authentication Frequency.

Table 4.1: The list of devices and how many participants indicated using them to enter passwords. Percentages recorded include the percentage within the category and percentage of overall responses (% Within; % Overall).

		Count (% Within; % Overall)
General		997 (100%)
	Phone	980 (98%; 98%)
	Laptop	847 (85%; 85%)
	Desktop	644 (65%; 64%)
	Tablet	481 (48%; 48%)
	Smartwatch	127 (13%; 13%)
	Smart speaker	36 (4%; 4%)
Physical		862 (86%)
	ATM	819 (95%; 82%)
	Physical keypad	379 (44%; 38%)
	Kiosk computer or tablet	168 (19%; 17%)
	Printer	136 (16%; 14%)
Smart		570 (57%)
	TV / Smart TV	416 (73%; 42%)
	Security alarm	165 (29%; 17%)
	Lock / Smart lock	141 (25%; 14%)
	Safe / Smart safe	112 (20%; 11%)
	Thermostat / Smart thermostat	34 (6%; 3%)
Gaming		447 (45%)
	PlayStation	265 (59%; 27%)
	Xbox	180 (40%; 18%)
	Nintendo Switch	178 (40%; 18%)
	VR headset	36 (8%; 4%)
	Other game console	23 (5%; 2%)
	Steam Deck	22 (5%; 2%)
Other		94 (9%)
	POS	16 (17%; 2%)
	Doors	11 (12%; 1%)

For the smart device columns, we felt that users authenticating on these devices were not impacted by whether the device was the smart variant or not, so we grouped those devices into the same answer choice. It should also be noted that the other category only shows those devices that 10 (1%) or more respondents indicated.

From Table 4.1, it is clear that general physical devices were used the most by people authenticating using a password or pin. As shown in the table, the five most used devices across all the categories are phones, laptops, ATMs, desktops, and tablets. In general, users were not authenticating on many devices outside of the ones that were listed in the first four main categories.

After this, we asked respondents to list the devices they most frequently authenticate on. For this question, they were asked to list at least the top three devices, but they could list up to the top five devices they most frequently authenticate on. Figure 4.2 shows the results of this question in a stacked format. This figure only reports devices that more than 25 (3%) respondents listed. This is because some devices were only listed by a very small number of respondents. So we focus on the top responses only to identify trends in the data.

For each device, the bars indicate what number of respondents listed that item as their most frequently used, second most frequently used, third most frequently used, fourth most frequently used, or fifth most frequently used device. The figure is ordered in descending order of frequency based on the most frequently used device. This means that phones were the most common most frequently used device for authentication. In fact, the five most common devices from Table 4.1 are also the most frequent devices used for authentication. Thinking about these devices in terms of input modalities, laptops, and desktops have physical keyboards, phones, and tablets have a touchscreen with a virtual keyboard, and ATMs use a keypad. This means that the input modalities that are most often used are physical keyboards, virtual keyboards on a touchscreen, and keypads.

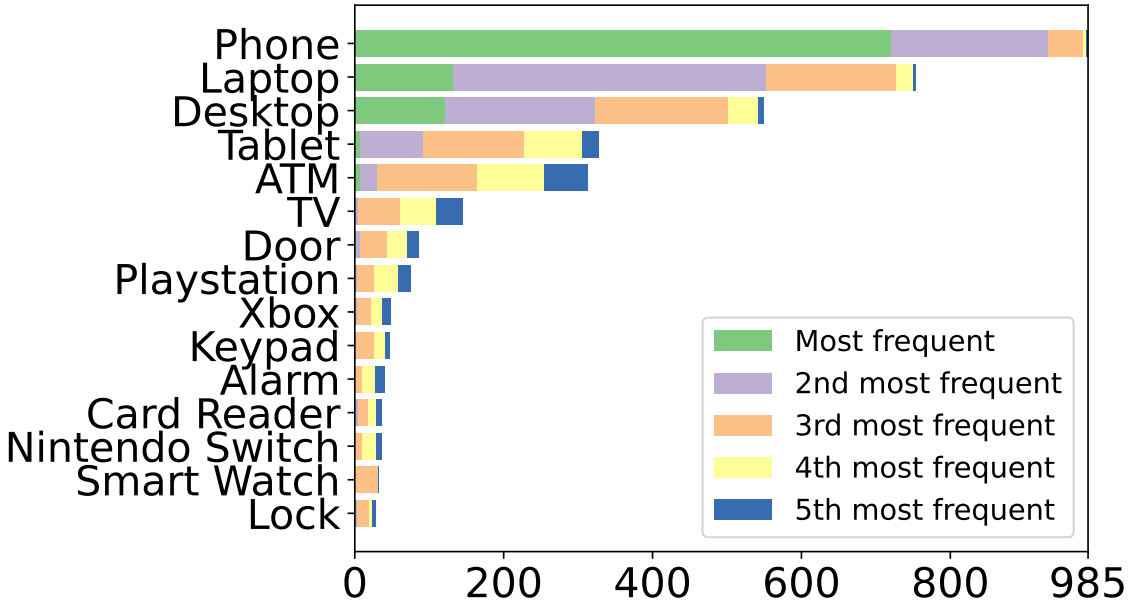


Figure 4.2: Devices Used for Authentication by Frequency.

Figure 4.3 shows the responses to different questions we asked the users about their experience authenticating and how that impacted them. In order, we asked them:

- I think there is a difference in how easy it is to enter passwords or PINs depending on what device I am using (for example, entering on an Xbox vs entering on a laptop).
- When creating passwords or PINs, I consider the types of devices where I will need to enter that password or PIN.
- If I need to create an account, I wait until I can do it on my preferred device type rather than immediately creating the account on the device I am currently using.

From the results we got, users are overwhelmingly agreeing with the idea that there is a difference in how easy it is to enter passwords or PINs depending on which devices they are using. Furthermore, more than half of the respondents admit that they consider the device type they are using when they create passwords or PINs. This means that users may have different passwords depending on what devices they will be using the account on. Finally, we also see a similar number of respondents admitting that they would prefer to wait to create their account on one of their preferred device types rather than just make it on the device they are currently using.

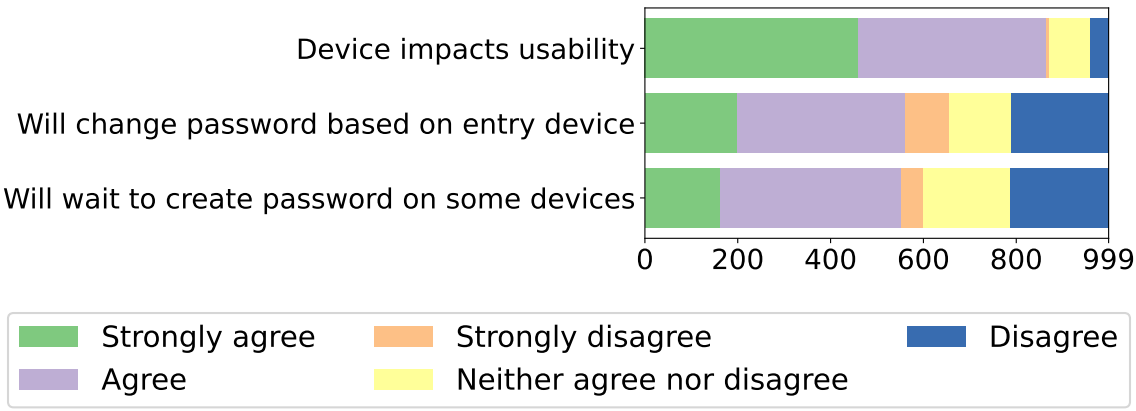


Figure 4.3: How Much Does Usability Impact User Experience.

Chapter 5

Qualitative Results

Following the quantitative questions that were asked, we then asked the respondents to answer some qualitative questions. These questions were more open-ended, and they were aimed at understanding more of what the user experienced when they authenticated on different devices. These questions also provided users with a place to give us more insight in the event that they had something to share and none of the questions we had asked so far had allowed them to share it. We asked a total of three questions, but when we coded the questions, we really looked at all three questions to assign codes to each respondent. These questions were:

- Please explain how the type of device you are authenticating to impacts your experience when using something other than a password or PIN.
- What challenges do you face when authenticating using something other than a password or PIN? What do you wish was easier about the process?
- Is there anything else you want to tell us about authenticating using something other than a password or PIN that could help us improve your experience?

5.1 Virtual Keyboards

Thinking about the other devices, game consoles, TVs, mobile phones, and touch-screen devices all use some form of virtual keyboards. We split the responses we received into different themes that represented the data. Table 5.1 has a list of these themes and the corresponding comments that relate to each theme.

In total, 421 respondents mentioned virtual keyboards, game consoles, or TVs in some fashion. For each concept within the theme, we report the number of people who reported each comment and then the percentage of people who reported the comment with respect to the total number of respondents who said anything about virtual keyboards and finally the percentage of people who said the comment with respect to the total number of responses in our data.

56 (13%) of people said that virtual keyboards were hard to use for authentication and 65 (15%) said the same about using a mobile device for authentication. As for why, one user mentioned specifically that it seems like long passwords were meant for PCs and not phones.

> *"Phones are fine unless you have to enter a very long password which was created for PCs. PCs are generally better for typing but...a phone is a necessity..."* (R424)

Another reason this perception of virtual keyboards could be present is due to frustration with game console and TV entry. 107 (25%) of respondents who mentioned virtual keyboards mentioned that authenticating on game consoles was hard. Similarly, 109 (26%) of those respondents said the same thing about authenticating on a TV.

These comments about controller entry are tied to the restrictions using arrow keys imposed on users. Each time arrow keys were brought up, there was a complaint about how they made the whole process of authenticating slower, more frustrating, or both. In fact, here are some comments from the respondents about why they felt like virtual keyboards were hard to use and not as good as physical keyboards.

Table 5.1: List of comments about virtual keyboards and how many participants indicated each comment. Percentages recorded include the percentage within the individual concepts, the overarching theme, and overall responses.

		Count (% Theme; % Theme Group; % Overall)			
		134 (32%; 13%)			
General	Virtual Keyboard Entry Hard	56	(42%;	13%;	6%)
	Mobile Entry Hard	65	(49%;	15%;	7%)
	Mobile Entry Slow	14	(10%;	3%;	1%)
	Touchscreen Entry Hard	23	(17%;	5%;	2%)
		207 (49%; 21%)			
Arrow Keys	Game Entry Hard	107	(52%;	25%;	11%)
	Game Entry Slow	38	(18%;	9%;	4%)
	Game Arrow Key Entry Bad	25	(12%;	6%;	3%)
	Game Entry Uncomfortable	4	(2%;	1%;	0%)
	TV Entry Hard	109	(53%;	26%;	11%)
	TV Entry Slow	109	(53%;	26%;	11%)
	TV Arrow Key Entry Bad	32	(15%;	8%;	3%)
	TV Entry Uncomfortable	2	(1%;	0%;	0%)
		102 (24%; 10%)			
Touchscreen	Touchscreen Entry Fast	4	(4%;	1%;	0%)
	Touchscreen Entry Easy	35	(34%;	8%;	4%)
	Mobile Entry Easy	78	(76%;	19%;	8%)
	Mobile Entry Fast	13	(13%;	3%;	1%)
		103 (24%; 10%)			
Layouts	Special Characters Hard to Use	35	(34%;	8%;	4%)
	Layout Switching Hard	20	(19%;	5%;	2%)
	Virtual Keyboard Layout Matters	22	(21%;	5%;	2%)
	Familiarity Matters	43	(42%;	10%;	4%)

> *"Typing with a TV remote where you have to choose each letter from a grid makes me want to cry."* (R951)

> *"The standard keyboard layout does not work well with a game controller or Tv remote, it should be optimized based on what letters are used most often to speed up the process."* (R803)

However, it should be noted that 35 (8%) of respondents thought that password entry on touchscreens was easy. And as for mobile password entry, 78 (19%) said it was easy, which is more than those who said it was hard. So while arrow keys on controllers were definitely looked down upon, it seems like touchscreens may actually be liked by users and might be a mitigating factor to the frustration with virtual keyboards.

In the same vein of virtual keyboards being bad, another common theme that was brought up alongside arrow keys was the idea of switching layouts on virtual keyboards. Table 5.1 also shows some of the comments respondents left about the layout of virtual keyboards. Interestingly, 22 (5 %) respondents indicated that the layout of the keyboard they were using mattered, and 20 (5%) respondents indicated that there came some frustration or complexity in having to switch the keyboard layout. Here, switching the keyboard layout indicates switching from a keyboard showing letters to one showing numbers and symbols or to one showing the letters in a different casing. This extra click on mobile phones, touchscreen devices, game consoles, and TVs is not present on physical keyboards. Here respondents had this to say about such challenges:

> *"It's always the easiest for me with the use of [a] keyboard, in case of [a] touchscreen it takes more time because of switching keyboards."* (R11)

> *""[Challenges faced include: f]inding special characters and switching between capitals and lower case"* (R71)

Specifically on the topic of switching virtual keyboard layouts, respondents mentioned that having to find or use special characters or different case letters was the source of needing to switch the keyboard layout. Having to search for characters on the different layouts of the keyboard contributed to the overall dislike of virtual keyboards. This is likely why 43 (10%) respondents reported that being familiar with the device they were using was an important factor when it came to authentication.

5.1.1 Cross-Device Authentication

Another theme that was brought up by respondents was the idea of cross-device authentication. When we talk about cross-device authentication, we mean authenticating on a secondary device in order to complete authentication on the primary device. For example, if you need to log into a streaming service on your TV, you would log in through your laptop's web-browser first, and it would automatically complete the log in on your TV without needing to type in a password. Respondent's clearly brought up this idea with regards to authenticating using virtual keyboards. For them, this seems like a good way to get around having to use a TV or game controller.

> *"...If you could use your phone or tablet to log into a console instead of using a controller to log in it would make it easier."* (R460)

> *"Typing a password with a remote/controller can take a lot of time. Some services let you type the password on your phone/PC and then you automatically login on the TV/Console and usually it works well but I wish it was more widespread."* (R568)

5.2 Physical Device Entry

In contrast to virtual keyboards being hard, many respondents agreed that physical devices were the easiest for authentication. For example, 221 users mentioned that

they found desktops and laptops to be easy to use, which were by far the devices that respondents liked the most. This might seem like common sense, but it is important to realize that we now have data that backs up any conjectures we may have had.

When it comes to why respondents liked physical devices the most, we can look at their responses to identify common themes and comments about physical devices. Table 5.2 shows the some key themes mentioned in comments left by respondents and how many respondents mentioned each comment. In total, 271 respondents commented on physical entry, and the percentages represented in the table are based on this total and then the overall number of respondents. As seen from the table, 221 (82%) of respondents indicated that they thought physical entry for authentication was easy. Furthermore, 5 (2%) respondents explicitly mentioned that they liked physical device entry because it led to less mistakes.

5.3 Cross-Device Considerations

Continuing with this theme of looking at different devices, we wanted to explore some of the comments about the different devices that respondents commented on. First, it should be noted that, it seems like respondents agree that the device they are using matters. In fact, only 53 (5%) users indicated that the device they were using had no impact on their experience authenticating. This is shown through their comments about how the devices are different, leading to results like easier use, more mistakes, or faster authentication.

For example, the following comment from one of our respondents summarizes the common themes we saw quite nicely.

Table 5.2: List of comments about physical devices and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
Physical Entry		271 (27%)
	Physical Entry Easy	221 (82%; 22%)
	Physical Entry Hard	10 (4%; 1%)
	Physical Entry Fast	47 (17%; 5%)
	Physical Entry Comfortable	8 (3%; 1%)
	Physical Entry Less Mistakes	5 (2%; 1%)

> *"For me, the desktop computer with a keyboard is the easiest device for authentication, because typing on a large keyboard is very comfortable and you can easily type in special characters or symbols that are on the keyboard itself, so that passwords can be long and secure and are easy to type in. On other devices without a physical keyboard, such as a smartphone, it is more difficult to type the characters without making a mistake and it is harder to find the symbols, so the authentication process is slower and produces more errors. On devices like smart TV where you have to select characters with the TV remote control it is even more complex than on a smartphone, because the system forces you to scroll letter by letter with the remote control until you find the appropriate character, and the process is very slow."* (R783)

One thing that R783 mentions is that authentication is slower and is done with more errors on devices without physical keyboards. Other users also had comments about how the speed of authenticating would impact their choice of device, their frustration (or lack thereof), and their overall experience. Table 5.3 shows the list of different comments users had about speed. 143 respondents indicated that speed mattered to them. For the remaining comments, the percentages shown are with respect to the percentage of these 143 respondents.

In this case, saying that speed matters means that they desired authentication to be as fast as possible. This difference in speed might be part of the reason that users preferred different devices. Notably, no users said that physical entry was slow, and physical entry was the most preferred method of authentication. In fact, when it came to comments about speed, respondents were usually very direct about how it impacted them. When the process became too slow or complicated, some respondents even admitted to giving up on the whole authenticating process entirely.

Table 5.3: List of comments about speed and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
		143 (14%)
Speed	Physical Entry Fast	47 (33%; 5%)
	Physical Entry Slow	0 (0%; 0%)
	Mobile Entry Fast	13 (9%; 1%)
	Mobile Entry Slow	14 (10%; 1%)
	Touchscreen Entry Fast	4 (3%; 0%)
	Touchscreen Entry Slow	3 (2%; 0%)
	Game Entry Fast	0 (0%; 0%)
	Game Entry Slow	38 (27%; 4%)
	TV Entry Fast	0 (0%; 0%)
	TV Entry Slow	42 (29%; 4%)

"the longer it takes, the more annoying it is and i use it less" (R23)

"according to the device I am using, it is more or less quick and easy to authenticate. when it's complicated it's frustrating and sometimes I just give up" (R387)

In addition to these comments about speed, users had other comments when it comes to authenticating on different devices. These comments are summarized in Table 5.4. In total, 903 respondents had some comment about whether the device they used impacted them or not, we present the percentages based on these 903 respondents and then based on all 999 responses in our data. It is significant to note that 855 (94%) respondents indicated that the device they were using to authenticate had an impact on the authentication process.

Furthermore, 69 (8%) respondents indicated that the device size mattered to them when authenticating. This device size comment took form in a few different ways, such as comments about the actual device size, comments about the keyboard size, or comments about the screen size. Here are a few quotes for examples about what was being said about screen size.

"I don't like to authenticate anything on my phone as I can't see everything properly-[w]orried to make a mistake." (R75)

"It is preffered to use a laptop to enter passwords as it is easier to observe pop ups or other unwanted elements on the screen in comparison to phone or other similar deviced" (R77)

Furthermore, 57 (6%) respondents indicated that making mistakes had a serious impact on their authentication experience. 74 (8%) respondents also said that making mistakes made authenticating harder or more complex than it already was.

"sometimes when i am typing a password on the keyboard, im missing some letters/ using wrong letter size, which makes it more complicated" (R10)

Table 5.4: List of comments about cross-device considerations and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
	Devices Has Impact	855 (94%; 86%)
	Device Has No Impact	53 (6%; 5%)
		340 (34%)
Passwords	Comfort Matters	11 (1%; 1%)
	Device Size Matters	69 (8%; 7%)
	Mistakes Matter	57 (6%; 6%)
	Mistakes Cause Challenges	74 (8%; 7%)
	Frequency of Authentication Matters	12 (1%; 1%)
	Security Matters	83 (9%; 8%)

Some respondents mentioned that this was related to not being able to see the password as they were typing it in. Other respondents said that services they used deleted their password if it was wrong, even if it was just because they forgot a single character. This means that they had to retype the entire password after every mistake.

> *"Sometimes the device won't have the option to let you see the password you entered. I often mistype, so I like to check if I entered it correctly. Also, when I'm not sure if I have the right password in mind and the login fails, it's good to see if it was a simple mistype or if the password itself is incorrect. So I wish more devices had the option to reveal the entered password."* (R97)

> *"Sometimes if you make a mistake you can't always backtrack and have to start from the beginning, or you can't always see the numbers after you've entered them"* (R89)

Finally, 83 (9%) of respondents indicated that security mattered, regardless of the device they were authenticating on. This led some respondents to mention that they were wary of shoulder surfing or someone else seeing them type in their password. There were also other respondents who thought that entering a password onto a big device like a TV was insecure because it showed the characters as they were being typed in. These security concerns impacted how users created and used passwords.

> *"So for example.. I can enter my phone pin very quickly, and only I'm able to view the screen generally. If I'm entering my password on say.. Xbox Live, and other people are in the room - they could, if they wanted to, just watch which keys I was hitting on the onscreen keyboard. So because of this my Xbox password is shorter so that I can enter it as quickly as possible"* (R35)

"Entering passwords on some devices (those that are displayed via the TV) are not as safe as those on a computer or smartphone as everyone can see the keys that are being entered. This isn't very secure." (R151)

5.4 Passwords for Authentication

340 (34%) respondents answered our questions with comments about passwords in general instead of authentication. We would like to discuss those comments here. The most common comment, by far, was that remembering passwords was hard. Here is what respondents had to say about remembering passwords:

"You always end up with more passwords than you want, and you forget them." (R50)

"People who created this system need to understand that the average person does not have the mental bandwidth to remember dozens of individual passwords for each site, let alone change them every 90 days or whatever. The whole system is reaching "peak password" and I think the whole concept needs to go back to the drawing board." (R951)

Table 5.5 shows what kind of comments users had about using passwords for authentication. As with previous tables, the percentages for the comments are in reference to the percentage of the 340 respondents who talked about passwords as a form of authentication.

Some additional factors to remembering passwords being hard that make users frustrated with password authentication are that creating new passwords are hard and creating unique passwords are hard. Part of this problem is that many users understand that they can't just use the same password for every account, so they have to create a new, unique password often.

"I often forget passwords! So I end up using similar ones which of course isn't great for security!" (R165)

Table 5.5: List of comments about passwords and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
Passwords		340 (34%)
	Remembering Passwords Hard	250 (74%; 25%)
	Creating New Passwords Hard	24 (7%; 2%)
	Creating Unique Passwords Hard	50 (15%; 5%)
	PCP Requirements Bad	76 (22%; 8%)

"sometimes is hard to think about new password or pin" (R377)

Creating new passwords is also made harder due to password creation policies (PCP requirements), which 76 (22%) of the 340 respondents mentioned. Because of these requirements, sometimes, users are not even able to use the password they want to use. This can lead to added frustration but also contribute to making it hard to remember the password. Some common themes in the comments about PCP requirements were that users often forgot what they were when it was time to enter in their passwords, so they forget which password they need to enter in. Another theme was that respondents felt like some PCP requirements for specific types of websites were overkill for the data that ws being secured.

> *"Remembering the password as different places require different qualifications for a password, e.g. some require a special character and some don't"* (R277)

> *"Some [services require] long passwords on platforms [t]hat doesn't need bank level security"* (R317)

> *"Sometimes it's hard to remember my password, especially when i need to use special characters that i don't use for my other passwords, maybe saying that the password needed a special character so I remember that i needed to add one"* (R426)

In addition to these comments about passwords creation, there were also comments from respondents about the password life cycle, especially as it related to resetting and recovering their passwords. For this, there were 405 respondents that either talked about the lifecycle of the password or the hardware they were having trouble with. These comments are listed with their relative frequency in Table 5.6. 59 (15%) of respondents had trouble with the actual hardware they were using, and this caused problems when authenticating. A few other respondents, 12 (3%) felt like the number of times they had to authenticate in a given time period was too high.

Table 5.6: List of comments about passwords' lifecycle and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
Password Lifecycle		405 (41%)
	Hardware Doesn't Always Work	59 (15%; 6%)
	Authentication Frequency High	12 (3%; 1%)
	Password Forced Reset	24 (6%; 2%)
	Password Recovery Hard	16 (4%; 2%)
	Account Lockout Frustrating	6 (1%; 1%)

In regards to users' experience with hardware not being up to their standards or in regards to having to reauthenticate so often, here are some user quotes.

> *"the authentication process is not very smooth, it is often slow and not very responsive. It happened to me that using devices such as TV then there is no possibility to review the password and in case it was wrong, doing the same procedure with the remote control would be so slow that I would just give up. I'd change that."* (R714)

> *"I don't like having to reauthenticate so frequently."* (R718)

Finally, there were 24 (6%) comments about forced password resets, password recovery (16, 4%), and being locked out of accounts. Respondents found that being forced to reset their password worsened the issue of having to remember all the passwords. This was combined with the idea that password recovery was not an easy process. This meant that sometimes, users are being locked out of their account, and they go through many challenges to recover their password and regain access to the account. These ideas are expressed in a few comments from the respondents:

> *"It's way too complicated to renew them if you forgot them. It should be easier also to create them anew."* (R265)

> *"It should always there be a way to recover the password or PIN, otherwise someone could be locked out of his/her device/account."* (R290)

> *"The challenge is that you have many accounts to remember and also in some situations (e-banking i.e.) you have to change password every 3-6 months without using any of the last 10 passwords. That makes the process frustrating."* (R444)

5.4.1 Password Composition

Seeing that many respondents struggled with adapting to different PCP requirements, remembering passwords, creating new passwords, and overall maintaining their

passwords, it should be no surprise that 60 respondents also talked about how the usability of the device they were on impacted the password creation process. Table 5.7 lists some of comments about how usability impacted passwords creation and use. 28 (47%) of the 60 respondents who talked about how usability impacted them indicated that the passwords they create vary in length depending on the device they are using. Similarly, 35 (58%) of those same respondents said that they varied the complexity of their passwords depending on the device they were using. 6 (10%) of respondents also said that they would avoid a service if they found it too hard to use.

This is significant because these are respondents freely admitting to behaviors they are aware is bad. This suggests that many more users are following these habits, and this is also suggested by the quantitative data that was gathered and discussed previously.

> *"If I'm creating an account in a device like a TV, where entering a password takes too long, I might make it shorter or simpler"* (R459)

> *"I use longer passwords on keyboard, but shorter on touchscreens"* (R757)

> *"On devices without a user-friendly entry interface, I focus on easily entered passwords or avoid using them altogether."* (R804)

5.5 Password Alternatives and Augmentations

In response to the different frustrations caused by authentication in general and authenticating on different devices, users have adopted different strategies to make authentication easy again. These strategies include leveraging systems like passwords managers and biometrics where available. In talking about these topics, respondents also mentioned some of their thoughts on multi-factor authentication.

Table 5.7: List of comments about usability and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
		60 (6%)
Usability	Usability Impacts Length	28 (47%; 3%)
	Usability Impacts Complexity	35 (58%; 4%)
	Usability Impacts Reuse	1 (2%; 0%)
	Usability Impacts Usage	6 (10%; 1%)

5.5.1 Password Managers

With 187 (19%) respondents mentioning the concept of password managers, it seems like users thought that password managers were a good way to solve the problem of creating, remembering, and using passwords. Table 5.8 shows the different comments left by respondents about password managers, again with the percentages listed being relative to the 187 total responses about password managers. Interestingly, 157 (84%) of respondents who said something about password managers indicated that they used a password manager. Another 22 (12%) indicated that they wanted a password manager or something like it in the event that they did not know that password managers existed.

When it comes to why users wanted password managers, they provided a variety of reasons.

> *"ADHD means I have a poor memory. Saving passwords on browser or device helps massively"* (R163)

> *"I use a password manager which generates complex passwords. These are much faster to enter on a keyboard than a smartphone. This means that it can be time consuming to use a phone and therefore using a desktop computer or even a tablet is preferable. "* (R310)

This is great, because password managers seek to solve the very issues users were running into, but, as noted by some respondents, password managers are not a perfect solution. One major problem that 67 (36%) of respondents identified was that password managers are not always available.

This is a sharp downside because users that generate complex passwords using password managers and then rely on the password manager to store the password for them will face a lot of frustration trying to enter that password manually. This is not only because they are not used to entering the password manually, but also because sometimes the actual input modality makes typing hard all on its own (like arrow

Table 5.8: List of comments about password managers and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
		187 (19%)
Managers	Uses Password Manager	157 (84%; 16%)
	Wants Password Manager	22 (12%; 2%)
	Password Manager Not Available	67 (36%; 7%)
	Password Manager Syncing Issues	6 (3%; 1%)
	Distrusts Password Manager	17 (9%; 2%)

keys being slow, as mentioned above), without the added mental load of typing in a complex password.

> *"My phone saves my passwords, however I can't access these passwords via Google Chrome, so I usually make accounts on my phone. If it's a service that I will specifically use on my computer, I will then make an account on my computer...If I use an auto-generated one, I have to refer back to the original device to see what it was. I wouldn't want it to be easier though, as it's safer."* (R68)

> *"Keeping my encrypted password database synced and the versions up-to-date between my mobile and laptop [is a challenge I face]."* (R206)

A few other respondents said that they didn't trust password managers, so even though some desired to use them, they still would not on account of lacking trust. Though with this distrust, it seemed like some respondents didn't understand exactly how a password manager worked. The common misconception was that respondents presented the idea that password managers allowed the individual websites or services to store the password for the user, which is not how password managers work.

> *"Having to remember many different combos is difficult, but I don't trust password managers"* (R35)

> *"When websites are asking if they should save the password its a good system. That allows the user to save the password on websites that the user think are safe."* (R495)

> *"Remembering all passwords and pins and coming up with a new one that is both strong and easy to remember at the same time is a real modern-day struggle (I don't rely on the ones suggested by Google because I think saving your passwords on a website is extremely unsafe)"* (R614)

5.5.2 Biometrics

In addition to password managers, 333 (33%) respondents turned to biometrics as a way to augment the authentication process. As shown in Table 5.9, biometrics were preferred by 242 (73%) respondents who mentioned them, which is even more than those who used password managers.

Biometrics seemed to be preferred due to their speed and ease of use, which also included not needing to remember the password.

> *"I prefer to use fingerprint and not a password because a password can easier be forgotten"* (R91)

> *"The device I use is easy because I just have to enter my face and it unlocks and also brings up any passwords I may forgotten."* (R164)

However, like password managers, biometric authentication is not always available. 58 (17%) of respondents mentioned this, and further commented that when biometrics were not available, they felt like the authentication process was worse. This was especially bad on key devices, like game consoles, where respondents had already indicated that authenticating on those devices was harder than normal. The unavailability of biometrics even caused some respondents to not use a specific service because of how valuable they were to some respondents.

> *"If i cant use fingerprint sometimes i won't even bother creating [an] account especially if it have long password requirements"* (R317)

> *"Using a controller for the Xbox can seem clunkier and harder to use. It would be useful for Xbox to have a fingerprint identification system. "* (R446)

Furthermore, it was interesting to see that there are 117 (35%) respondents who commented that biometrics were inaccurate for them to some degree.

Table 5.9: List of comments about biometrics and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

		Count (% Theme; % Overall)
		333 (33%)
Biometrics	Prefers Biometrics	242 (73%; 24%)
	Biometrics Not Available	58 (17%; 6%)
	Biometrics Inaccurate	117 (35%; 12%)
	Distrusts Biometrics	16 (5%; 2%)
	Dislikes Biometrics	2 (1%; 0%)

This lack of accuracy negated the main benefit of speed offered by biometric authentication, and caused some respondents to stay away from biometrics. This is also interesting because 16 (5%) respondents also commented about how they did not trust biometrics, and 2 respondents explicitly stated that they did not like biometric authentication. As with password managers, some of these negative comments about biometrics were a factor of not understanding exactly how biometrics allowed one to authenticate. Others, however, were about legitimate security concerns revolving around the fact that biometrics can be used without the user intending for them to be used.

> *"Im sure face authentication seems uncomortable and sometimes even dangerous."* (R608)

> *"Remembering passwords is hell, but I'm uncomfortable with forms of authentication that bypass passwords such as facial recognition and fingerprint authentication, so I feel kind of stuck."* (R791)

> *"The fingerprint is not ideal as it is highly easy for anyone to get access to a phone with your fingerprint. At least with people at home or over night visitors. Example: my son placed my thumb on my phone, while I was asleep, and unlocked my phone to play games on my phone..."* (R988)

These mixed views on biometrics mean that they, like password managers, are not a perfect replacement for standard password authentication. However, it does seem to appease some user complaints in limited capacities, so there is still some value to augmentations like these.

5.5.3 Multi-Factor Authentication

In addition to comments about password manages and biometrics, 71 (7%) respondents also left some comments about multi-factor authentication. These comments

are summarized in Table 5.10. While not many people mentioned multi-factor authentication, more people (46, 65%) mentioned that they did not like it compared to those who did mention that they liked it (23, 35%).

While those who disliked multi-factor authentication seemed to dislike the key component, needing another device besides the one you are authenticating on, some mentioned that they still enjoyed the security that it brought. Other comments included practical problems with multi-factor authentication, such as requiring more time to authenticate or not having access to the codes being generated by multi-factor authentication.

> *"Multi factor authentication slows the process down. Having different criteria for different passwords can also be annoying - eg having the have different numbers of characters or special characters."* (R271)

> *"I dislike getting verification codes because I recently changed my number and don't have access to my previous phone number anymore."* (R766)

> *"I don't want to have multiple manual steps to authenticate. If I need to confirm a login I want the confirmation step to be automatic on my device. When an app reads a code from messaging to confirm. I've actually given up logging in when pressed for time on some apps."* (R882)

Table 5.10: List of comments about multi-factor authentication and how many participants indicated each comment. Percentages recorded include the percentage within the theme and percentage of overall responses.

	Count (% Theme; % Overall)		
Any Multi-Factor Comment	71	(100%;	7%)
Prefers Multi-Factor Authentication	25	(35%;	3%)
Multi-Factor Unavailable	4	(6%;	0%)
Distrusts Multi-Factor	1	(1%;	0%)
Dislikes Multi-Factor	46	(65%;	5%)

Chapter 6

Discussion

While the data is showing us what users are actively doing, we also want to comment about what could be done in response to user activity to help mitigate some unsafe habits. Furthermore, we want to comment on what current user habits might imply about how likely users are to adopt new systems and models for authentication in the future.

6.1 Bad Password Habits

Perhaps the biggest issue presented in this data that users are facing when it comes to authenticating on different devices is that they change their passwords based on the device they are using. As respondents R498 and R592 say, the device they use impacts the composition of their passwords.

> *"If I do not store confidential data on a given device, I come up with a simple password."* (R498)

> *"If it's on a device like xbox, ps or nintendo switch, I tend to use a more simple password or a password where the letters are all closeby"* (R592)

Combining these comments with the results from section 5 which showed that over half of the respondents change their password composition based on the device

they are using or will wait to create the account until they can use their preferred device type, it is clear that there is a lot of evidence that the usability of the devices, and the underlying input modalities, greatly impacts the authentication process on devices.

This is problematic for all of the reasons already shown in the literature about the need for strong passwords in addition to being frustrating for users when they cannot immediately create accounts because the device they are using is too burdensome to use. However, it is hard to say that the users are completely at fault. Many of these device input modalities simply are not what synergistic with password based authentication, but this also does not mean we can overlook this problem.

6.1.1 More Options for Authentication

One way to combat bad password habits would be to allow users to have more authentication options. As noted by R713, some websites and services that allow you to use a QR code to authenticate, but there are other websites and services that do not.

> *'...Now, when I am thinking, there are also some websites (very known websites) where it is impossible to use the QR scan....even if such an option exists, so, I use the link to update some engines on this website. All this is really annoying because I don't want to use my laptop just to go and check some info, I prefer to do it with my phone, which seems faster but in fact, it is not because of the issues I encounter with some websites I use"* (R713)

If this option for single sign-on was more readily available to users, then perhaps they would not have to make weaker passwords for some accounts. One of the main frustrations with input modalities was through using a game console controller or a TV remote to authenticate because one had to select each letter individually by

using arrow keys to scroll over to the letter. If single sign-on could even just be more available for these sets of devices, that would remove a lot of frustration users have with authentication. Further research could be done to understand the obstacles of allowing these systems to be more widespread. We also present another promising mitigation to bad password habits by way of password manager modifications in section 7.

6.2 Adopting New Models of Authentication

Part of the data collected in this research seems to suggest potential roadblocks to adopting any new models of authentication. While there may be no new models of authentication to speak of right now, we can still talk about what a new model of authentication would have to do in order to help users adopt it faster.

6.2.1 Avoidance

This research has shown that users are actively avoiding services when it is hard or inconvenient to authenticate. More than 50% of our respondents admitted to wanting to wait to create an account until they could do so on their preferred device type. Furthermore, many users explicitly commented that when the process was too hard or slow, they would give up and avoid using a service altogether. Some examples of such responses were R387 and R714.

> *"according to the device I am using, it is more or less quick and easy to authenticate. when it's complicated it's frustrating and sometimes I just give up"* (R387)

> *"for example, using the remote control to enter a pin is extremely slow and stressful, that is why I often avoid using a platform from the TV if it needs authentication"* (R714)

In terms of impact on future work, it seems like any new models of authentication will need to focus on the user experience to prevent frustration or slowness from causing users to give up on the authentication process.

6.2.2 Comparison to Already Present Models

In addition to not causing frustration that leads to avoidance, it is also likely that new authentication models will need to work as smoothly as how users perceive current augments to password authentication working. The biggest example of this is the use of biometrics for authentication. Here, two things must be understood.

First, it seems like at least a portion of respondents did not understand exactly how biometrics worked, so their perceived ease of use and security might not be what one would expect or agree with if they are intimately familiar with the inner-workings of these systems. Second, perhaps because there is not a great depth of understanding of how biometrics work, the perception of biometrics is that it may or may not have to do with a password, but it authenticates quickly and without much hassle. Therefore, a new model of authentication would have to hold the speed of biometrics as a standard that users will compare it to when it is used.

Additionally, users already dislike multi-factor authentication because it prolongs the authentication process and adds more complexity. This is even the view of some users who understand that multi-factor authentication helps with account security. Therefore, a new authentication model would need to take into account the pre-existing dislike of multi-factor authentication and find a way to either justify it to the users or work around it so that it does not impact the users as much.

6.2.3 Informed Use

It would also be helpful for new models of authentication to explain clearly how they work so users can make more accurate judgments about how secure they consider these models of authentication, which could factor into whether they will use them or

not. Being more informed about the method of authentication a new model presents would also help users understand what problems this new model does and does not actually solve. For example, some respondents presented responses that seemed to indicate that they thought biometrics removed the need for passwords. However, those respondents that have had biometrics fail know that password based authentication is still available for their account in many cases. This means that biometrics are not completely replacing passwords and therefore, for example, not preventing users from needing to still create strong passwords.

Chapter 7

Conclusion and Future Work

The effects of this research have been to provide more information to fill in the knowledge gap about what devices users are authenticating on and what device-specific and input-modality-specific challenges they are running into. We now have a list of devices that users are authenticating on, with information about how frequently they are using these devices and how frequently they are using specific input modalities to authenticate.

We also set out to get a better understanding of users' needs and frustrations when authenticating on different devices. Throughout the research, it has been seen that the types of devices that users use do matter, not only explicitly to users through active frustration, refusal to engage with specific services, the unavailability of key tools like password managers and biometrics, and elongated authentication times, but also implicitly through users modifying their account creation habits to accommodate for different devices and input modalities.

Users also allow the device and input modalities to dictate password composition. To this end, users indicate without prompting that they are changing their passwords to better fit the device they are using and waiting to make accounts until they can use the device they like best. It is clear that users desire an authentication scheme

or process that does not require them to bear the burden of complexity for security's sake nor the burden of memorizing the passwords.

Additionally, physical input modalities seem to be the ones favored most by users in terms of usability, but phones remain the device that users authenticate on the most. This means that users sometimes would prefer not to use their phone but either out of convenience or necessity, they use their phone and a virtual keyboard instead of some physical input method.

While some users seem to talk about security and being able to put up with longer authentication processes if it means that their data is more secure, it seems like many other users are quick to point out that they prefer convenient authentication processes and would rather the process be fast over the process being secure.

In addition to these takeaways, we also present some ideas for further research. One exciting prospect for users would be the modification of password managers to better suite user needs. This could potentially be a password manager that took into account the device the user was authenticating on in order to create passwords tailored to that device. We would like to conduct further research to understand exactly how these systems would work, but we propose a preliminary idea where the proximity of characters is taken into account when generating passwords, which would help when entry is limited to the use of a controller with arrow keys on a virtual keyboard. Furthermore, password managers could be modified to take into account device-specific shortcuts for switching virtual keyboard layouts in order to access specific character in different character sets with fewer clicks.

Another concept would be trying to bring password managers over to devices like game consoles and TVs where they are currently lacking. Such a migration would require an understanding of the technical specifications of these devices, but, if possible, would greatly help those users who are already using password managers and might even help promote the use of password managers.

The increased use of password managers in either case is exciting because, as mentioned previously in section 2, users are not using the full capacity of password

managers. So, any effort that would help users use password managers more would be very helpful.

Bibliography

Bobeth, J., Schrammel, J., Deutsch, S., Klein, M., Drobics, M., Hochleitner, C., and Tscheligi, M. (2014). Tablet, gestures, remote control? influence of age on performance and user experience with itv applications. In *Proceedings of the ACM International Conference on Interactive Experiences for TV and Online Video*, TVX '14, pages 139–146, New York, NY, USA. Association for Computing Machinery. 8

Bonneau, J., Herley, C., van Oorschot, P., and Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the Thirty-Third IEEE Symposium on Security and Privacy*, pages 553–567. IEEE. 1

Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X. (2014). The Tangled Web of Password Reuse. In *Network and Distributed System Security (NDSS)*, volume 14, pages 23–26. 1

Dell'Amico, M., Michiardi, P., and Roudier, Y. (2010). Password strength: An empirical analysis. In *2010 Proceedings IEEE INFOCOM*, pages 1–9. IEEE. 1

Fagan, M., Albayram, Y., Khan, M. M. H., and Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7(1):12. 1

Florencio, D. and Herley, C. (2007). A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657–666. ACM. 1

Greene, K., Franklin, J. M., and Kelsey, J. M. (2015). Tap on, tap off: onscreen keyboards and mobile password entry. Technical report, NIST. 5

Greene, K. K., Gallagher, M. A., Stanton, B. C., and Lee, P. Y. (2014). I can't type that! p$$w0rd entry on mobile devices. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 160–171. Springer. 5

Jakobsson, M. and Akavipat, R. (2011). Rethinking passwords to adapt to constrained keyboards. 6

Jones, J. M., Duezguen, R., Mayer, P., Volkamer, M., and Das, S. (2021). A literature review on virtual reality authentication. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*, pages 189–198. Springer. 8

Karat, C.-M., Halverson, C., Horn, D., and Karat, J. (1999). Patterns of entry and correction in large vocabulary continuous speech recognition systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '99, pages 568–575, New York, NY, USA. Association for Computing Machinery. 6

Kürtünlüoğlu, P., Akdik, B., and Karaarslan, E. (2022). Security of virtual reality authentication methods in metaverse: An overview. 7

Lee, S. and Zhai, S. (2009). The performance of touch screen soft buttons. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, pages 309–318, New York, NY, USA. Association for Computing Machinery. 7

Lyastani, S. G., Schilling, M., Fahl, S., Backes, M., and Bugiel, S. (2018). Better managed than memorized? studying the impact of managers on password strength and reuse. In *USENIX Security Symposium*, pages 203–220. 2, 4

MacKenzie, I. S. and Soukoreff, R. W. (2002). Text entry for mobile computing: Models and methods,theory and practice. *Human-Computer Interaction*, 17(2-3):147–198. 7

Oesch, S., Gautam, A., and Ruoti, S. (2016). "it basically started using me:" An observational study of password manager usage. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 4298–4308. ACM. 2, 5

Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Forget, A. (2017). Let's go in for a closer look: Observing passwords in their natural habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 295–310. ACM. 1

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., and Cranor, L. F. (2019). Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2019)*. 1, 4

Ray, H., Wolf, F., Kuber, R., and Aviv, A. J. (2021). Why older adults (don't) use password managers. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association. 1

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, 8(1):2833–2836. 1

Ruoti, S., Roberts, B., and Seamons, K. (2015). Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th international conference on World wide web*. International World Wide Web Conferences Steering Committee. 1

Scorecard, S. (2018). Statistics: Cybersecurity data breaches on the rise. https://securityscorecard.com/blog/cybersecurity-data-breaches-statistics-on-the-rise. Accessed: 2023-02-22. v, 1

Verizon (2021). Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/. Accessed: 2023-02-22. v, 1

Appendix

Appendix A

A.1 Survey

A.1.1 Page 1

In our research group, we are trying to understand on which devices people need to log in to an account. **The process of logging into an account is referred to as authentication.** We are studying this topic so that in future research we can help make the process of authenticating more seamless, regardless of the device you are using.

Being in this study is up to you. After completing the survey, we cannot remove your responses because we will delete any information linking you to your data. There are no risks or direct benefits associated with participation in this study. Results from this survey will be published in scientific publications. Please do not include your name or other identifying information in your survey responses.

If you have questions or concerns about this study, contact us at [email redacted]. For questions or concerns about your rights or to speak with someone other than the research team about the study, please contact: [contact information redacted].

Statement of Consent By continuing in the survey below, I am confirming that I have read the above information and am agreeing to be in this study. I can print or save a copy of this consent information for future reference. If I do not want to be in this study, I can close my internet browser.

A.1.2 Page 2

On which of the following have you entered a password or a PIN? (*Select all that apply*)

- *Desktop*
- *Laptop*
- *Phone*
- *Touchscreen tablet*
- *Smartwatch*
- *Smart speaker (e.g. Amazon Alexa)*
- *None of the above*

On which of the following have you entered a password or a PIN? (*Select all that apply*)

- *Nintendo Switch*
- *Xbox*
- *PlayStation*
- *Steam Deck*
- *VR*
- *Other game console* [text entry]
- *None of the above*

On which of the following have you entered a password or a PIN? (*Select all that apply*)

- *TV / smart TV*
- *thermostat / smart thermostat*
- *lock / smart lock*
- *safe / smart safe*
- *security alarm*
- *None of the above*

On which of the following have you entered a password or a PIN?
(*Select all that apply*)

- *kiosk computer or tablet*
- *printer*
- *physical keypad (such as when entering a building)*
- *ATM*
- *None of the above*

Are there any other devices on which you have entered a password or a PIN? Please enter them below.
[text entry]

A.1.3 Page 3

On which 3–5 devices do you most frequently enter a password or a PIN? Please enter them in order of frequency, from most frequent to least frequent.

- *Device 1* [text entry]

- *Device 2* [text entry]
- *Device 3* [text entry]
- *Device 4* [text entry]
- *Device 5* [text entry]

How often do you use the following entry methods to enter a password or a PIN?

Daily, A few times a week, A few times a month, A few times year, Never

- *Keyboard*
- *Mouse*
- *Touchscreen*
- *Physical PIN pad or dial*
- *TV remote*
- *Video game controller*
- *Other* [text entry]

A.1.4 Page 4

Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly agree

I **think there is a difference in how easy it is to enter passwords or PINs depending on what device I am using (for example, entering on an Xbox vs entering on a laptop).**

Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly agree

When creating passwords or PINs, I consider the types of devices where I will need to enter that password or PIN.

Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly agree

If I need to create an account, I wait until I can do it on my preferred device type rather than immediately creating the account on the device I am currently using.

A.1.5 Page 5

Please explain how the type of device you are using to enter a password or PIN impacts your experience.

[text entry]

What challenges do you face when entering passwords or PINs? What do you wish was easier about the process?

[text entry]

Is there anything else you want to tell us about entering passwords or PINs that could help us improve your experience?

[text entry]

A.1.6 Page 6

How old are you?

- *18-25*
- *26-35*
- *36-45*
- *46-55*
- *55+*
- *I prefer not to enter*

What is your sex?

- *Male*

- *Female*
- *I prefer not to enter*

What is your ethnicity?

- *White or Caucasian*
- *Black or African American*
- *Asian*
- *Pacific Islander*
- *Mixed race*
- *Other (specify)* [text entry]
- *I prefer not to enter*

What is the highest level of school you have completed or the highest degree you have received?

- *Less than high school degree*
- *High school graduate (high school diploma or equivalent including GED)*
- *Some college but no degree*
- *Associate's degree in college (2-year)*
- *Bachelor's degree in college (4-year)*
- *Master's degree*
- *Professional degree (JD, MD)*
- *Doctoral degree*
- *I prefer not to answer*

Appendix B

B.1 Tables With Demographic Breakdown

Table B.1: Demographics for the participants taking the study, less those that were removed for quality reasons.

		Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Participants		999 (100%)	601 (60%)	299 (30%)	99 (10%)
Gender	Male	495 (50%)	300 (50%)	149 (50%)	46 (46%)
	Female	486 (49%)	292 (49%)	144 (48%)	50 (51%)
	I prefer not to answer	18 (2%)	9 (1%)	6 (2%)	3 (3%)
Age	18-25	373 (37%)	282 (47%)	70 (23%)	21 (21%)
	26-35	343 (34%)	205 (34%)	103 (34%)	35 (35%)
	36-45	161 (16%)	83 (14%)	67 (22%)	11 (11%)
	46-55	72 (7%)	22 (4%)	34 (11%)	16 (16%)
	55+	47 (5%)	9 (1%)	24 (8%)	14 (14%)
	I prefer not to answer	3 (0%)	0 (0%)	1 (0%)	2 (2%)
Education	Less than high school degree	19 (2%)	12 (2%)	3 (1%)	4 (4%)
	High school graduate (high school diploma or equivalent including GED)	184 (18%)	130 (22%)	41 (14%)	13 (13%)
	Some college but no degree	191 (19%)	94 (16%)	73 (24%)	24 (24%)
	Associate's degree in college (2-year)	55 (6%)	30 (5%)	20 (7%)	5 (5%)
	Bachelor's degree in college (4-year)	337 (34%)	192 (32%)	109 (36%)	36 (36%)
	Master's degree	172 (17%)	117 (19%)	41 (14%)	14 (14%)
	Doctoral degree	15 (2%)	11 (2%)	3 (1%)	1 (1%)
	Professional degree (JD, MD)	18 (2%)	9 (1%)	8 (3%)	1 (1%)
	I prefer not to answer	8 (1%)	6 (1%)	1 (0%)	1 (1%)

Table B.2: The list of devices and how many participants indicated using them to enter passwords.

		Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
		997 (100%)	599 (100%)	299 (100%)	99 (100%)
	Phone	980 (98%)	590 (98%)	291 (97%)	99 (100%)
	Laptop	847 (85%)	499 (83%)	263 (88%)	85 (86%)
General	Desktop	644 (64%)	398 (66%)	189 (63%)	57 (58%)
	Tablet	477 (48%)	254 (42%)	170 (57%)	53 (54%)
	Smartwatch	127 (13%)	57 (9%)	58 (19%)	12 (12%)
	Smart speaker	36 (4%)	19 (3%)	13 (4%)	4 (4%)
		862 (86%)	496 (83%)	270 (90%)	96 (97%)
	ATM	819 (82%)	464 (77%)	262 (88%)	93 (94%)
Physical	Physical keypad	379 (38%)	194 (32%)	137 (46%)	48 (48%)
	Kiosk computer or tablet	168 (17%)	69 (11%)	82 (27%)	17 (17%)
	Printer	136 (14%)	72 (12%)	37 (12%)	27 (27%)
		570 (57%)	320 (53%)	187 (63%)	63 (64%)
	TV / Smart TV	416 (42%)	238 (40%)	127 (42%)	51 (52%)
Smart	Security alarm	165 (17%)	78 (13%)	68 (23%)	19 (19%)
	Lock / Smart lock	141 (14%)	75 (12%)	58 (19%)	8 (8%)
	Safe / Smart safe	112 (11%)	55 (9%)	47 (16%)	10 (10%)
	Thermostat / Smart thermostat	34 (3%)	12 (2%)	17 (6%)	5 (5%)
		447 (45%)	246 (41%)	158 (53%)	43 (43%)
	PlayStation	265 (27%)	147 (24%)	91 (30%)	27 (27%)
	Xbox	180 (18%)	88 (15%)	77 (26%)	15 (15%)
Gaming	Nintendo Switch	178 (18%)	85 (14%)	80 (27%)	13 (13%)
	VR headset	36 (4%)	16 (3%)	19 (6%)	1 (1%)
	Other game console	23 (2%)	13 (2%)	9 (3%)	1 (1%)
	Steam Deck	22 (2%)	8 (1%)	10 (3%)	4 (4%)
		101 (10%)	59 (10%)	29 (10%)	13 (13%)
	POS	16 (2%)	12 (2%)	2 (1%)	2 (2%)
	Doors	11 (1%)	5 (1%)	3 (1%)	3 (3%)
	Touchscreen tablet	8 (1%)	4 (1%)	4 (1%)	0 (0%)
	Nintendo DS	7 (1%)	6 (1%)	1 (0%)	0 (0%)
Other	Biometrics	6 (1%)	3 (0%)	1 (0%)	2 (2%)
	Locker	5 (1%)	4 (1%)	1 (0%)	0 (0%)
	Time Clock Machine	5 (1%)	2 (0%)	0 (0%)	3 (3%)
	Gates	5 (1%)	4 (1%)	1 (0%)	0 (0%)
	Safe	5 (1%)	2 (0%)	3 (1%)	0 (0%)
	Car	5 (1%)	0 (0%)	5 (2%)	0 (0%)

Table B.3: List of comments about virtual keyboards and how many participants indicated each comment.

Theme	Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
	Any Virtual Keyboard Comment	421 (100.00%)	253 (100.00%)	123 (100.00%)	45 (100.00%)
Virtual Keyboards are Hard	Virtual Keyboard Entry Hard	56 (13.30%)	33 (13.04%)	17 (13.82%)	6 (13.33%)
	Mobile Entry Hard	65 (15.44%)	42 (16.60%)	15 (12.20%)	8 (17.78%)
	Mobile Entry Slow	14 (3.33%)	10 (3.95%)	3 (2.44%)	1 (2.22%)
	Touchscreen Entry Hard	23 (5.46%)	15 (5.93%)	6 (4.88%)	2 (4.44%)
Controller Entry is Hard	Game Entry Hard	107 (25.42%)	60 (23.72%)	34 (27.64%)	13 (28.89%)
	Game Entry Slow	38 (9.03%)	18 (7.11%)	15 (12.20%)	5 (11.11%)
	Game Arrow Key Entry Bad	25 (5.94%)	13 (5.14%)	9 (7.32%)	3 (6.67%)
	Game Entry Uncomfortable	4 (0.95%)	4 (1.58%)	0 (0.00%)	0 (0.00%)
	TV Entry Hard	109 (25.89%)	62 (24.51%)	38 (30.89%)	9 (20.00%)
	TV Entry Slow	109 (25.89%)	62 (24.51%)	38 (30.89%)	9 (20.00%)
	TV Arrow Key Entry Bad	32 (7.60%)	14 (5.53%)	16 (13.01%)	2 (4.44%)
	TV Entry Uncomfortable	2 (0.48%)	2 (0.79%)	0 (0.00%)	0 (0.00%)
Touchscreens May Be Better	Touchscreen Entry Fast	4 (0.95%)	2 (0.79%)	0 (0.00%)	2 (4.44%)
	Touchscreen Entry Easy	35 (8.31%)	20 (7.91%)	9 (7.32%)	6 (13.33%)
	Mobile Entry Easy	78 (18.53%)	47 (18.58%)	25 (20.33%)	6 (13.33%)
	Mobile Entry Fast	13 (3.09%)	10 (3.95%)	1 (0.81%)	2 (4.44%)

Table B.4: List of comments about virtual keyboard layout and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Virtual Keyboard Comment	421 (100.00%)	253 (100.00%)	123 (100.00%)	45 (100.00%)
Special Characters Hard to Use	35 (8.31%)	21 (8.30%)	10 (8.13%)	4 (8.89%)
Layout Switching Hard	20 (4.75%)	13 (5.14%)	4 (3.25%)	3 (6.67%)
Virtual Keyboard Layout Matters	22 (5.23%)	15 (5.93%)	6 (4.88%)	1 (2.22%)
Familiarity Matters	43 (10.21%)	28 (11.07%)	11 (8.94%)	4 (8.89%)

Table B.5: List of comments about physical devices and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Physical Entry Comment	271 (100.00%)	176 (100.00%)	68 (100.00%)	27 (100.00%)
Physical Entry Easy	221 (81.55%)	141 (80.11%)	59 (86.76%)	21 (77.78%)
Physical Entry Hard	10 (3.69%)	7 (3.98%)	2 (2.94%)	1 (3.70%)
Physical Entry Fast	47 (17.34%)	32 (18.18%)	9 (13.24%)	6 (22.22%)
Physical Entry Comfortable	8 (2.95%)	8 (4.55%)	0 (0.00%)	0 (0.00%)
Physical Entry Less Mistakes	5 (1.85%)	4 (2.27%)	0 (0.00%)	1 (3.70%)

Table B.6: List of comments about speed and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Speed Comment	143 (100.00%)	91 (100.00%)	38 (100.00%)	14 (100.00%)
Physical Entry Fast	47 (32.87%)	32 (35.16%)	9 (23.68%)	6 (42.86%)
Physical Entry Slow	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Mobile Entry Fast	13 (9.09%)	10 (10.99%)	1 (2.63%)	2 (14.29%)
Mobile Entry Slow	14 (9.79%)	10 (10.99%)	3 (7.89%)	1 (7.14%)
Touchscreen Entry Fast	4 (2.80%)	2 (2.20%)	0 (0.00%)	2 (14.29%)
Touchscreen Entry Slow	3 (2.10%)	2 (2.20%)	1 (2.63%)	0 (0.00%)
Game Entry Fast	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Game Entry Slow	38 (26.57%)	18 (19.78%)	15 (39.47%)	5 (35.71%)
TV Entry Fast	0 (0.00%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
TV Entry Slow	42 (29.37%)	24 (26.37%)	14 (36.84%)	4 (28.57%)

Table B.7: List of comments about cross-device considerations and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Devices Has Impact	855 (85.59%)	523 (87.02%)	249 (83.28%)	83 (83.84%)
Device Has No Impact	53 (5.31%)	32 (5.32%)	15 (5.02%)	6 (6.06%)
Comfort Matters	11 (1.10%)	11 (1.83%)	0 (0.00%)	0 (0.00%)
Device Size Matters	69 (6.91%)	42 (6.99%)	17 (5.69%)	10 (10.10%)
Mistakes Matter	57 (5.71%)	37 (6.16%)	14 (4.68%)	6 (6.06%)
Mistakes Cause Challenges	74 (7.41%)	51 (8.49%)	17 (5.69%)	6 (6.06%)
Frequency of Authentication Matters	12 (1.20%)	7 (1.16%)	5 (1.67%)	0 (0.00%)
Security Matters	83 (8.31%)	66 (10.98%)	8 (2.68%)	9 (9.09%)

Table B.8: List of comments about passwords and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Password Comment	340 (100.00%)	180 (100.00%)	118 (100.00%)	42 (100.00%)
Remembering Passwords Hard	250 (73.53%)	127 (70.56%)	88 (74.58%)	35 (83.33%)
Creating New Passwords Hard	24 (7.06%)	15 (8.33%)	7 (5.93%)	2 (4.76%)
Creating Unique Passwords Hard	50 (14.71%)	19 (10.56%)	24 (20.34%)	7 (16.67%)
PCP Requirements Bad	76 (22.35%)	36 (20.00%)	30 (25.42%)	10 (23.81%)

Table B.9: List of other comments about passwords and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Password Lifecycle or Hardware Comment	405 (100.00%)	223 (100.00%)	136 (100.00%)	46 (100.00%)
Hardware Doesn't Always Work	59 (14.57%)	37 (16.59%)	19 (13.97%)	3 (6.52%)
Authentication Frequency High	12 (2.96%)	7 (3.14%)	5 (3.68%)	0 (0.00%)
Password Forced Reset	24 (5.93%)	15 (6.73%)	7 (5.15%)	2 (4.35%)
Password Recovery Hard	16 (3.95%)	8 (3.59%)	6 (4.41%)	2 (4.35%)
Account Lockout Frustrating	6 (1.48%)	3 (1.35%)	2 (1.47%)	1 (2.17%)

Table B.10: List of comments about usability and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Any Usability Impacts Comment	60 (100.00%)	28 (100.00%)	26 (100.00%)	6 (100.00%)
Usability Impacts Length	28 (46.67%)	13 (46.43%)	10 (38.46%)	5 (83.33%)
Usability Impacts Complexity	35 (58.33%)	15 (53.57%)	17 (65.38%)	3 (50.00%)
Usability Impacts Reuse	1 (1.67%)	1 (3.57%)	0 (0.00%)	0 (0.00%)
Usability Impacts Usage	6 (10.00%)	1 (3.57%)	5 (19.23%)	0 (0.00%)

Table B.11: List of comments about password managers and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Uses Password Manager	157 (15.72%)	89 (14.81%)	49 (16.39%)	19 (19.19%)
Wants Password Manager	22 (2.20%)	7 (1.16%)	12 (4.01%)	3 (3.03%)
Password Manager Not Available	67 (6.71%)	39 (6.49%)	21 (7.02%)	7 (7.07%)
Password Manager Syncing Issues	6 (0.60%)	2 (0.33%)	3 (1.00%)	1 (1.01%)
Distrusts Password Manager	17 (1.70%)	14 (2.33%)	2 (0.67%)	1 (1.01%)

Table B.12: List of comments about biometrics and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Prefers Biometrics	242 (24.22%)	152 (25.29%)	63 (21.07%)	27 (27.27%)
Biometrics Not Available	58 (5.81%)	29 (4.83%)	22 (7.36%)	7 (7.07%)
Biometrics Inaccurate	117 (11.71%)	78 (12.98%)	30 (10.03%)	9 (9.09%)
Distrusts Biometrics	16 (1.60%)	10 (1.66%)	4 (1.34%)	2 (2.02%)
Dislikes Biometrics	2 (0.20%)	2 (0.33%)	0 (0.00%)	0 (0.00%)

Table B.13: List of comments about multi-factor authentication and how many participants indicated each comment.

Comment	Overall (Overall %)	EU (EU %)	USA (USA %)	UK (UK %)
Prefers Multi-Factor Authentication	25 (2.50%)	12 (2.00%)	12 (4.01%)	1 (1.01%)
Multi-Factor Unavailable	4 (0.40%)	4 (0.67%)	0 (0.00%)	0 (0.00%)
Distrusts Multi-Factor	1 (0.10%)	0 (0.00%)	1 (0.33%)	0 (0.00%)
Dislikes Multi-Factor	46 (4.60%)	17 (2.83%)	25 (8.36%)	4 (4.04%)

Vita

John Ezat Sadik was born in Cairo, Egypt. He was born to two loving and Christian parents. Shortly after his birth, his family immigrated to the United States. It was in the United States that he completed highschool and the went to college. John attended the University of Tennessee, Knoxville (UTK) for his undergraduate college career. He had a major in computer science and a double minor in math and cybersecrutiy. In the course of completing his undergraduate degree at UTK, he got involved with research in Dr. Scott Ruoti's research lab.

Continuing on into his master's degree, he continued working with Dr. Scott Ruoti. His work, as outlined in this thesis, was concentrated on password managers and their usage. In his free time, John consistently attended church, led a Bible study on campus, and was involved with other Christian organizations. Working on his thesis was a new challenge for John, but through hard work and the help of his community, he was able to get through it and finally get his thesis accepted. After completing this master's degree in comptuer science, John was accepted into the PhD program at UTK.

Throughout his life, and especially during college, John loved to debate and explore ideas, and whenever he found an opportunity to do so, he woud always take it. Furthermore, John enjoyed building small computer science projects to help make his life a little easier.