Study of Deployed Authentication Mechanisms

A Major Qualifying Project submitted to the faculty of

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfilment of the requirements for the degree of Bachelor of Science

By Charles Anderson, Ian Grzembski,

Daniel Onyema, and Caitlyn Puiia

April 2024

Advisor: Professor Craig E. Wills

Abstract

This project studies the use and perception of two-factor authentication (2FA) and multi-factor authentication (MFA). Our background research relates to the different mechanisms of 2FA and MFA there are. We interviewed a few companies and larger organizations to understand their usage of 2FA and MFA and how this relates to the general public's perception. To understand the usage and prevalence of different authentication mechanisms, we compiled and classified 95 popular websites that people use daily. We also created a survey asking the general population how convenient or efficient these factors are in their opinion. We found that businesses and users alike tend to prioritize usability over security unless their insecurity caused them to be hacked, which backs up why we found 91 of the websites we researched had made MFA optional. It was also discovered that users found biometrics the most convenient and secure and secure of the provided authentication mechanisms. Physical security keys were considered the least convenient and email was considered the least secure by users. We anticipate our research will help businesses understand what MFA mechanisms exist, what the public thinks of what they have currently, and how effective what they are using is security-wise.

Table of Contents

List of Figures

1. Introduction

Authentication is an important aspect of technology and security in modern society. It determines that the user is who they say they are and that the data they are viewing is accurate for them. Authentication comes in many forms: people can visually verify that they are 21 at a bar by looking at the person's ID, or biometrically verify their identity through Face ID on some Apple devices. The main form of authentication we investigate in this project is passwords; specifically, the use of passwords coupled with other forms of authentication, also known as Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA).

As cyber threats become increasingly sophisticated, single-password authentication is no longer a secure way to authenticate a user. MFA can help remedy the lack of security of passwords. When a user inputs a correct password, they are then prompted with another task, such as inputting a string of numbers sent by SMS or through a notification on an application. This second step may also be followed by another form of authentication. As MFA has become a topic of interest recently, there is a gap between how quickly researchers recommend new authentication mechanisms and how well businesses, websites, and other organizations implement these new mechanisms. There is no standard operating procedure for these authentication mechanisms; therefore, there is no baseline when new procedures are introduced and implemented. Also, new procedures such as MFA are not well accepted by the larger population who are often resistant to change that may be tedious.

Our project aims to outline these gaps, help those organizations better understand where they can go with authentication, and how they can help users perceive and accept the new measures of authentication. We achieved this goal by understanding how businesses currently interact with authentication mechanisms, which mechanisms are commonly used in industry, and users' perception of these commonly used mechanisms.

The remainder of the report is organized as follows. In Chapter 2, we discuss password-only authentication, and how its inefficacy paved the way for MFA. We describe our three-pronged approach to study deployed authentication mechanisms in Chapter 3, involving interviews with businesses, case studies with 95 commonly used websites, and a survey of user perspectives on authentication. We present our findings in Chapters 4-6, synthesize results from these three methods in Chapter 7, and discuss how our findings could impact industry in Chapter 8.

2. Background

In this section, we introduce both password-only authentication and multi-factor authentication and analyze what literature has found about these mechanisms. We start by analyzing password-only authentication and why its insecurities led to the introduction of multi-factor authentication.

2.1: Password-only Authentication

Passwords have served as a primary method of authentication since the inception of digital systems; however, their effectiveness in safeguarding user accounts against unauthorized access has been questioned. Passwords are susceptible to known vulnerabilities such as brute-force attacks, malware attacks, phishing attacks, and hash cracking, significantly compromising their reliability as a sole authentication factor [11]. Moreover, human factors such as users' tendency to choose weak passwords or share them inadvertently further undermine their efficacy. Password keyspace also plays a large factor in the effectiveness of a password, as the limitations on the possibility of specific characters in a password may give leverage to an attacker. Keyspace refers to the total range of different possible values of a key, password, pin, etc. A password with n characters, where each of those characters can have c different values, will have a keyspace size of $k_p = c^n$ [8]. If a website requires that a user make a password up to $n = 10$ characters using only the 26 letters of the alphabet and whitespace ($c = 27$), the keyspace size is $27^{10} \approx 2.059 \cdot 10^{14}$ unique passwords. The password keyspace size k_p relates directly to the maximum entropy H_{max}, which is calculated with the following formula: $H_{max} = \log_2(k_p)$ [in bits] [8]. Continuing from the prior example, a website with a password keyspace of $2.059 \cdot 10^{14}$ has a statistical entropy of 44.51 bits. While that space seems large, the entropy decreases when one recalls that users tend to pick memorable words or phrases for their passwords. Assuming that there are a billion words across all languages (approximately half of a billion words) and that a user was likely to use one of those words for a password, the keyspace would drop to 10^9 and the statistical entropy to 29.9 bits. That is a significant loss in both keyspace and entropy, reducing the amount of work it takes for attackers to determine one's password, even with brute force. Over time, the inadequacies of traditional password practices have prompted the development of stringent password policies and conventions. These include requirements for password complexity, length, and rotational updates. However, studies suggest that while such policies may enhance security to some extent, they often impose burdens on users and may lead to unintended consequences, such as users resorting to insecure practices to comply with the requirements [5][9]. For instance, password expiration requirements may prompt users to choose easily guessable passwords or resort to writing them down, thereby negating the intended security benefits. These policies also do nothing to stop phishing or malware attacks, which is why these attacks are more commonly used against password-only authentication systems [11].

2.2: Multi-Factor Authentication

The shortcomings of passwords have catalyzed the adoption of multi-factor authentication (MFA) as an additional layer of security. MFA combines two or more authentication factors—something the user knows, has, or are—to verify identities. This approach mitigates the limitations of passwords by requiring multiple forms of authentication, thereby enhancing security [10]. MFA encompasses various authentication methods, each offering distinct advantages in terms of security and usability. The commonly used authentication mechanisms examined in this report are SMS, email, phone calls, third party apps, biometrics, time-based one-time passwords (TOTP), and physical security keys such as YubiKey.

SMS, email-based authentication, and phone calls, while being easy and cheap to implement, have been shown to be the least secure and not usable. Although they provide an additional layer of authentication beyond passwords, they are vulnerable to interception through techniques like SIM swapping and phishing attacks. Moreover, reliance on SMS as a delivery channel poses risks associated with the security of the telecommunication infrastructure. Similarly, email-based authentication suffers from similar vulnerabilities, along with the added risk of compromised email accounts leading to unauthorized access [1]. Phone calls are similarly manipulatable through call rerouting and phone number spoofing [11]. Users also tended to dislike that SMS and phone call-based authentication required them to have an external device to authenticate [6][10], which is a common theme among MFA mechanisms. Despite their shortcomings, SMS and email-based authentication methods remain popular among businesses due to their widespread availability and ease of implementation, particularly in contexts where higher security requirements are not a primary concern.

Third-party authentication apps and TOTP offer a more secure alternative to SMS and email-based authentication methods. These apps generate time-limited codes that users input alongside their passwords during the authentication process. Unlike SMS, they are not vulnerable to interception via SIM swapping or phishing attacks. Additionally, TOTP-based authentication does not rely on external communication channels, reducing the risk of interception [10]. However, users of these mechanisms are concerned about the potential for device loss or failure. Since third-party authentication apps are often tied to a specific device, if the user loses access to that device or it malfunctions, they may face difficulties accessing their accounts. Additionally, the setup process for third-party authentication apps can be more complex compared to other methods, potentially leading to usability issues, especially for less tech-savvy users [2]. Moreover, reliance on the time-sensitive nature of TOTP codes may cause inconvenience if the user's device clock is out of sync or if they encounter network connectivity issues [2]. Third-party authentication apps and TOTP remain popular choices for organizations seeking to enhance security with minimal sacrifices to usability.

Biometric authentication leverages unique biological traits such as fingerprints, facial features, and iris patterns for identity verification. This method offers a high level of security, as biometric data is inherently difficult to replicate or spoof. Moreover, biometric authentication enhances usability by eliminating the need for users to remember complex passwords or carry physical tokens [7]. However, concerns regarding privacy and data protection have been raised, as biometric data, once compromised, cannot be easily replaced. Additionally, the accuracy and reliability of biometric authentication systems may vary depending on factors such as environmental conditions and the quality of the biometric sensors used [2]. Biometric authentication continues to gain traction as a secure and user-friendly alternative to traditional authentication methods, especially for mobile devices [7].

Physical security keys, such as the FIDO2 YubiKey, provide a hardware-based approach to authentication. These devices generate cryptographic keys that are used to verify the user's identity during the authentication process. Physical security keys offer a high level of security, as they are immune to phishing attacks and other forms of online fraud. Additionally, their simplicity and ease of use make them an attractive option for both individual users and organizations. However, the widespread adoption of physical security keys may be hindered by factors such as cost and compatibility with existing systems [4]. Physical security keys represent a promising avenue for enhancing authentication security while ensuring a seamless user experience.

2.3: Summary

Authentication has become an integral part of cybersecurity. Password-only authentication was secure enough for a while and protected against most breaches. However, technology and breaches advancing along with more sensitive information being stored on websites and applications demanded stronger authentication practices such as 2FA and MFA. Along with this increased security comes change; people oftentimes dislike change and rebel against it which can defeat the purpose of security if authentication is too cumbersome. Our study compares the convenience and the effectiveness of mechanisms used in MFA along with password-only authentication.

3. Approach

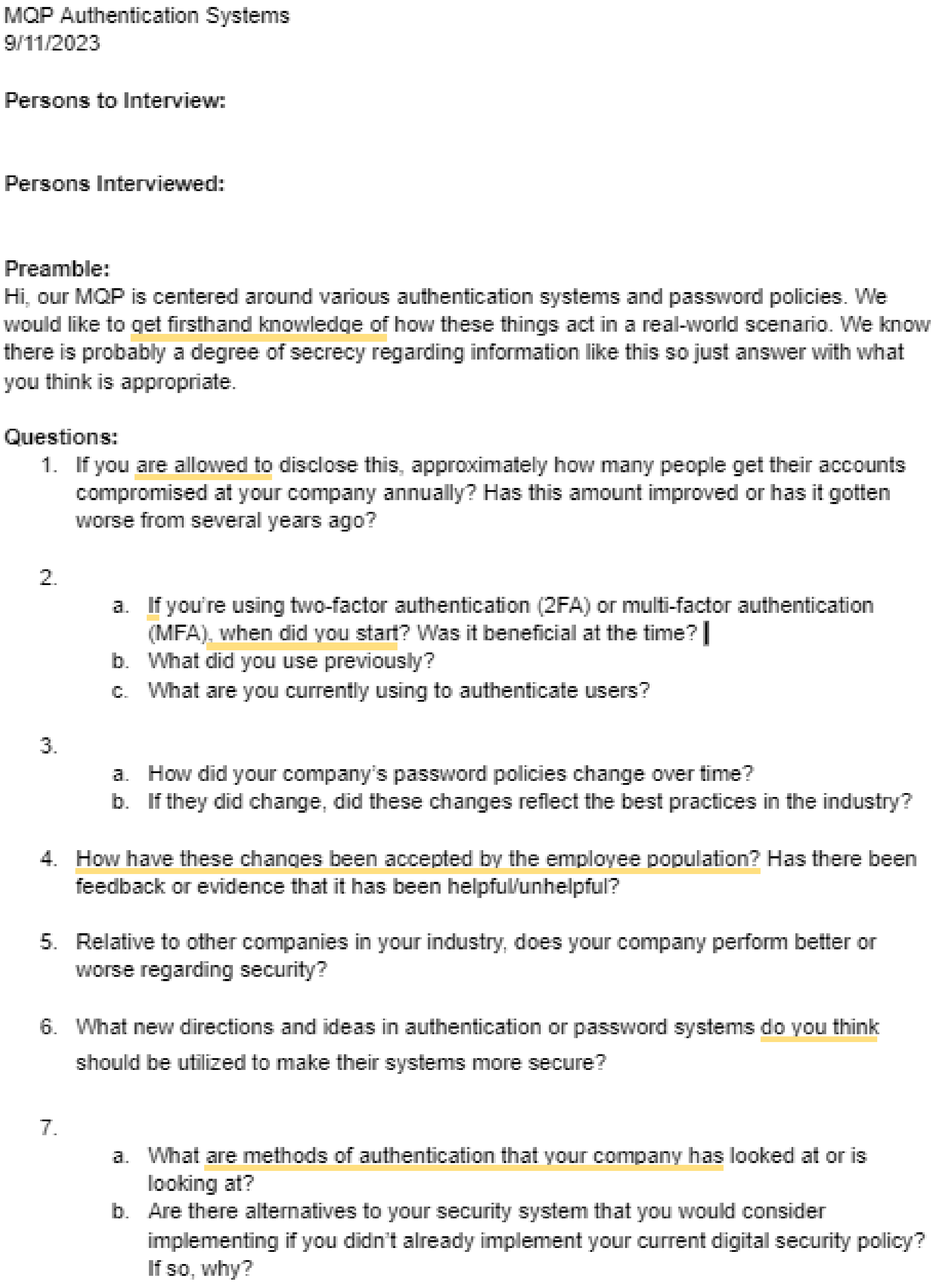
The goal of our project is to help companies implement authentication mechanisms guided by user perspectives on authentication and currently available security research. To achieve this goal, we pursue a three-pronged approach. Our first prong is interviewing different companies and organizations to gain insight as to what they are currently using as an authentication method. We hope to gain more information as to what is currently in place in industry. We also ask questions about how their employees perceived these new methods and if these methods reduced the amount of data breaches they have. We also want to further understand their logic behind choosing their authentication methods, how long they have implemented them, and how effective they perceive the methods to be.

The second prong to our approach is to compile a comprehensive list of widely used websites. This list consists of various categories of websites from banking and financial services to email and communications sites. We hope to understand the different forms of authentication used on these websites. We also hope to understand how widely used MFA was on these websites versus password-only authentication, and if MFA is enforced on these websites.

The third prong to our approach is a survey. We sent a survey to the public in hopes of understanding their perception of authentication mechanisms, password-only authentication, and MFA. We also want to know how widely used different authentication mechanisms are and the perception of those in terms of effectiveness. The surveys also provide us with user feedback about authentication and their thoughts about how it worked and how effective it was. With these three prongs of approach, we hope to create a comprehensive overview of the usage and perception of security in terms of convenience and security.

4. Company Interviews

Company interviews were the first prong in our approach to this project. To determine what authentication mechanisms are currently deployed, we conducted semi-structured interviews with various businesses not in the same industry. We planned to interview businesses of varying sizes that attended the WPI 2023 Fall Career Fair, which could provide a more holistic view of how different businesses choose authentication mechanisms to deploy. These interviews informed us why these different businesses use the authentication mechanisms they do, as well as their opinions on the backend of authentication. The questions we asked during these interviews are shown in Figure 1:



MQP Authentication Systems
9/11/2023

Persons to Interview:

Persons Interviewed:

Preamble:
Hi, our MQP is centered around various authentication systems and password policies. We would like to get firsthand knowledge of how these things act in a real-world scenario. We know there is probably a degree of secrecy regarding information like this so just answer with what you think is appropriate.

Questions:

1. If you are allowed to disclose this, approximately how many people get their accounts compromised at your company annually? Has this amount improved or has it gotten worse from several years ago?

2.
   a. If you're using two-factor authentication (2FA) or multi-factor authentication (MFA), when did you start? Was it beneficial at the time?
   b. What did you use previously?
   c. What are you currently using to authenticate users?

3.
   a. How did your company's password policies change over time?
   b. If they did change, did these changes reflect the best practices in the industry?

4. How have these changes been accepted by the employee population? Has there been feedback or evidence that it has been helpful/unhelpful?

5. Relative to other companies in your industry, does your company perform better or worse regarding security?

6. What new directions and ideas in authentication or password systems do you think should be utilized to make their systems more secure?

7.
   a. What are methods of authentication that your company has looked at or is looking at?
   b. Are there alternatives to your security system that you would consider implementing if you didn't already implement your current digital security policy? If so, why?

Figure 1: Interview questions sent to businesses.

Data collection involved recording and transcribing the interviews verbatim to code participants' responses and find common trends. We also had a few companies that we only communicated with through email, which gave us an easy interview transcript. It also made it easier to converse with the larger companies that could not give us the sort of time needed for a traditional interview.

We found that employees that did not work in cybersecurity preferred convenience over security when it came to authentication mechanisms. They preferred the one step password which was more vulnerable to breaches. They oftentimes felt that the second or third step was cumbersome and annoying to take every time they tried to log in. They understood the potential security benefits, but they felt that saving time was more important.

By contrast, we found that those who were more involved in cybersecurity generally wanted to keep the organization secure above all else. The IT staff at WPI, for example, gave us some valuable insight into what larger organizations use for cybersecurity management and how they adapt to different issues that arise. They determined that resetting passwords every 6 months, in a practice called “password rotation”, was a bad idea, as it encouraged people to use predictable changes (like incrementing a number or adding a repeated special character) when the time to reset passwords came. This was unexpected since infographics for keeping accounts safe and being vigilant about breaches stressed the notion of changing passwords frequently. Before the interview, we hypothesized this approach should work theoretically; however, the frequency at which the experts want it to be done made people prefer insecure password changes due to their simplicity, negating all security benefits.

WPI also must wrestle with both younger generations and older generations and how to balance that dynamic. The younger students were oftentimes more adaptable to changes and more open than faculty. One of the main issues facing WPI and their overall security is the fact that WPI is not over-performing in the world of security as it thinks it is. WPI does not have a Default Deny firewall, which even home routers do. Default Deny firewalls reject all network traffic which is not specifically allowed by their policy. At the firewall level, it involves defining permissible ports and protocols and turning everything else off [3]. The WPI IT staff have been trying to implement a firewall like this but have received some backlash from faculty. It is hard to be proactive in this certain context with the backlash from people they need to be onboard to make sure these policies are implemented properly. We hope that our paper can give them some advice on what to try next and how to implement more secure ways of authentication that will be well received by the population.

4.1: Summary

The current practice of deploying authentication mechanisms in businesses has gone through refinement. The institutional scale deployments find compromise between what users and employees want. The IT Staff at WPI is a microcosm of this phenomenon. Not every implementation of a measure will be successful or even liked. Institutions generally react to breaches as opposed to creating measures which are proactive against them. An employee might be discontented with stricter security measures being put into place, causing them to prefer insecure methods of practicing such measures, negating all potential security benefit. We hope to bring these trends to light of companies so they can adjust their authentication systems to implement mechanisms that are not only more secure, but more convenient for employees to use.

5. Deployed Authentication Mechanisms

In addition to interviewing companies, we compiled a comprehensive spreadsheet cataloging popular and frequently visited websites. This dataset provided insights into the array of authentication mechanisms employed across various online platforms accessible to the public. Our spreadsheet was a selection of 95 websites across 12 categories such as gaming and entertainment to finance and e-commerce. For each website, we documented their password policies and the types of authentication mechanisms used, including password-only systems, one-time passwords, biometric verification, and multi-factor authentication. This shed light on authentication practices but also enabled us to discern patterns and trends in the adoption of different authentication methods across different industries and sectors (see Appendix D). Furthermore, it served as a foundational resource for our analyses, providing an empirical basis for our decision-making processes and analytical frameworks.

To visualize this spreadsheet, we developed two decision trees delineating the spectrum of security implications associated with various authentication mechanisms employed by the surveyed websites. One decision tree counted the most secure authentication method that was offered by a website. Conversely, the other decision tree counted the least secure methods. The outline for these decision trees can be seen in Figure 2:

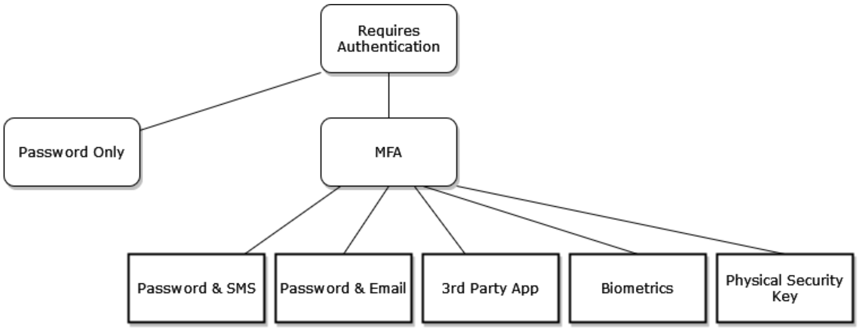


Figure 2: Decision tree showing the methods to log into the websites we classified in the spreadsheet.

Note that in the tree, the authentication mechanisms are increasingly secure from left to right in the leaves.

From our spreadsheet, we noticed some trends that go against peoples' perceptions on authentication. Categories corresponding to websites we know have sensitive data, such as financial websites and banking websites, did not have noticeably more or less secure authentication practices in general than other websites. Most of these websites did not enforce MFA, and those that did only allowed the user to choose between SMS and email, the two least secure mechanisms. Another trend we noticed is how small the minimum password length requirements were despite security research: 6 and 7 character long minimum passwords were surprisingly common. To compensate for this, companies introduced special character requirements to boost the keyspace size.

The decision trees revealed the popularity of certain authentication mechanisms as the most secure and least secure options. Notably, 91 of the 95 websites we could find information on made MFA completely optional and allowed users to not use it if they wish. Of the 5 websites that required MFA, all of them allowed SMS. This can be seen in Figures 3 and 4:

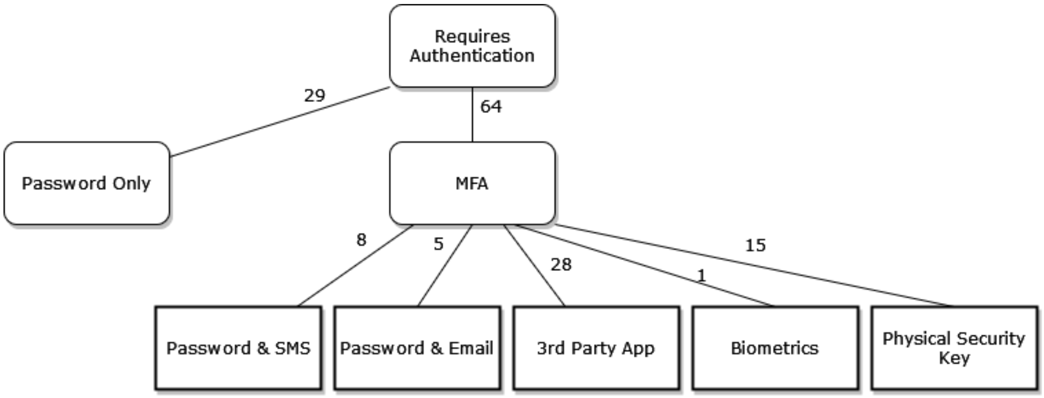


Figure 3: Decision Tree showing the most secure way to log into the websites that we classified in a spreadsheet.

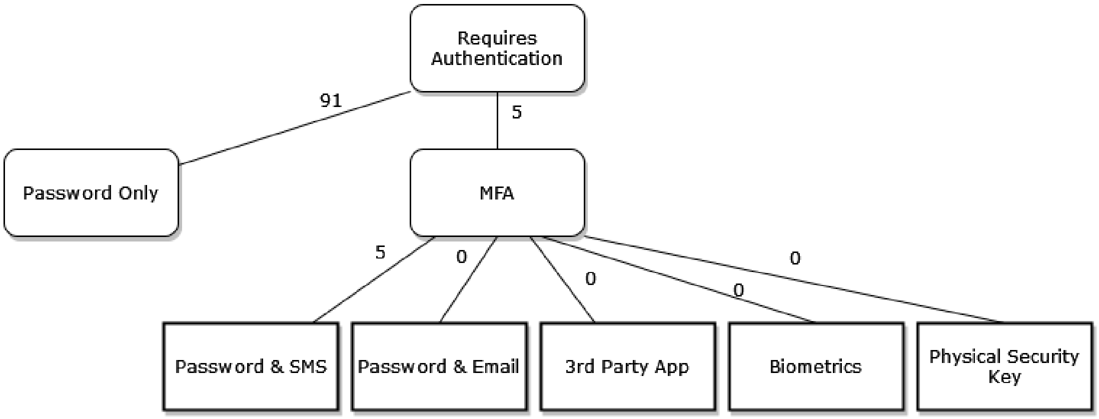


Figure 4: Decision tree showing the least secure way to log into the websites we classified in the spreadsheet.

Even in the decision tree counting the most secure authentication mechanisms offered, password-only authentication remained popular. However, SMS-based authentication declined, and a lot of websites allow 3rd party apps or physical security keys, which are deemed more secure options. Interestingly, biometric authentication is not commonly used as a multi-factor authentication method, but we did notice that it was much more common as a single-factor authentication mechanism in mobile devices. We also thought it was interesting how many websites supported a physical key log in and wondered how these were implemented since they were websites.

5.1: Summary

We examined 95 popular websites dispersed into 12 categories. The overwhelming majority of websites we examined allow password-only authentication; that is, only five of the websites we examined enforced MFA to be enabled on all accounts. However, most websites allowed users the option of MFA, with the most secure options commonly used being 3rd party authenticator apps and physical security keys. Biometric authentication is not commonly used for MFA, which was surprising. We also found that websites holding sensitive information, such as banking websites, do not necessarily have increased security over other websites. These results helped us evaluate our survey results and view the business interviews with a different perspective.

6. User Perspectives on Authentication Mechanisms

We also conducted surveys among users of the authentication mechanisms identified as the most common, aiming to assess the usability of these systems. We developed the survey questions to compare users' perspectives on password-only authentication and MFA. The questions were focused on thoughts on both security and usability of these authentication options (see Appendix E). Usability was deemed crucial in authentication mechanisms, as its absence could lead users to seek alternative, potentially insecure methods of authentication, thereby undermining the effectiveness of the system in practice compared to its theoretical efficacy. To analyze our data, we compared the perceived convenience and security of password-only authentication to MFA. We similarly compared different mechanisms used in MFA to determine how the public perceives specific mechanisms. We also collected demographic data to compare different age groups, genders, and technical experience levels with their responses and opinions about passwords and MFA. To quantify technical experience, we created four categories: "Expert," "Advanced," "Intermediate," and "Novice." We created descriptions to fit each of these categories and asked users to report which one fits them the best. To share our survey, we used social media platforms such as Facebook and Discord and word of mouth. Our target audience was the public.

The remainder of this chapter details our results for our survey. We introduce general results among all survey takers then we split our results by age, gender, and perceived technical ability and find trends within these groups.

6.1: General Results

We had a total of $n = 345$ responses to our survey. We split the data into categories by the demographic data. We subdivided the categories into demographic groups to capture people's responses by age, gender, or technical background. We discarded results for any group with less than 10 members to ensure a sufficient sample size for each group. Figures 5-7 detail the results to our demographic questions:

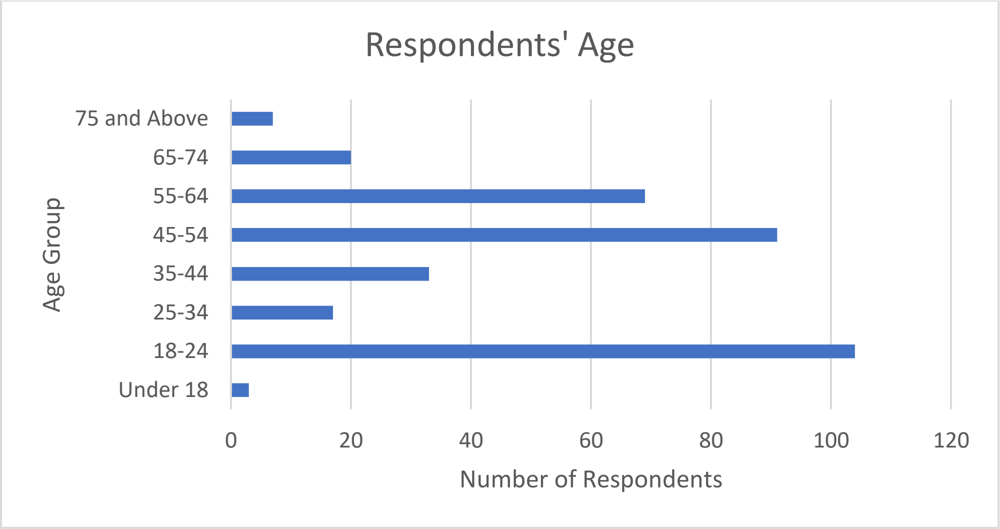


Figure 5: The breakdown of survey-takers by age.

As seen in Figure 5, most of our respondents were either between the ages of 18-24 or 45-54. This was likely due to sharing among colleagues and parents on social media. Since there were not enough survey respondents under the age of 18 (3 respondents) or 75 and above (6 respondents), we discarded those results in our analysis by age. Figure 6 details our results for our gender demographic question:

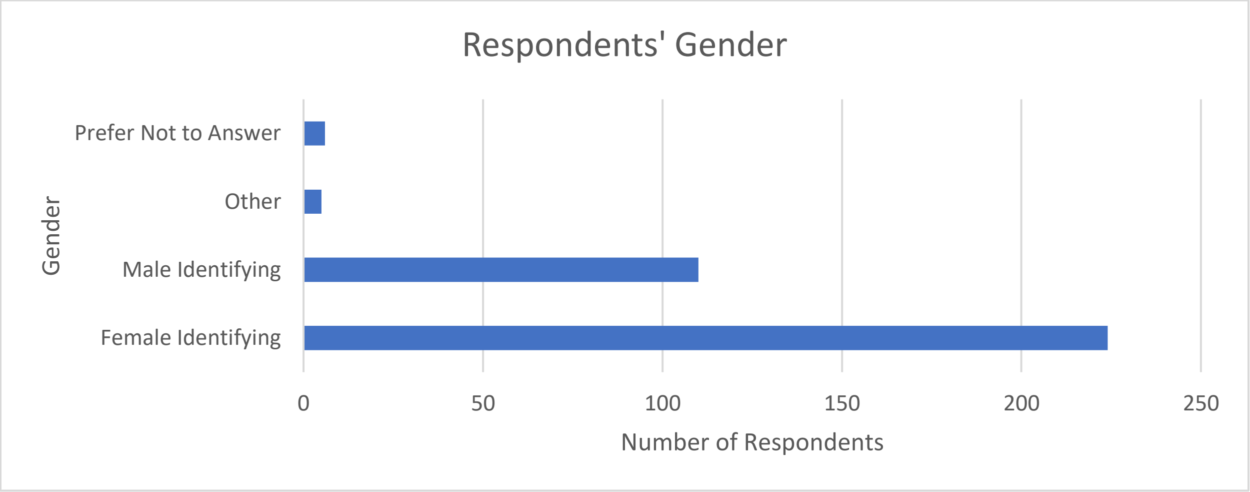


Figure 6: The breakdown of survey-takers by gender.

Most of our respondents were female identifying. Since there were not enough survey respondents who were not male or female identifying (5 reporting as "Other" and 6 reporting as "Prefer not to answer"), we discarded those results in our analysis by gender. Figure 7 details our results for our technical ability demographic question:

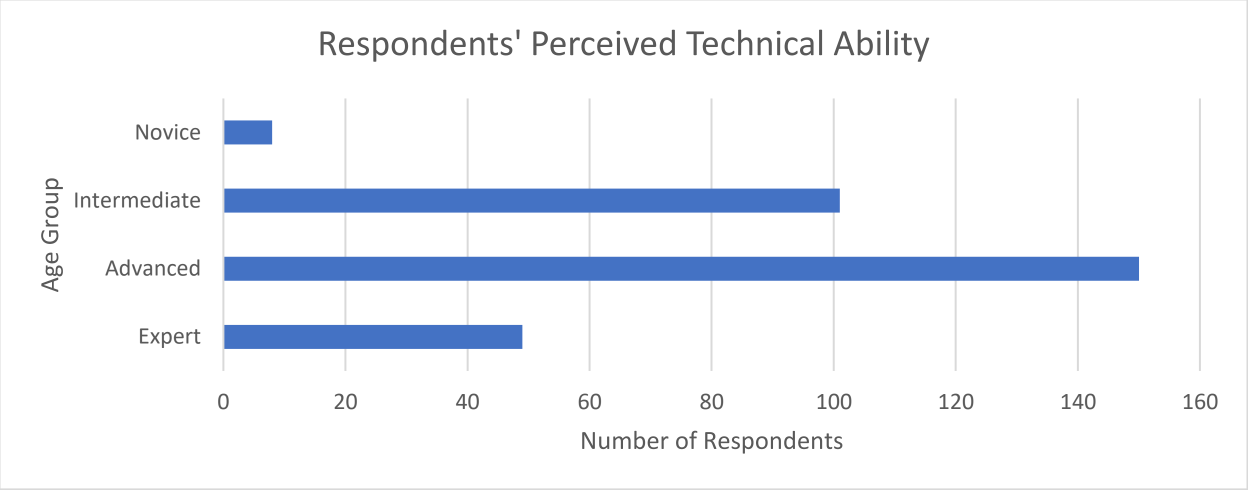


Figure 7: The breakdown of survey-takers by technical knowledge.

Most of our respondents self-reported as being in the “Advanced” category. Since there were not enough survey respondents who were in the “Novice” category (8 respondents), we discarded those results in our analysis by technical expertise.

6.1.1: Authentication Mechanisms: Convenience vs. Effectiveness

We next asked users their opinions on specific factors used for MFA. In particular, we asked them which factor they thought was the easiest/hardest to use and which one they thought was the least/most secure. We asked these questions to gauge how specific factors contribute to perception of MFA as a whole. The results to these questions are shown in Figures 8 and 9:

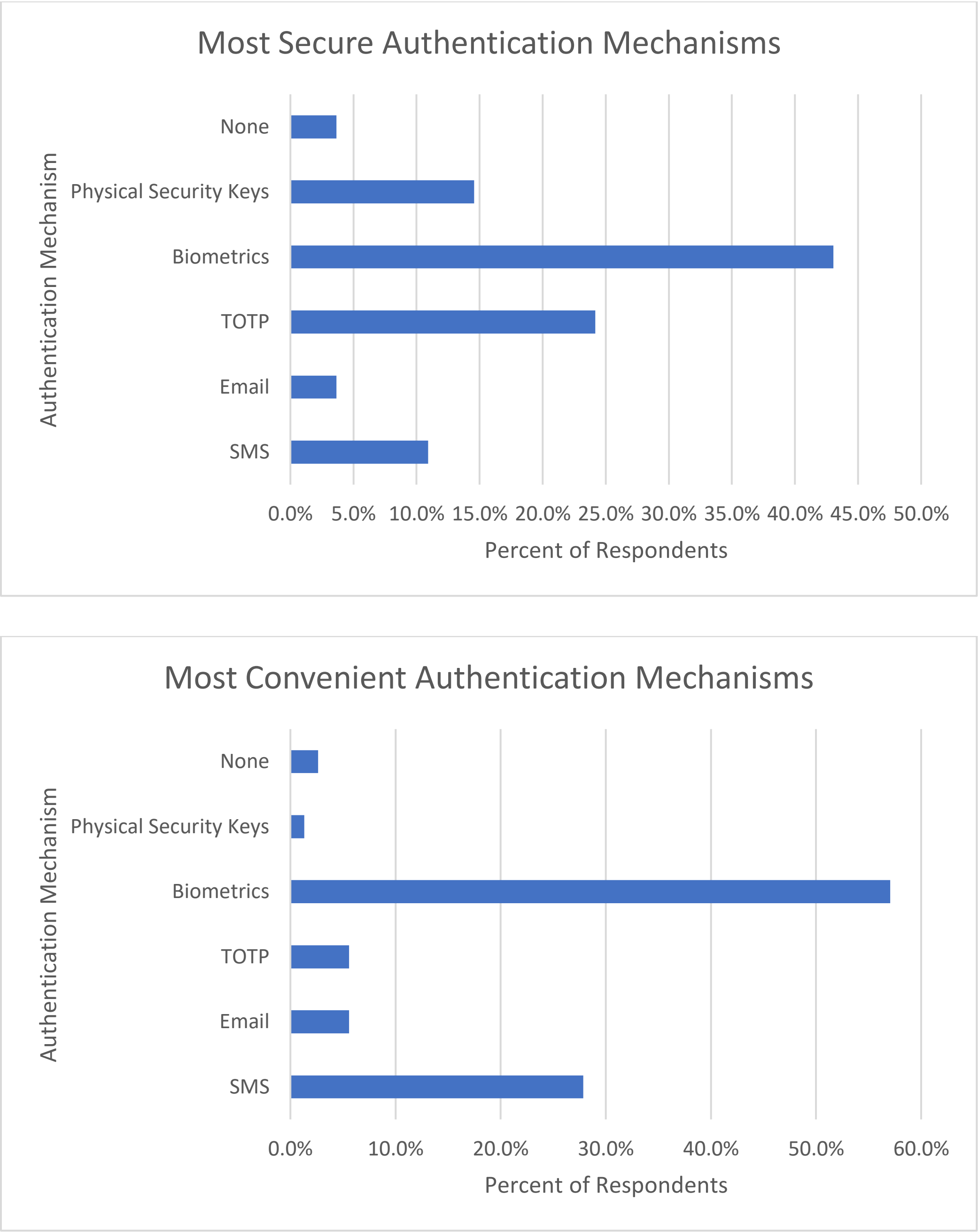


Figure 8: Bar graphs detailing perceived most secure and convenient authentication mechanisms.

We found that people generally viewed biometric authentication favorably. We hypothesize that this is because biometric authentication does not require users to type in any codes or plug anything into their laptop. One user mentioned that they would prefer biometrics because they do not need Wifi to work properly. However, some concerns that users had is with companies selling biometric data since it is incredibly hard to replace, as well as how it can require an external device to log in. Figure 9 details the least favorable authentication mechanisms for users:

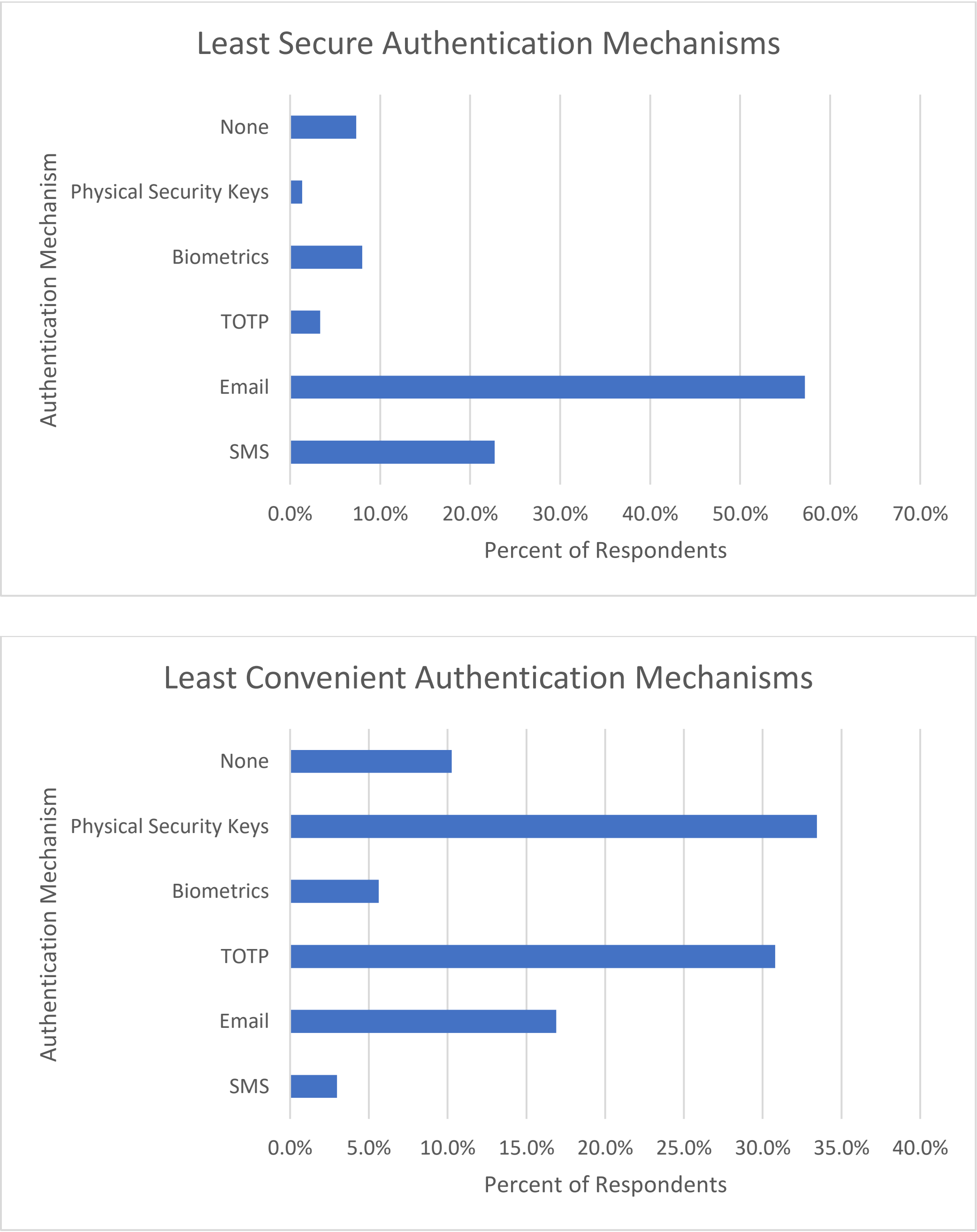


Figure 9: Bar graphs detailing perceived least secure and convenient authentication mechanisms.

We found that physical security keys were deemed the hardest to use. We hypothesize this is due to a lack of familiarity with this mechanism, as well as concerns about theft of the physical key. Similarly, we found TOTP was also inconvenient among users, likely due to their limited timeframe to enter a PIN. Lining up with our research, we also found email was perceived as the least secure mechanism, with SMS in 2nd place.

6.1.2: MFA vs. Password-only Authentication: Convenience vs. Effectiveness

We asked each participant, on a scale from 1-5 (1 is least effective, 5 is most effective), to rank how effective password-only authentication and MFA and repeated the ranking for convenience. Relative to password only authentication, users found MFA to be 34% more effective and 20% less convenient. Users tended to prefer convenience over security, especially for websites which do not contain "valuable information." One user put it like this: "it depends on what data is being accessed, and how easy the MFA is to access." Similarly, users tended to be more frustrated with mechanisms that are inconvenient, especially those that require an external device such as a cellphone. Common issues people cited were unreliability, forgetting an external device, giving major tech companies too much user data, and theft of an external device.

6.2: Results by Age

We found that older respondents did not find newer technologies such as physical security keys as convenient as younger respondents. Interestingly, biometrics were still popular among all age groups besides people between the ages of 25-34: these respondents ranked biometrics as less secure and less convenient than all other age groups. (See Appendix A).

We found no correlation between age and perceived security and convenience of password-only authentication vs. MFA as shown in Figure 10:

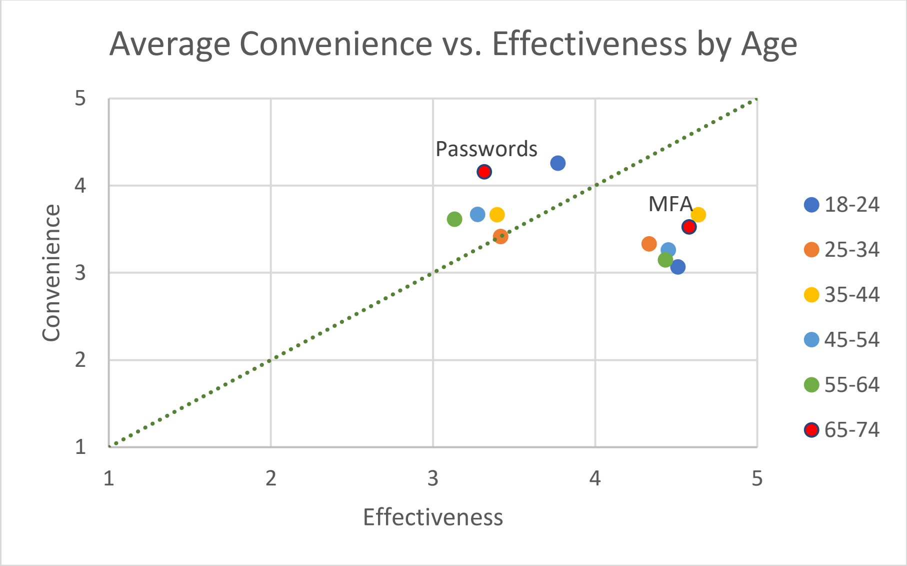


Figure 100: Graph detailing demographic groups' average effectiveness vs. convenience for Passwords and MFA.

We anticipated a correlation between younger people being able to adapt to newer technologies faster and thus ranking MFA as more convenient. However, we suspect authentication has been used to secure important information to all ages such as banking information, thus all have had to adapt to using the technology.

6.3: Results by Gender

We did not find much of a difference between the genders we studied. However, we did find that male identifying respondents found physical security keys more secure but less convenient than female identifying respondents (See Appendix B). We also found both gender groups we considered ranked authentication similarly, with female identifying respondents ranking passwords as slightly more effective and MFA as slightly more convenient than male identifying correspondents as seen in Figure 11:

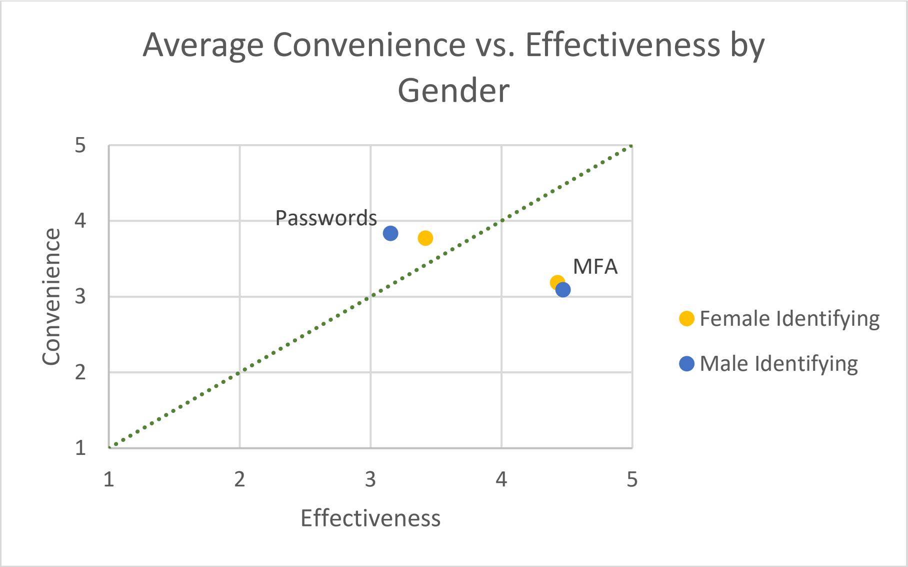


Figure 11: Graph detailing demographic groups' average effectiveness vs. convenience for Passwords and MFA.

We suspect that the differences between these groups to be insignificant, as people of all genders use authentication regardless. The differences are also smaller than those in the other two demographic groups.

6.4: Results by Technical Ability

While we did not find significant differences in perceived least secure authentication mechanisms, less perceived technical experience tended to correlate with perceiving biometrics as more secure (see Appendix C). We suspect that lack of familiarity with attacks against biometric data could be a potential cause of this. We also found that physical security keys were found to be far less convenient yet more secure by people in the "Advanced" category.

Increasing perceived technical ability also led to an increase in perceived security of MFA, and decrease in perceived security of passwords as seen in Figure 12:

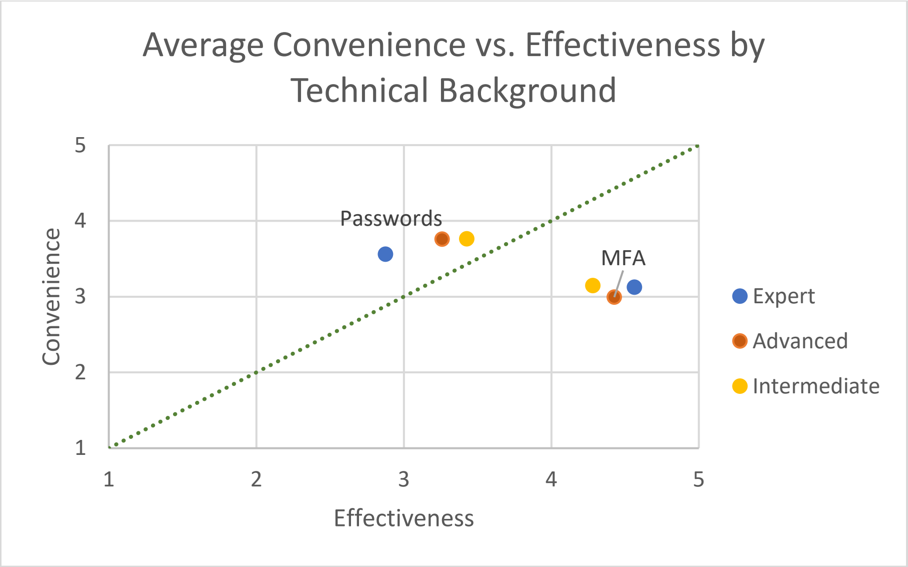


Figure 112: Graph detailing demographic groups' average effectiveness vs. convenience for Passwords and MFA.

We hypothesize that this could be a result of knowing more about the field, as people research authentication they find the shortcomings of password-only authentication as we did in our research. Conversely, we suspect that people who did not know as much about authentication would be more trusting towards password-only authentication and not rank MFA as highly due to a lack of knowledge as reflected in Figure 12.

6.5: Summary

Biometric authentication was a popular choice among users, ranking the highest in both security and usability. SMS and email were seen as the least secure authentication methods, yet SMS was seen as one of the most convenient authentication mechanisms and email being one of the least convenient. 3rd party authentication apps and physical security keys were seen as secure, but inconvenient, especially physical security keys.

Users overall found MFA to be 34% more secure and 20% less convenient than password-only authentication. They brought some concerns about MFA to light, especially methods that require external devices. They were concerned about losing an external device either by theft or misremembering.

There was no significant difference between perspectives among genders, however there was a significant difference among those with different ages and technical experience. Mainly, those between the ages of 25-34 did not perceive biometric authentication as secure or convenient as their fellow survey-takers. Interestingly, we found no correlation between age and perception of usability/security of authentication mechanisms. However, we found a positive correlation between perceived technical ability and perception of usability and security of MFA and a negative correlation between perceived technical ability and perception of usability and security of password-only authentication.

7. Discussion

Our research along with our three-pronged approach revealed the prominent preference of convenience over security in industry. Businesses tended to hold back on stronger factors of authentication due to insecure methods saving more time for employees who did not prioritize security such as those working in IT. However, this did not hold if the business had just been breached; in that case, people would deal with the lost time in fear of being breached again. This reactionary mindset reflected what we found with our surveys, as respondents were more willing to accept the inconvenience of MFA if the website held sensitive data out of fear of breaches. If users did not perceive the data going into the website as important, we found respondents preferred password-only authentication due to its convenience. We also found more experienced users were more accepting of MFA than those with less experience. Users perceived password-only authentication as more convenient than it was secure, and the opposite was mostly true of MFA. One common issue we found people had with MFA was requiring external devices to authenticate: people feared theft or loss of the device as well as its dependency on network connectivity.

We found an overwhelming number of the 95 websites we examined did not enforce MFA. Websites that required MFA allowed users to use SMS. This includes banking and financial websites, which consumers may assume enforce higher security even if that is not how it is in practice. Around ¾ of the websites allowed users the option of MFA, with most of them allowing 3rd party authentication apps or physical security keys. Again, banking/financial websites did not particularly have more secure authentication options than any other website.

7.1 Limitations

One main limitation of our project was the limited amount of information on authentication mechanisms for certain websites. Some websites had us enter sensitive information to create an account, mostly banking and financial websites. To minimize this limitation, we searched for banking websites we already had accounts for. Other websites did not allow us to make an account and/or did not make their policies on authentication clear. To minimize this limitation, we dropped these sites in our analysis since we could not properly analyze them. This is why the decision trees may not add exactly up to 95 websites.

Another limitation we discovered was a lack of responsiveness from businesses. Only a few businesses got back to us and answered the questions we provided, and their responses were minimal. To minimize this limitation, we focused our analysis on the WPI IT staff, who gave us the most valuable information out of the businesses we interviewed.

The last limitation that arose was the potential for skewed data in our survey. We had over 95 more respondents identify as female than male. We also had a large majority of people answer in the "Advanced" technical background category. To minimize this limitation, we only made conclusions from demographic groups with at least 10 people, and we normalized our results to base our conclusions on percentages of respondents. This way, the larger groups should have about an equal impact on our results as the smaller groups.

8. Conclusion

The fight to keep user accounts secure in the digital age with authentication mechanisms is constantly evolving. Through our examination of certain authentication mechanisms, ranging from traditional password-based authentication to MFA, our project has underscored the critical importance of striking a balance between security and usability.

Our findings highlight the evolving landscape of authentication technologies, driven by the imperatives of cybersecurity and user experience. Organizations are increasingly leveraging innovative solutions to enhance access control and safeguard sensitive information. Moreover, our survey of user perceptions and preferences has revealed the significance of usability in shaping authentication behaviors and attitudes. By prioritizing user-friendly authentication mechanisms such as biometric authentication, organizations can foster greater user acceptance and compliance, thereby mitigating the risks of circumvention and unauthorized access.

8.1: Future Work

While our research has shed light on various authentication practices and their implications, it is essential to acknowledge the ongoing challenges and complexities inherent in authentication security. As cyber threats continue to evolve and proliferate, there is a pressing need for continual innovation and adaptation in authentication technologies and practices. Moving forward, further research and collaboration among stakeholders are needed to address emerging threats, enhance authentication resilience, and promote user-centric authentication experiences. By fostering a holistic approach to authentication security, grounded in the principles of usability, effectiveness, and adaptability, we can collectively advance the security posture of digital ecosystems and safeguard the integrity of online interactions for all stakeholders.

Works Cited

[1] K. L. Chiew, K. S. C. Yong, and C. L. Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” *Expert Systems with Applications*, vol. 106, pp. 1–20, Sep. 2018, doi: 10.1016/j.eswa.2018.03.050.

[2] S. Das, B. Wang, A. Kim, and L. J. Camp, *MFA is A Necessary Chore!: Exploring User Mental Models of Multi-Factor Authentication Technologies*. 2020. Available: http://hdl.handle.net/10125/64411

[3] Information Services, University of Regina, “Default Deny Campus Firewall.” [Online]. Available: https://www.uregina.ca/is/security/resources/resource-firewall.html#:~:text=Default-deny%20means%20that%20network,and%20turning%20everything%20else%20off

[4] S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes, and S. Bugiel, “Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication,” in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 268–285. doi: 10.1109/SP40000.2020.00047.

[5] K. Lee, S. Sjöberg, and A. Narayanan, “Password policies of most top websites fail to follow best practices,” *USENIX*, Aug. 2022, [Online]. Available: https://www.usenix.org/system/files/soups2022-lee.pdf

[6] K. Marky *et al.*, “‘Nah, it’s just annoying!’ A Deep Dive into User Perceptions of Two-Factor Authentication,” *ACM Trans. Comput.-Hum. Interact.*, vol. 29, no. 5, p. 43:1-43:32, Oct. 2022, doi: 10.1145/3503514.

[7] S. Mujeye, “A Survey on Multi-Factor Authentication Methods for Mobile Devices,” in *Proceedings of the 2021 4th International Conference on Software Engineering and Information Management*, in ICSIM ’21. New York, NY, USA: Association for Computing Machinery, Jul. 2021, pp. 199–205. doi: 10.1145/3451471.3451503.

[8] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," in *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021-2040, Dec. 2003, doi: 10.1109/JPROC.2003.819511

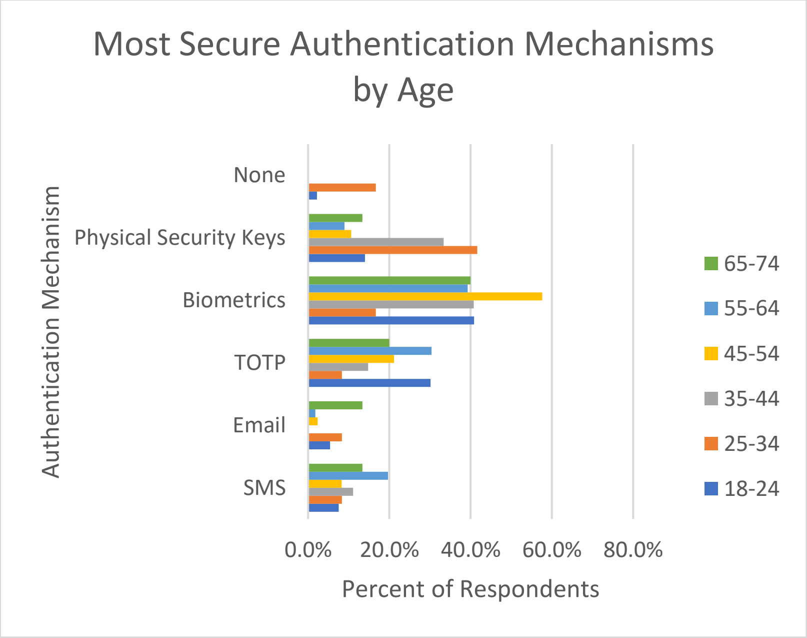
[9] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, “Why people (don’t) use password managers effectively,” *USENIX*, Aug. 2019, [Online]. Available: https://www.usenix.org/system/files/soups2019-pearman.pdf

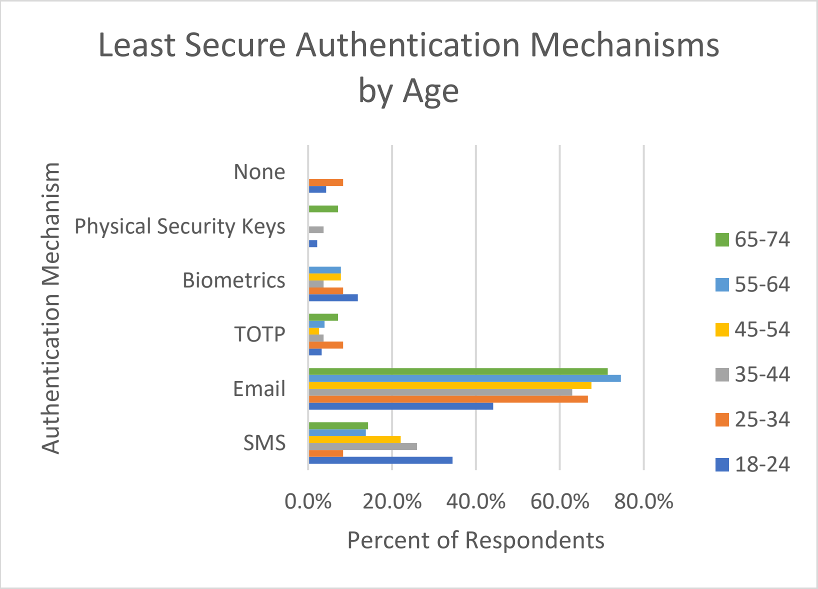
[10] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A Usability Study of Five Two-Factor Authentication Methods,” *USENIX*, Aug. 2019, [Online]. Available: https://www.usenix.org/system/files/soups2019-reese.pdf

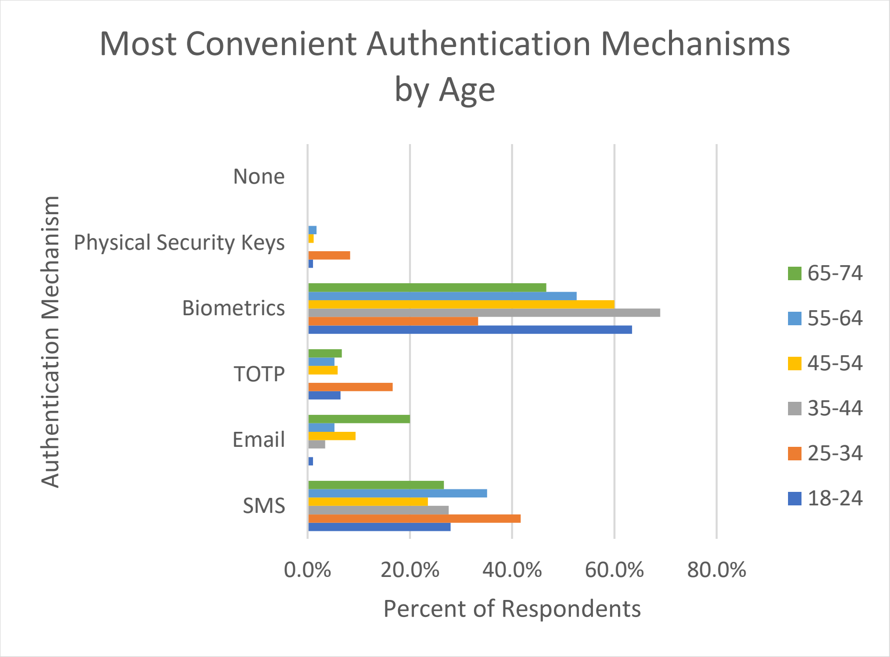
[11] M. Stanislav, *Two-Factor Authentication*. Ely, UNITED KINGDOM: IT Governance Ltd, 2015. Accessed: Sep. 11, 2023. [Online]. Available: http://ebookcentral.proquest.com/lib/wpi/detail.action?docID=2048577

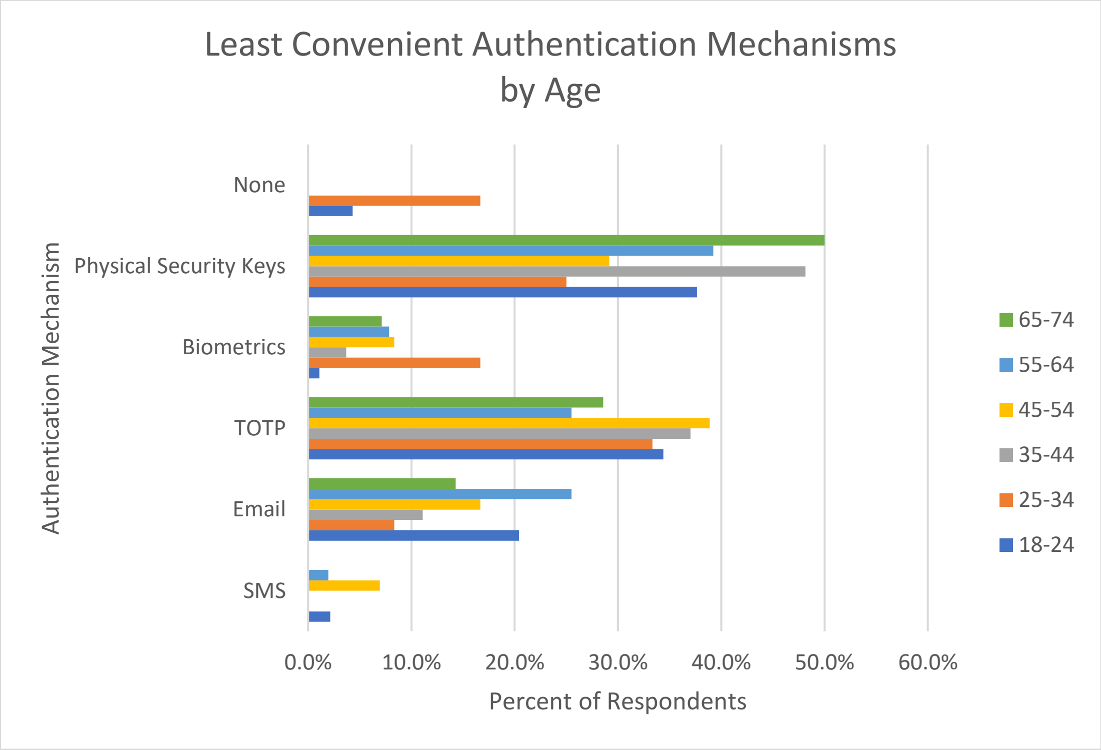
Appendix A: Breaking Down Authentication Mechanisms by Age

Here are four graphs detailing the specific authentication mechanisms we prompted survey users on. We asked users which factor they thought was the most secure, least secure, most convenient, and least convenient. Below are results for each of these questions by age:



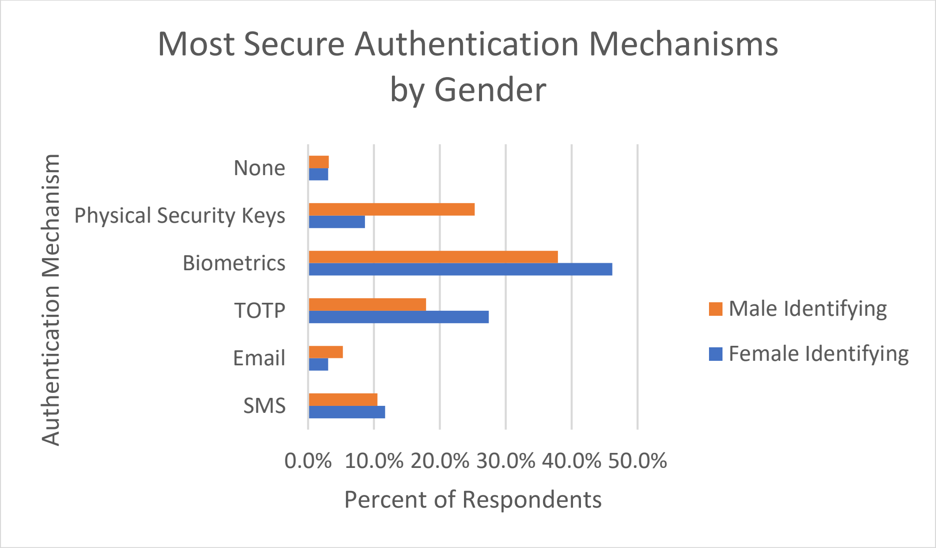


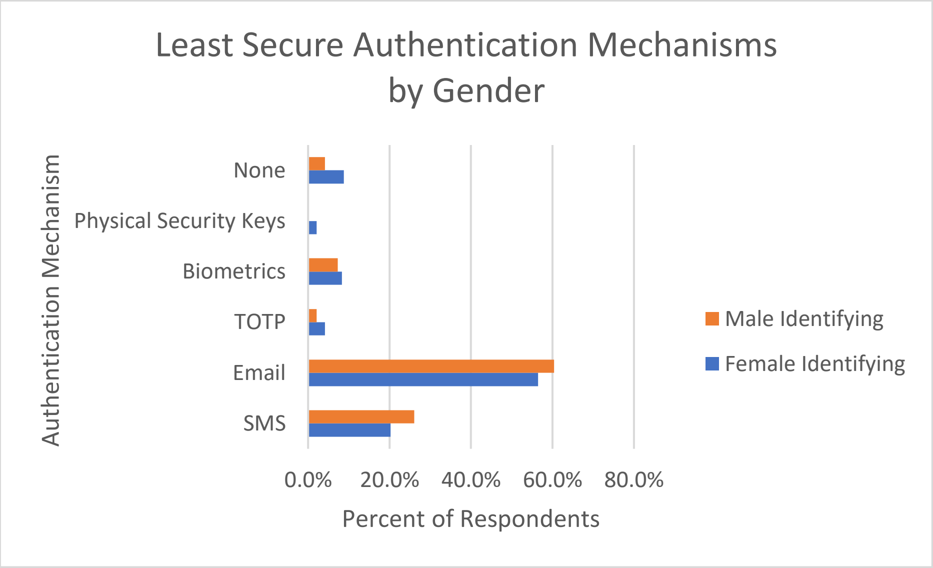

Most Convenient Authentication Mechanisms by Age
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
20.0%
40.0%
60.0%
80.0%
Percent of Respondents
65-74
55-64
45-54
35-44
25-34
18-24

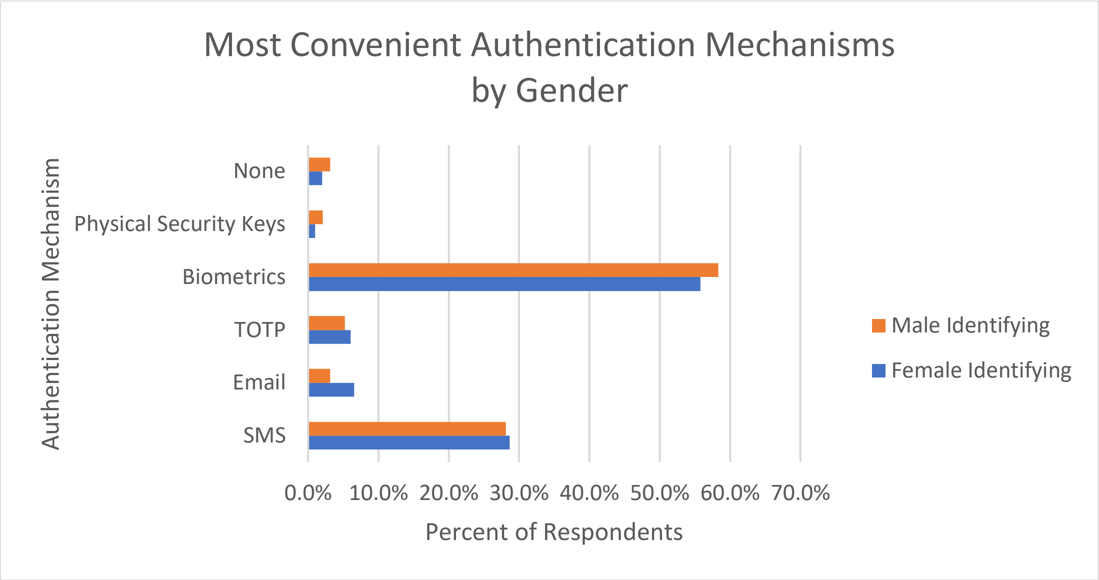

Least Convenient Authentication Mechanisms by Age
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
Percent of Respondents
65-74
55-64
45-54
35-44
25-34
18-24

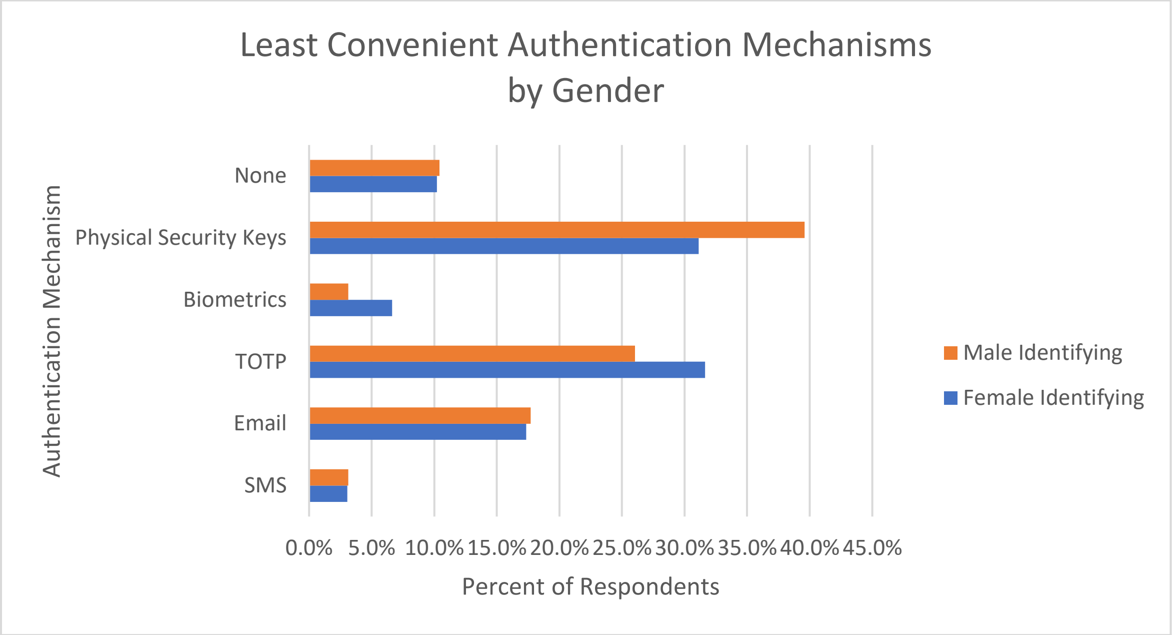
Appendix B: Breaking Down Authentication Mechanisms by Gender

Here are four graphs detailing the specific authentication mechanisms we prompted survey users on. We asked users which factor they thought was the most secure, least secure, most convenient, and least convenient. Below are results for each of these questions by gender:



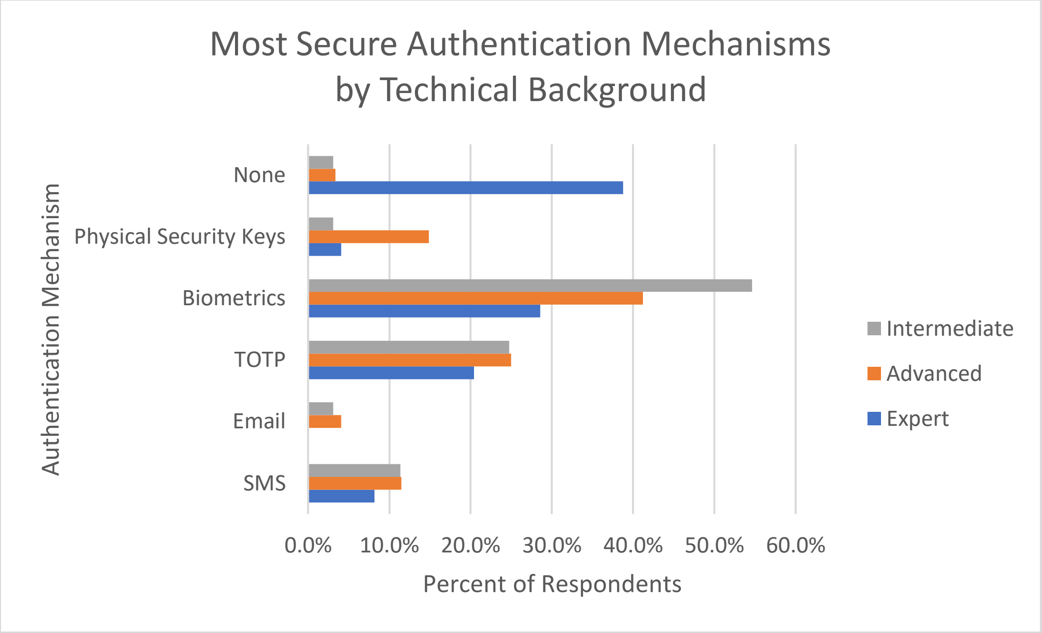


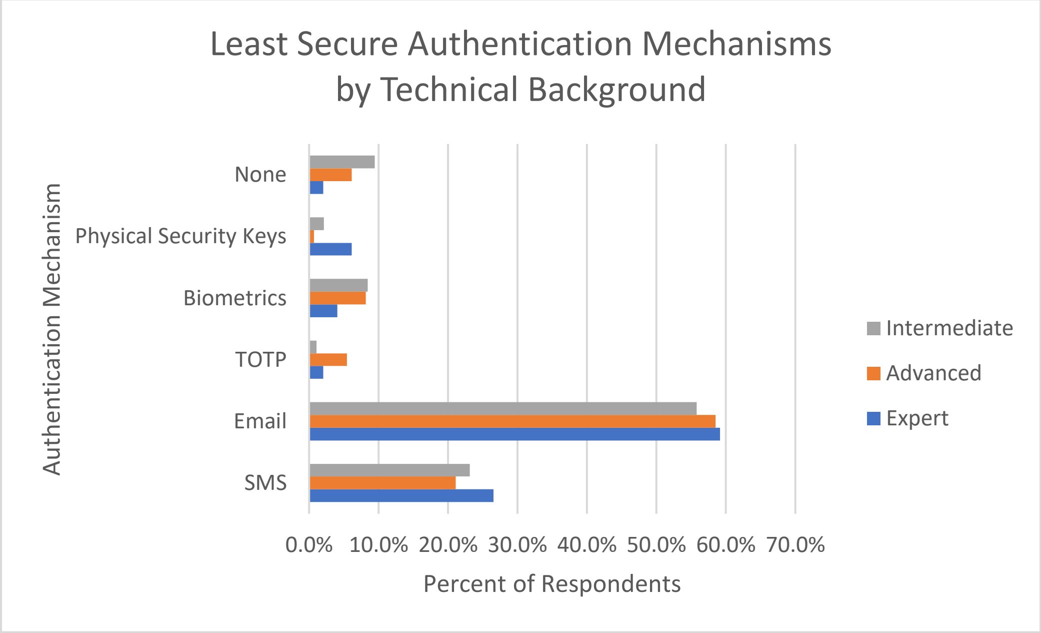

Most Convenient Authentication Mechanisms by Gender
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
Percent of Respondents
🟧 Male Identifying
🟦 Female Identifying

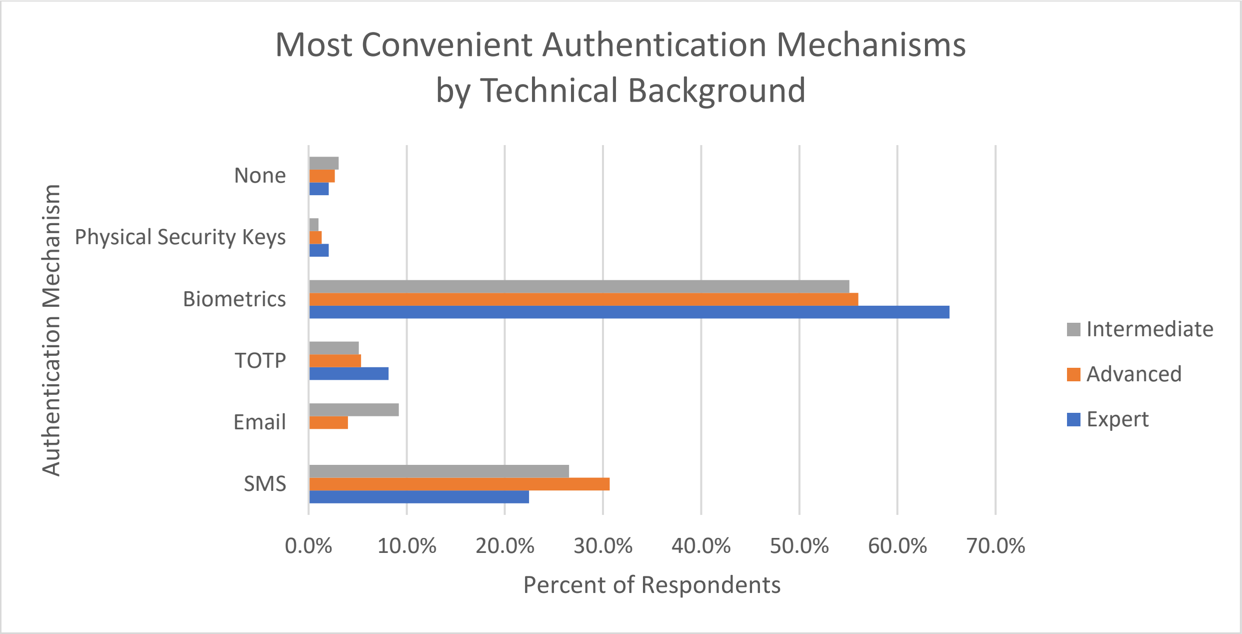

Least Convenient Authentication Mechanisms by Gender
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
5.0%
10.0%
15.0%
20.0%
25.0%
30.0%
35.0%
40.0%
45.0%
Percent of Respondents
🟧 Male Identifying
🟦 Female Identifying

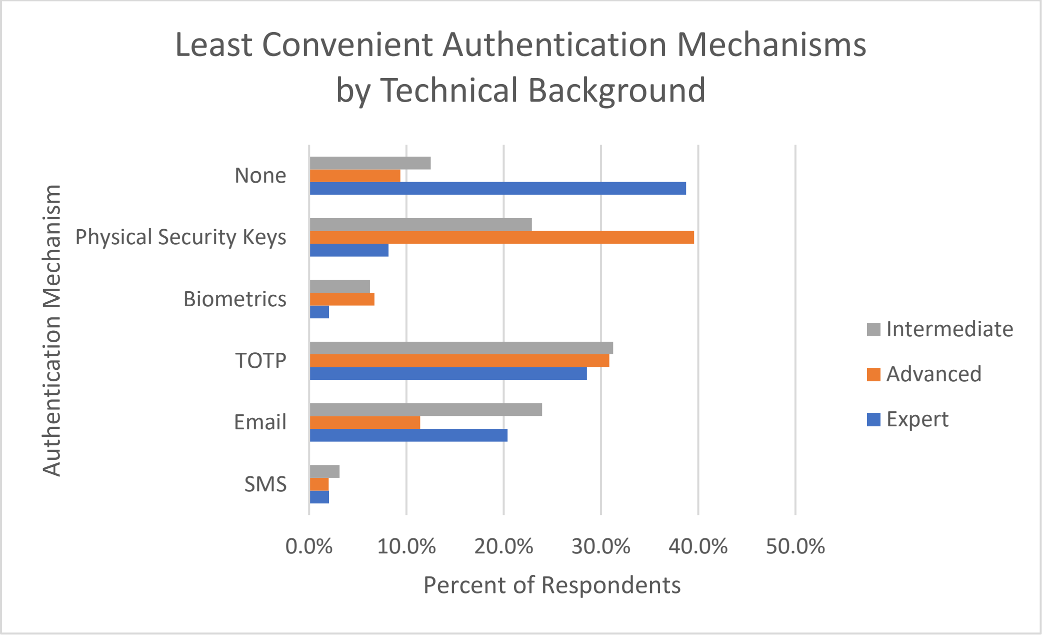
Appendix C: Breaking Down Authentication Mechanisms by Technical Background

Here are four graphs detailing the specific authentication mechanisms we prompted survey users on. We asked users which factor they thought was the most secure, least secure, most convenient, and least convenient. Below are results for each of these questions by technical background:






Most Convenient Authentication Mechanisms
by Technical Background
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
Percent of Respondents
Intermediate
Advanced
Expert


Least Convenient Authentication Mechanisms
by Technical Background
Authentication Mechanism
None
Physical Security Keys
Biometrics
TOTP
Email
SMS
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
Percent of Respondents
Intermediate
Advanced
Expert

Appendix D: Websites Used for Analysis

This appendix is to list the websites referenced in the Deployed Mechanisms chapter.

The 12 categories of the websites are:

1. Antivirus Vendor
2. Banking / Credit Cards
3. Developer Platforms
4. Email
5. Finances/Financial Planning
6. Game Shops/DRM
7. General Shopping
8. Music Streaming
9. Social Media
10. TV / Movie Streaming
11. Video Streaming
12. Miscellaneous

List of Websites examined:

Category	Website	URL	Num
Antivirus Vendor	Avast / AVG	www.avast.com	1
Antivirus Vendor	Avira	https://www.avira.com/	2
Antivirus Vendor	BitDefender	https://www.bitdefender.com/	3
Antivirus Vendor	ESET	https://www.eset.com/us/	4
Antivirus Vendor	Kaspersky	https://usa.kaspersky.com/antivirus	5
Antivirus Vendor	Malwarebytes	https://www.malwarebytes.com/	6
Antivirus Vendor	McAfee	https://www.mcafee.com/	7

Antivirus Vendor	Norton	https://us.norton.com/	8
Antivirus Vendor	Protegent	https://protegent360.com/	9
Banking	Bank of America	https://www.bankofamerica.com/	10
Banking	Charles Schwab	https://www.schwab.com/	11
Banking	Chase	https://www.chase.com/	12
Banking	Citibank	https://www.citi.com/	13
Banking	Discover	https://www.discover.com/	14
Banking	Santander	https://www.santanderbank.com/	15
Developer Platform	Amazon AWS	https://aws.amazon.com/	16
Developer Platform	Canva	https://www.canva.com/	17
Developer Platform	Geeks For Geeks	https://www.geeksforgeeks.org/	18
Developer Platform	Github	https://github.com/	19
Developer Platform	Khan Academy	https://www.khanacademy.org/	20
Developer Platform	LeetCode	https://leetcode.com/	21
Developer Platform	Stack Overflow	https://stackoverflow.com/	22
Developer Platform	Trello	https://trello.com/	23
Developer Software	W3Schools	https://www.w3schools.com/	24
Developer Platform	Wordpress	https://wordpress.com/	25

Email	AOL Mail	https://help.aol.com/products/aol-mail	26
Email	Evite	https://www.evite.com/	27
Email	Gmail	https://mail.google.com	28
Email	Mail.com	https://www.mail.com/	29
Email	Mailchimp	https://mailchimp.com/	30
Email	Proton Mail	https://proton.me/mail	31
Email	Outlook (Microsoft)	https://outlook.office.com/mail/	32
Email	Yahoo Mail	https://www.yahoo.com/	33
Finances	Credit Karma	https://www.creditkarma.com/	34
Finances	Experian	https://www.experian.com/	35
Finances	PayPal	https://www.paypal.com/	36
Finances	Robinhood	https://robinhood.com/us/en/	37
Finances	Venmo	https://venmo.com/account/sign-in	38
Game Shop/DRM	Activision/Blizzard	https://www.blizzard.com/en-us/games	39
Game Shop/DRM	Chess.com	chess.com	40
Game Shop/DRM	Cool Math Games	https://www.coolmathgames.com/	41
Game Shop/DRM	EA Origin	https://www.ea.com/ea-app	42
Game Shop/DRM	Epic Games	https://store.epicgames.com/en-US/	43
Game Shop/DRM	GOG	https://www.gog.com/	44
Game Shop/DRM	itch.io	https://itch.io/	45
Game Shop/DRM	Nintendo	https://www.nintendo.com/us//	46

Game Shop/DRM	Roblox	https://www.roblox.com/	47
Game Shop/DRM	Sony	https://www.sony.com/en/	48
Game Shop/DRM	Steam	https://store.steampowered.com/	49
General Shopping	Amazon	https://www.amazon.com/	50
General Shopping	BJ’s Wholesale Club	https://www.bjs.com/	51
General Shopping	Costco	https://www.costco.com/	52
General Shopping	eBay	https://www.ebay.com/	53
General Shopping	Etsy	https://www.etsy.com/	54
General Shopping	Rakuten	https://www.rakuten.com	55
General Shopping	Samsung	samsung.com	56
General Shopping	Target	https://www.target.com/	57
General Shopping	Walmart	www.walmart.com/	58
General Shopping	Wayfair	https://www.wayfair.com/	59
Music Streaming	Apple Music	https://music.apple.com/us/browse	60
Music Streaming	iHeart	https://www.iheart.com/	61

Music Streaming	Last.fm	https://www.last.fm/	62
Music Streaming	Online Radio Box	https://onlineradiobox.com/us/	63
Music Streaming	Pandora	https://www.pandora.com/	64
Music Streaming	Qobuz	https://www.qobuz.com/us-en/discover	65
Music Streaming	Sirius XM	https://www.siriusxm.com/	66
Music Streaming	Soundcloud	https://soundcloud.com/	67
Music Streaming	Spotify	https://open.spotify.com/	68
Music Streaming	TIDAL	https://tidal.com/	69
Social Media	Discord	https://discord.com/	70
Social Media	Facebook	https://www.facebook.com/	71
Social Media	Instagram	https://www.instagram.com/	72
Social Media	Linkedin	https://www.linkedin.com/	73
Social Media	Myspace	https://myspace.com/	74
Social Media	Reddit	https://www.reddit.com/	75
Social Media	Snapchat	https://www.snapchat.com/	76
Social Media	X (Formerly Twitter)	https://twitter.com/	77
TV/Movie Streaming	Amazon Prime Video	https://www.amazon.com/ref=nav_logo	78
TV/Movie Streaming	CrunchyRoll	https://www.crunchyroll.com/	79

TV/Movie Streaming	Disney+	https://www.disneyplus.com/	80
TV/Movie Streaming	Hulu	https://www.hulu.com/welcome	81
TV/Movie Streaming	Netflix	https://www.netflix.com/browse	82
Video Sharing Platform	Kick	https://kick.com/	83
Video Sharing Platform	TikTok	https://www.tiktok.com/explore	84
Video Sharing Platform	Twitch	https://www.twitch.tv	85
Video Sharing Platform	Vimeo	https://vimeo.com/	86
Video Sharing Platform	YouTube	https://www.youtube.com	87
Miscellaneous	Cloudflare	https://www.cloudflare.com/	88
Miscellaneous	Indeed	https://www.indeed.com/	89
Miscellaneous	Instructure (Canvas)	https://www.instructure.com/canvas	90
Miscellaneous	MEGA	https://mega.io/	91
Miscellaneous	Open AI	https://chat.openai.com/auth/login	92
Miscellaneous	WhatsApp	whatsapp.com	93
Miscellaneous	Wikipedia	wikipedia.org	94

Miscellaneous	Workday	https://www.workday.com/	95

Password/MFA Requirement Data Companion:

Charles Anderson, Ian Grzembski, Daniel Onyema, Caitlyn Puiia, Password/MFA Requirement Companion to the table:

Preface:

True = Yes

False = No

Black Cell Column: Pertains to Metadata

Gray Cell Column: Pertains to Passwords

Brown Cell Column: Pertains to Multi Factor Authentication

Blue Cell Column: Special Notes

Metadata Fields:

- Website Name
- Similarweb Classification
- URL

Password Fields (Password Guidelines Quantified):

- Minimum Length (Integer)
- Maximum Length (Integer)
- Numbers Required? (Boolean)
- Special Characters Required (Boolean)
- Prevents easily guessable / leaked passwords / specific phrases (Boolean)

- Contains a “Strength Meter” (Boolean)
- Password Rotation/Expiration (Boolean)

Authentication Buckets (Boolean True/False Toggles):

- SMS One Time PW
- SMS Authentication
- (Verification Thru) Phone Call
- Email One Time PW
- Authenticator App
- FIDO
- No MFA
- MFA Required to access account
- Biometrics (Mobile Device Only, like face recognition)

Special Buckets:

- One-Time MFA/Recovery MFA (use it to set up account or for account recovery)

Bizarre Traits:

- This is a special category for noted behaviors of the site, verification system or account. This should really be more like a qualitative description of such a thing.
- This can include the back-end logic for managing passwords not being the same as the recommended requirements.

Appendix E: Survey Sent to the Public

This appendix includes the full survey we sent out to the public.

Preamble: We are working on a research project to evaluate commonly used authentication mechanisms (passwords, two-factor authentication (2FA), multi-factor authentication (MFA), etc.) that are used to secure online accounts.

This survey aims to determine how the user experience relates to the security of these mechanisms. This survey should take around two minutes. Your participation is voluntary, and you may end your participation at any time. All questions are optional, so if you do not feel comfortable answering a question, you do not have to answer it.

This survey is anonymous, but you are limited to taking it only once. This survey is confidential and identifying responses will not be disclosed. By taking the survey, you will be able to see how your responses compare with other respondents at the end of the survey. Optionally, a copy of the resulting project report will be sent out if an email is given at the end of the survey.

1. What age group do you fall under?
    1. Under 18
    2. 18-24
    3. 25-34
    4. 35-44
    5. 45-54
    6. 55-64
    7. 65-74
    8. 75+

2. What is your gender?
    1. Female Identifying
    2. Male Identifying
    3. Other
    4. Prefer not to answer

3. How would you describe your technical background?
    1. Expert: I can provide guidance, troubleshoot, and answer questions about technology. I am well-known as a person who can answer questions about using computers and the internet.
    2. Advanced: I can use computers and other forms of technology without assistance and can usually answer questions from others.
    3. Intermediate: I can usually use computers and the internet with minimal help.
    4. Novice: I have limited experience with computers and the Internet and generally rely on help.

4. Are passwords by themselves an effective means for authentication?

5: Very effective 4: Effective 3: Neither 2: Not Effective 1: Not effective at all

5. Are passwords by themselves a convenient means for authentication?

5: Very effective 4: Effective 3: Neither 2: Not Effective 1: Not effective at all

6. Have you used Two-factor authentication (2FA) or Multi-factor authentication (MFA) before (for example, messages on your phone asking you to verify yourself, authenticator apps, email verification)?

Yes No

7. Which factors are you familiar with? (multi-select)

1. SMS
2. Email
3. Time-based One-Time Passwords (TOTP)
4. Biometrics like FaceID or TouchID
5. Physical Security keys like Yubikey
6. None

8. Out of the listed factors you know about, which is the most secure in your opinion? (Pick one)

1. SMS
2. Email
3. Time-based One-Time Passwords (TOTP)
4. Biometrics like FaceID or TouchID
5. Physical Security keys like Yubikey
6. None

9. Out of the listed factors you know about, which is the least secure in your opinion? (Pick one)

1. SMS
2. Email
3. Time-based One-Time Passwords (TOTP)
4. Biometrics like FaceID or TouchID
5. Physical Security keys like Yubikey
6. None

10. Which of the listed factors is the easiest to use in your opinion? (Pick one)

1. SMS

2. Email
3. Time-based One-Time Passwords (TOTP)
4. Biometrics like FaceID or TouchID
5. Physical Security keys like Yubikey
6. None

11. Which of the listed factors is the hardest to use in your opinion? (Pick one)
    a. SMS
    b. Email
    c. Time-based One-Time Passwords (TOTP)
    d. Biometrics like FaceID or TouchID
    e. Physical Security keys like Yubikey
    f. None

12. Is 2FA/MFA an effective means for authentication?

5: Very effective   4: Effective   3: Neither   2: Not Effective   1: Not effective at all

13. Is 2FA/MFA a convenient means for authentication?

5: Very effective   4: Effective   3: Neither   2: Not Effective   1: Not effective at all

14. Any other thoughts on 2FA, MFA, and/or any of the aforementioned factors?

15. If you would like to view our project report once this project is finished, please put your email here. (OPTIONAL)

At the end of the survey the respondent should be directed to a page showing a summary of the results thus far. This is possible to do in Qualtrics and lets them see how others responded.