



Undergraduate Honors Theses

2021-06-18

Who Uses Multi-Factor Authentication?

Leah Roberts

Follow this and additional works at: https://scholarsarchive.byu.edu/studentpub_uht

BYU ScholarsArchive Citation

Roberts, Leah, "Who Uses Multi-Factor Authentication?" (2021). *Undergraduate Honors Theses*. 202.
https://scholarsarchive.byu.edu/studentpub_uht/202

This Honors Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in Undergraduate Honors Theses by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.

HONORS THESIS

WHO USES MULTI-FACTOR AUTHENTICATION?

By

Leah Roberts

Submitted to Brigham Young University in partial fulfillment of graduation requirements
for University Honors

Computer Science Department

Brigham Young University

June 2021

Advisor: Casey Deccio

Honors Coordinator: Seth Holladay

ABSTRACT

WHO USES MULTI-FACTOR AUTHENTICATION?

Leah Roberts
Computer Science Department
Bachelor of Science

A sample of 47 BYU students were recruited to participate in this study to determine who was using Multi-factor Authentication (MFA) on their online accounts. This study determined that there were many different factors that separated those who used MFA and those who did not. Some of those factors included: time spent on the internet each day, gender, the website itself, and personal privacy behaviors.

ACKNOWLEDGEMENTS

I would like to thank Dr. Casey Deccio, Dr. Xinru Page, Dr. Daniel Zappala, and Dr. Seth Holladay for being compassionate and patient educators and advisors.

TABLE OF CONTENTS

Abstract..... i
Acknowledgements..... iii
Table of Contents..... v
List of Figures..... viii
List of Tables..... ix

1 Introduction..... 1
2 Current Research..... 1
 2.1 Studies on Measuring User Attitudes 2
 2.1.1 Measuring user attitudes in a laboratory study 2
 2.1.2 Measuring user attitudes through surveys and questionnaires..... 3
 2.2 Studies on MFA Adoption..... 3
 2.2.1 Too busy to use MFA 3
 2.2.2 The perceived learning curve..... 4
 2.2.4 Limitations of the studies..... 4
3 Study of Who Uses Multi-Factor Authentication 4
 3.1 Data Collection Method..... 5
 3.2 Ethical Considerations 5
 3.3 Mechanics of the Study..... 6
4 Results..... 6
 4.1 Sample..... 6
 4.2 Sample & Population 7
 4.3 Differences Between MFA Students and Non-MFA Students 8
 4.3.1 Technical vs. Non-Technical MFA Use 8
 4.3.2 Internet Usage on MFA Use 9
 4.3.3 Gender and MFA Use 12
 4.4 Website Providers’ MFA Feature 13
 4.5 Privacy Behavior and MFA Use..... 15
 4.5.1 Relationship between MFA use and good password practices 15
5 Discussion of Results..... 17
 5.1 Differences Between MFA Students and Non-MFA Students..... 17

5.2 Websites' MFA.....	18
5.3 Students' Privacy Behavior.....	18
5.4 Limitations	18
6 Conclusion	19
Appendix A: Survey Questions	21

LIST OF FIGURES

FIGURE 1: Sample Population Bar Chart.....	7
FIGURE 2: MFA by Colleges Stacked Bar Chart.....	8
FIGURE 3: Internet Usage Line Chart.....	9
FIGURE 4: Internet Usage Bar Chart.....	10
FIGURE 5: MFA by Gender Pie Chart.....	12
FIGURE 6: Proportion of Websites' MFA Accounts.....	14
FIGURE 7: Password Practices of All Students Bar Chart.....	16
FIGURE 8: Password Practices of Non-MFA Students Bar Chart.....	17

LIST OF TABLES

TABLE 1: T-Test Values.....	10
TABLE 2: T-Test Data Sets.....	11
TABLE 3: Chi-Square Test Data.....	13
TABLE 4: Websites' Total Accounts & MFA Accounts.....	13
TABLE 5: Password Creation Questions.....	16

1 Introduction

Popular online systems, such as Facebook, Google, and others offer multi-factor authentication to their users, but it is unknown how many people choose to use these services. In their attempts to make accounts more secure to protect the privacy of their users, online sites are possibly being thwarted in their efforts by the users themselves. Multi-factor authentication solutions (MFA) use a combination of authentication schemes to increase the security of private accounts. A common example is using a password and verification by something a user owns (like their smartphone device).

Despite the development of alternative/additional authentication methods, authentication solely via password is ubiquitous in internet applications, and has been found to be the preferred method by users [1]. However, there are many drawbacks to password protection. Many users who have difficulty memorizing complicated, stronger passwords simply create passwords that are easy to remember and, unfortunately, easy to guess [2]. Even if users create strong passwords, they may be using the same password on other systems [3].

This research attempts to determine whether people are using optional multi-factor authentication methods on their online accounts with Google, Facebook, etc. Determining the degree to which users are integrating multi-factor authentication in their online lives is an important finding, because it could help developers make the necessary changes to their multi-authentication protocols so that they appeal to the user.

2 Current Research

Previous studies have shown that there are better solutions than basic password protection and have recommended MFA as a lower security risk alternative [3], [4],

therefore the literature that discusses the security advantages of MFA will not be considered in reviewing the body of literature that surrounds the topic of MFA. The current research that will be looked at focuses on two main issues: user attitudes towards MFA, and MFA adoption. Much of the research has been focused on Two-factor Authentication. Two-factor authentication specifically refers to MFA that only uses two forms of authentication (e.g., password and biometric). Since Two-factor Authentication falls under the umbrella of MFA, those studies will also be considered as part of the body of literature that surrounds this topic, and we will refer to Two-Factor Authentication as 2FA.

2.1 Studies on Measuring User Attitudes

In the past ten years, there have been several studies seeking to measure users' attitudes and preferences of MFA. Two main approaches have been taken in these studies—questionnaires and surveys, and laboratory studies. This paper looked at two studies done, one in which a survey was used, and the other in which a laboratory study was used.

2.1.1 Measuring user attitudes in a laboratory study

A study done in 2010 [5] looked at user preferences for authentication methods when it came to eBanking. It compared participants' experiences across three different methods of authentication: 1-factor via password, and two different types of two-step verification. The researchers wondered if the environment in which an authentication method was being used (e.g. eBanking, which users would hope to be very secure) would influence preferences and opinions. They found that most of their participants preferred the 1-factor method and saw it as the most secure and convenient. However, they also found that for those who had previous experience with 2FA methods, they rated the two

2FA methods available in the study as more usable than their counterparts who did not have 2FA experience. There are obvious limitations to this study, however, as it was done more than ten years ago.

2.1.2 Measuring user attitudes through surveys and questionnaires

A study done at BYU in 2019 [6] surveyed 4,275 faculty, students, and staff. The study focused on the usability of Duo Security. The 30-question survey focused on a few things such as whether participants thought Duo actually protected them, how usable Duo was, and common concerns they had about Duo's usability. The limitations of this study were that participants were recruited only from BYU, but since the participants for this paper came from almost the same population, the findings should be as relevant as this paper's sample is representative of the population of BYU students. The main finding of the study done at BYU in 2019 was that participants felt Duo was secure and easy to use.

2.2 Studies on MFA Adoption

Studies that focus on analyzing the adoption of MFA among users are more aligned with the purpose of this paper's research. Many different methods were used to analyze the adoption of MFA among users, but a few common impediments to adoption remained consistent throughout all the research that was reviewed. We review two of those items here: too busy, and the learning curve. We will also look at the three works of literature that those items were taken from, and their limitations.

2.2.1 Too busy to use MFA

Ackerman [7], used fear appeal video messages to promote adoption among the 90 people that participated in this study. The participants were immediately surveyed after the video. Although 83% of the participants agreed that 2FA services were easy to use, the next week when the researchers had participants take a follow-up survey, they

found that 62% of them did not adopt because they were too busy to set it up. Another study which focused on how to create videos that promoted better security practices, found that the second most mentioned reason for not using 2FA was lack of time (the first was that they forgot) [8].

2.2.2 The perceived learning curve

In a study done at Carnegie Mellon University [9], researchers explored the adoption of Duo Security among its faculty, students, and staff members. They were interested in what hindered and drove adoption among their population of interest. Some of their findings suggested that for those who had never used 2FA before, they were more likely to perceive it as more difficult to use than it actually was. In some of their open-ended questions, students reported that using Duo was easier than they thought it would be. In the end, the users in their study found Duo to be more usable than anticipated.

2.2.4 Limitations of the studies

There were limitations to all of the studies that were just looked at. Colnago et. al. [9] mentioned their concern that they seemed to have under sampled non-adopters. The study that used 2FA as a use case for creating videos that promote better security practices mentioned that a more longitudinal study was needed to observe the behavior of participants after they watched the video tutorials [8]. Finally, Ackerman [7] admits that its sample might not be completely representative of millennials in general.

3 Study of Who Uses Multi-Factor Authentication

This work is an exploratory study to see if BYU students use the MFA features provided by popular websites such as Google, Facebook, Instagram, etc. The specific research questions focused on are:

- What are the differences between students that use MFA and students that do not?
- Which websites had more accounts with MFA enabled and why?
- What is the relationship between students' privacy behaviors and their use of MFA?

3.1 Data Collection Method

An online survey was published for the purposes of this study. The 26-question survey was made up of a few different parts:

- Demographics
- MFA use and attitudes
- Privacy practices

After getting the participants approximate age, year in school, gender, and college they were enrolled in, participants were asked whether they used MFA on any of the popular websites that offer MFA. The participants were then asked to give details about their feelings about the importance of privacy and their current privacy practices. The survey included 3 questions that used a Likert Scale. Depending on their responses, participants saw the set of questions that was most applicable to them. The survey questions can be found in Appendix A.

3.2 Ethical Considerations

The research described in this paper was done after many potential ethical problems were taken into consideration. The study was approved by BYU's Institutional Review Board before the survey was published and active advertising began. All responses were anonymous and kept confidential. Participation was voluntary, and participants were informed that at any point during the survey, they could withdraw without any consequence to themselves. Before the survey began, participants received

an explanation of the purposes of the survey, its risks and benefits, and provided their implied informed consent.

3.3 Mechanics of the Study

After receiving approval from BYU's Institutional Review Board, the online survey was published. Participants were volunteers who were recruited through various means such as: department newsletters, social media, or word of mouth. Participation was compensated. After receiving and reviewing the information that was given on the purpose and mechanics of the study, participants gave their implied consent and then took the approximately 10-minute survey. After completing the main survey, participants could be redirected if they chose to another separate survey where they could input the information that was needed so that they could be compensated. No follow-up survey was used. Participation in the study ended with the completion of the survey.

4 Results

4.1 Sample

The participants consisted of 44 undergraduate students, and 3 graduate students. A total of 25 students identified as male, and 22 students identified as female. They were evenly split between technical colleges and non-technical colleges; 22 students were from Physical and Mathematical Sciences, and 24 students were from Life Sciences, Family Home and Social Sciences, Business, Fine Arts and Communications, and Education, with one student from a college not listed. There were 4 participants that gave partial responses. Their responses will be included in the data for the sections of the survey which they answered but will not be counted in the sections where they gave an incomplete response.

The responses will be split into two groups throughout the rest of the discussion of the results of the survey; students who indicated they use MFA, and students who indicated that they did not use MFA. Students that use MFA with any of the websites listed in the survey will be referred to as MFA students, and students that did not use MFA with any of the websites will be referred to as non-MFA students.

4.2 Sample & Population

BYU's student population is made up of 33,181 undergraduate and 2,834 graduate students. That means the undergraduates make up about 92% of the population, and 8% are graduate students. 50% of BYU's students are male, while 50% are female [10]. This study's survey did not ask for any other demographic information, so only the demographic information that can be compared has been included in this paper. The participants who were volunteers from this population were 94% undergraduate and 6% graduate students. This sample's male-female ratio was 53% male 47% female.

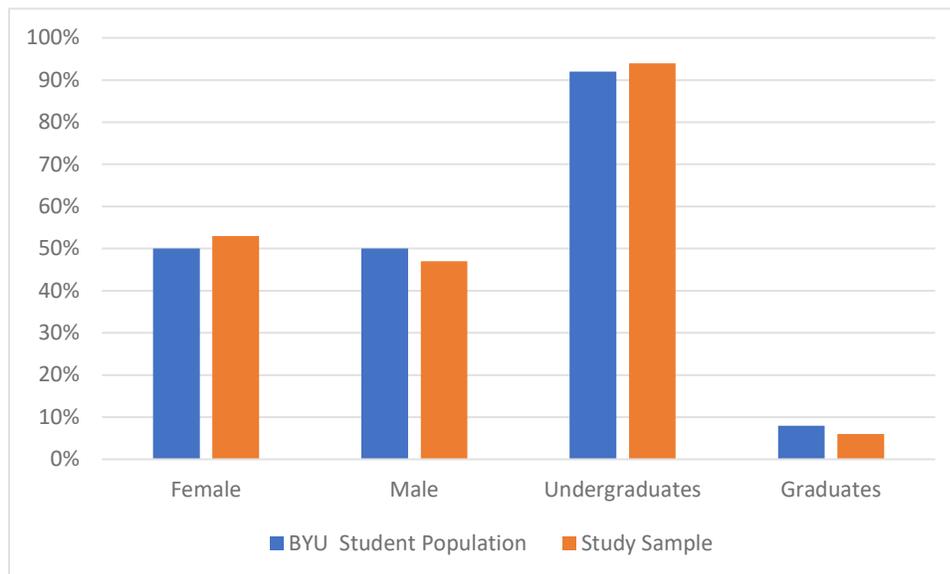


Figure 1: Comparison of BYU's student population and this study's representative sample of the population.

Figure 1 above gives a visual comparison of BYU's student population and the study sample. As can be seen, the two groups are similar in the demographics that the survey asked for. However, there are many other demographics that characterize BYU students which this study's survey did not ask for, so the extent to which the study sample represents BYU's student population is unknown because some of those details were not retrieved from the participants.

4.3 Differences Between MFA Students and Non-MFA Students

4.3.1 Technical vs. Non-Technical MFA Use

While analyzing the data, one of the questions that was asked was: is there a difference between the MFA use of technical vs. non-technical students? This work defined technical students as students majoring in fields such as math, science, and engineering. Non-technical students were students majoring in humanities, arts, business, or social sciences. The hypothesis was that perhaps technical students would be more inclined to use MFA than non-technical students. However, the results of this study did not seem to indicate that this was the case.

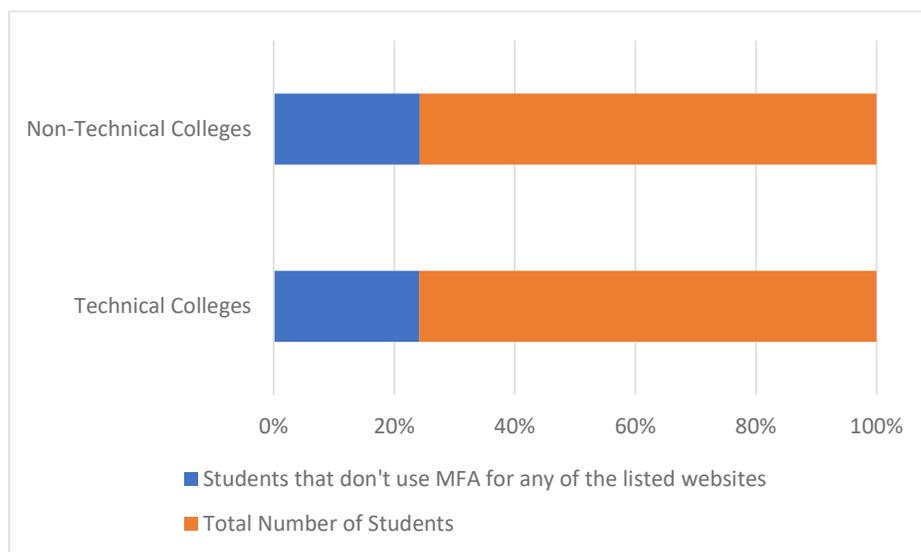


Figure 2: Stacked bar chart showing ratio of non-MFA students to the total number of students that participated in the survey from non-technical and technical colleges.

Although there were slightly more non-technical college participants than technical college participants who said that they did not use MFA for any of the websites listed in the survey, there were also slightly more non-technical than technical college participants overall. As can be seen in Figure 2, the ratio of students that don't use MFA to the total number of students for both technical and non-technical colleges is 32%. Therefore, this study did not find any difference between the MFA use of technical and non-technical college students.

4.3.2 Internet Usage on MFA Use

Another question that was asked while reviewing the data was: did students who used the internet more daily also use MFA more? Some interesting observations were made. Figure 3 is a chart of the time spent on the internet everyday by all the participants.

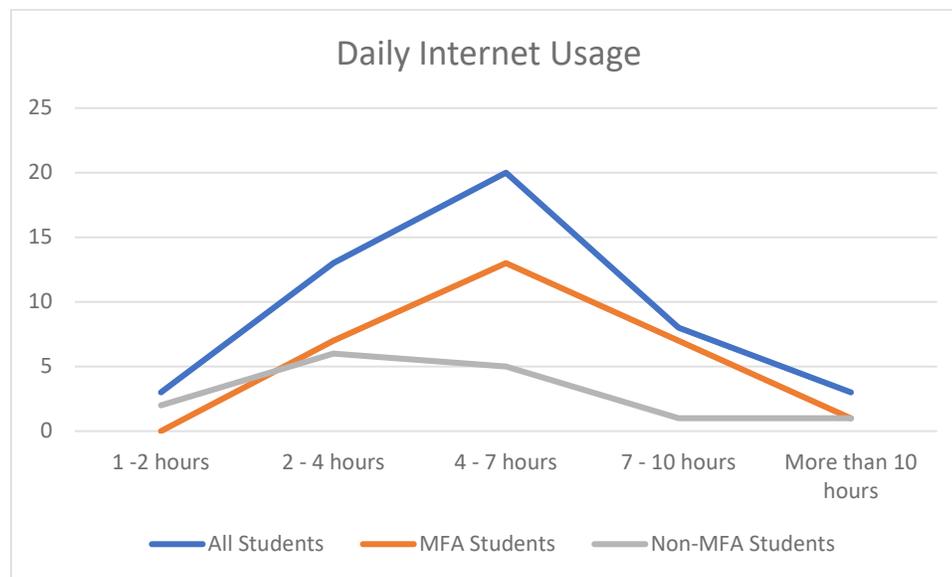


Figure 3: Line graph of daily internet usage of all students, MFA students and non-MFA students.

Figure 3 shows how many participants use the internet for a given number of hours every day. The blue line, representing the responses of all of the student participants, peaks at 4 – 7 hours. The median number of hours for all students was 4 – 7 hours. The orange line

shows the internet usage of students that use MFA on the listed websites. Their peak usage is also at 4 – 7 hours, and that was their median number of hours as well. The gray line represents the responses of the students that don't use MFA. As can be seen in the graph, the non-MFA students used the internet less everyday than the MFA students. Their median internet usage time was 2 – 4 hours. They also used the internet less than the total number of participants.

To determine whether the difference between internet usage of the MFA and non-MFA students was statistically significant, a t-test was run on the data sets from the two groups. Table 1 shows how the different survey options (i.e. 2 – 4 hours, More than 10 hours) were turned into ordinal values.

Time	Assigned Value
1 - 2 hours	1
2 - 4 hours	2
4 - 7 hours	3
7 - 10 hours	4
More than 10 hours	5

Table 1: Table of time spent on the internet to the assigned numeric value for the t-test.

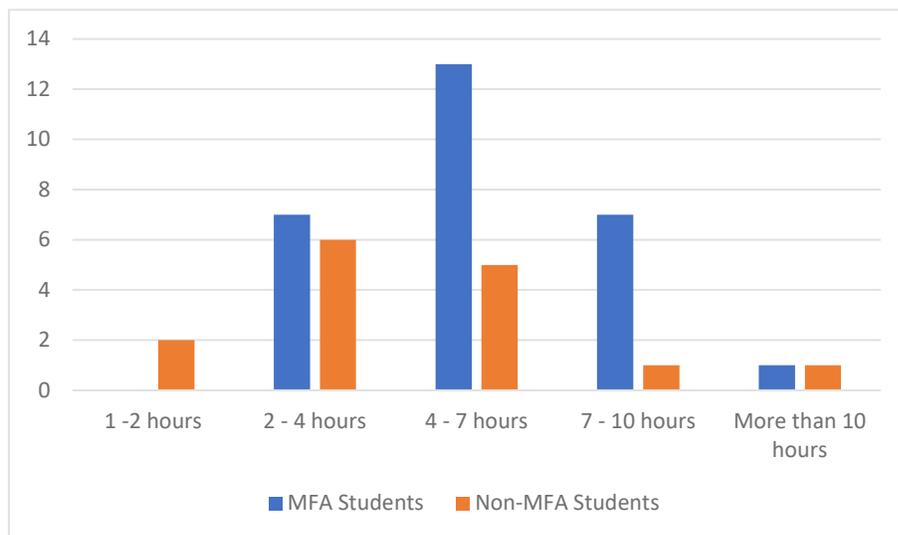


Figure 4: Bar chart of MFA and non-MFA students' internet usage; appears to be a normal distribution.

After assigning numeric values to each of the different options that were listed in the survey, a one-tailed, two-sample unequal variance t-test was performed on the following sets of data in Table 2. The data was assumed to have a normal distribution. As can be seen in Figure 4, when plotted, the two data sets result in a normal distribution.

After running the t-test, the resulting p value was $p = 0.04996414$. The t-test was one-tailed because the question asked about the data was “Do MFA students spend more time on the internet than non-MFA students?” The results of the t-test were statistically significant as $p < 0.05$.

The findings of this statistical analysis were interesting, as it indicates there might be a relationship between the amount of time students at BYU spend on the internet every day, and whether they were more likely to use MFA or not. Unfortunately, the two sets of data were not equal, and their respective means were not the same either, so more surveying may need to be done to confirm this finding.

MFA Students	Non-MFA Students
2	1
2	1
2	2
2	2
2	2
2	2
2	2
2	2
3	2
3	3
3	3
3	3
3	3
3	3
3	4
3	5
3	
3	
3	
3	
3	
4	
4	
4	
4	
4	
4	
4	
4	
5	

Table 2: Responses of internet usage of MFA and non-MFA students.

4.3.3 Gender and MFA Use

The relationship between gender and MFA use was observed. There were 6% more men that participated in this survey than women, so that should be kept in mind. There were more responses from participants who identified as male than female. The results of gender and MFA use can be seen in Figure 5. As will be seen from the figure, there was a larger percentage of males that responded to the question of whether they used MFA or not than females. 46% of the results were from females, and 54% were from males.

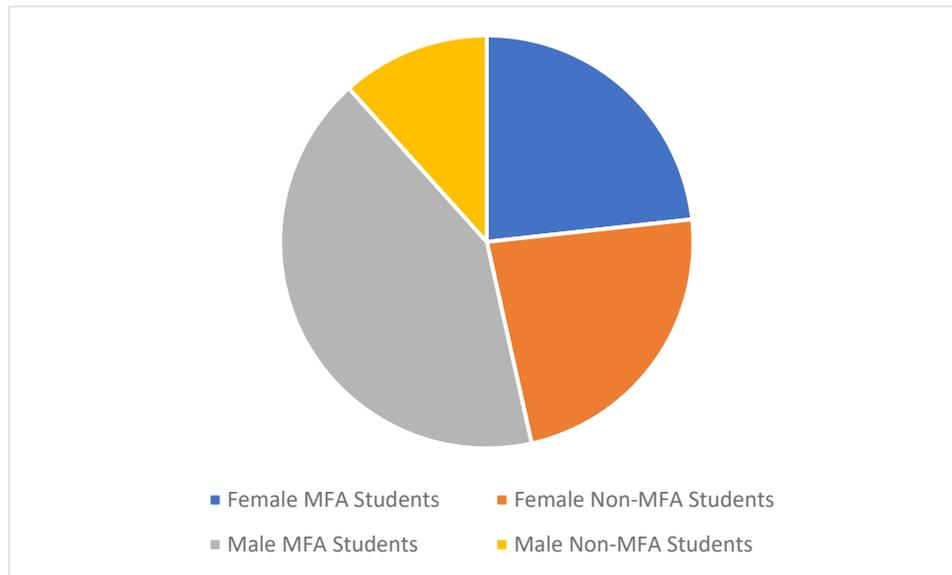


Figure 5: Pie chart of male and female use of MFA.

A statistical analysis was done on the data from Table 3. A chi-square test for independence was done to determine whether the two categorical variables (gender and MFA use) were related. Table 3 shows the expected and actual frequencies of MFA use by gender. Expected frequencies were calculated using the column and row totals for the actual data. After running the chi-square test on the data sets in Table 3, a p-value of $p = 0.052449$ was calculated. Since p was not less than 0.05, the data does not give a 95%

confidence that the two categories are related, but there is some indication that they might be.

	Female Actual	Female Expected	Male Actual	Male Expected	Grand Total Actual
MFA Students	10	13.02325581	18	14.97674419	28
Non-MFA Students	10	6.976744186	5	8.023255814	15
Grand Total	20		23		43

Table 3: Expected and actual frequencies of MFA Students and non-MFA students by gender.

4.4 Website Providers' MFA Feature

This study was especially interested in which websites saw more MFA use from the students who responded to the survey. Table 4 shows the overall number of accounts with each website from the total number of participants who responded to the survey.

Table 4 is ordered by the Total Accounts column in descending order. All the websites listed were websites that have the ability to have MFA enabled on a user's account. These numbers in Table 4 were retrieved by asking survey respondents to indicate which websites they owned an account with. After indicating which website they owned an

Website	Total Accounts	MFA Accounts	Percentage of MFA Accounts
Google	47	16	34%
Facebook	42	11	26%
Amazon	41	11	27%
Instagram	39	7	18%
Apple ID	33	12	36%
Slack	33	4	12%
Microsoft	31	8	26%
LinkedIn	30	4	13%
WhatsApp	25	3	12%
Dropbox	19	3	16%
GitHub	18	4	22%
PayPal	18	3	17%
Twitter	16	2	13%
Snapchat	16	1	6%
Intuit Turbo Tax	12	3	25%
LastPass	10	3	30%
Yahoo	10	2	20%
Evernote	6	0	0%
Tumblr	3	0	0%

Table 4: Number and percentage of MFA accounts for each website.

account with, participants were asked whether they used the optional MFA feature for those accounts. Table 4 shows the percentage of MFA accounts for each website.

Numerically, Google had the most total accounts and accounts with MFA enabled, while Tumblr had the least number of accounts. Figure 6 gives a different perspective to the above raw data.

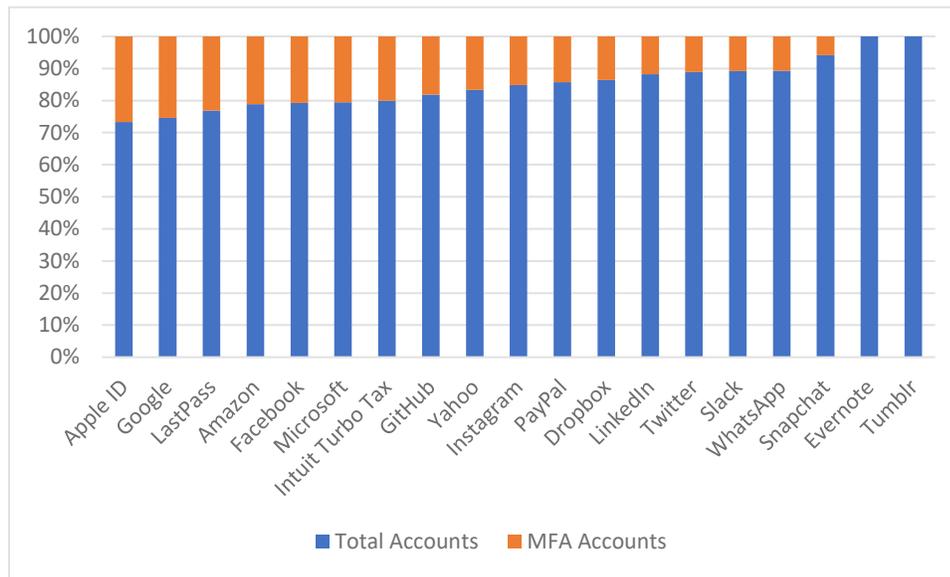


Figure 6: Proportion of MFA accounts to total accounts.

Apple ID, though it had 14 less accounts than Google, had proportionally more MFA account users than Google did. LastPass as well, though it had much fewer users than Amazon and Facebook, performed a little better with its number of MFA accounts. In order to get a sense for why this was, the comments of the students that had MFA enabled on their Apple ID and LastPass account were looked at. There were two comments that specifically mentioned LastPass or Apple ID: “LastPass stores my passwords, so I want it to be extra secure. If someone gets the password to LastPass, they still won’t be able to get access to my other passwords”, Apple ID: “I think it’s required (or I just can’t figure out how to turn it off).”

Two comments are not representative, but along with the results of the survey, there does seem to be an indication that the type of material stored on an account (passwords in the case of LastPass for example) might influence a student's desire to enable MFA. This research did not attempt to find out if Apple ID required MFA for the accounts held with them but considering that there were 33 total Apple ID accounts and only 11 of them enabled MFA, it should be safe to assume that Apple ID's MFA feature is not required. It is possible the participant who made the comment about Apple ID's MFA feature just could not figure out how to turn it off.

4.5 Privacy Behavior and MFA Use

Overall, 28 (59%) of the participants used MFA on at least one of the websites they owned an account with, and only 15 (32%) of the participants did not use MFA on any website. There were 4 (9%) respondents who failed to respond to this question, so they were not included in this grouping. However, 42 (89%) students responded "Yes" to the question: "Do you think that using multi-factor authentication could help keep your accounts more secure?" and only 4 (9%) students responded "Don't know" to the same question. There appeared to be a discrepancy between behavior and students' belief that MFA would help protect their accounts.

4.5.1 Relationship between MFA use and good password practices

A section of the survey asked participants if they followed certain prescribed "best practices" for creating passwords. After looking at the two groups, MFA and non-MFA students, the following data was compiled. Figure 7 shows the results of the two groups combined. Table 5 shows the mapping between the question numbers and the actual questions.

Question	Value
How often do you forget your passwords, causing you to create new ones?	Q1
On sites that don't have password requirements, how often do you use the following principles when making a new password? - More than 8 characters	Q2
On sites that don't have password requirements, how often do you use the following principles when making a new password? - Includes numbers	Q3
On sites that don't have password requirements, how often do you use the following principles when making a new password? - Includes special characters	Q4
On sites that don't have password requirements, how often do you use the following principles when making a new password? - Makes a different password for every account	Q5

Table 5: Mapping between question and the value assigned to it in Figure 7.

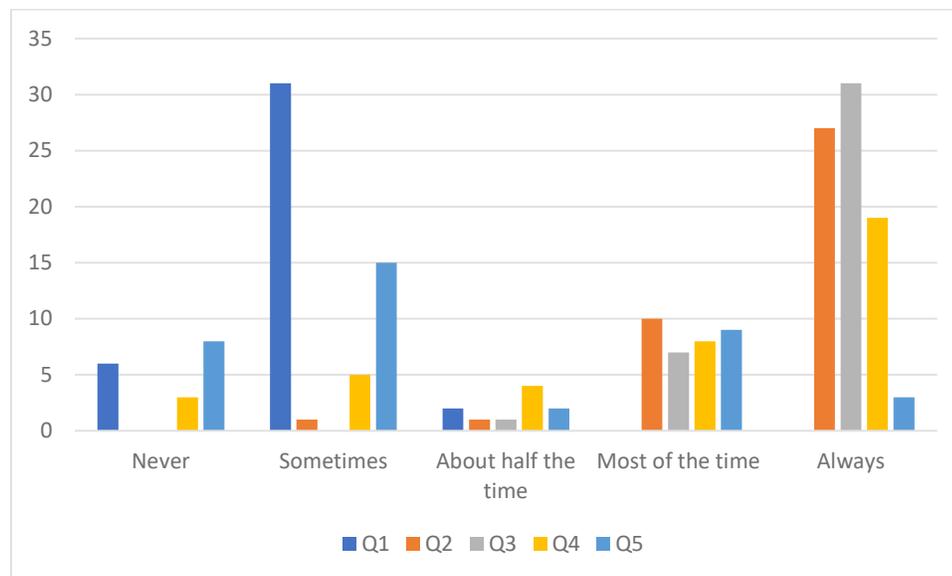


Figure 7: Distribution of responses on questions in Table 5.

For the most part, the students who participated in this study employed good password creation practices. The students in this study reportedly rarely forget the passwords to their accounts, they almost always use more than 8 characters, and include numbers and special characters. Unfortunately, despite employing these great password creation practices, 8 (17%) of the students reportedly never make a different password for every account, 15 (32%) of the students make a different password sometimes, and 13 (28%) of the students do it more regularly.

It appears that despite students creating strong passwords, they are using those strong passwords across different accounts that they own. Figure 8 shows the same chart, but the group is just non-MFA students. The two bar charts are very similar in the distribution, but there are some interesting things to note. The total number of students that responded they never make different passwords was 8, but for non-MFA students it was 2. That means that 75% of those that responded never to Q5 were MFA students.

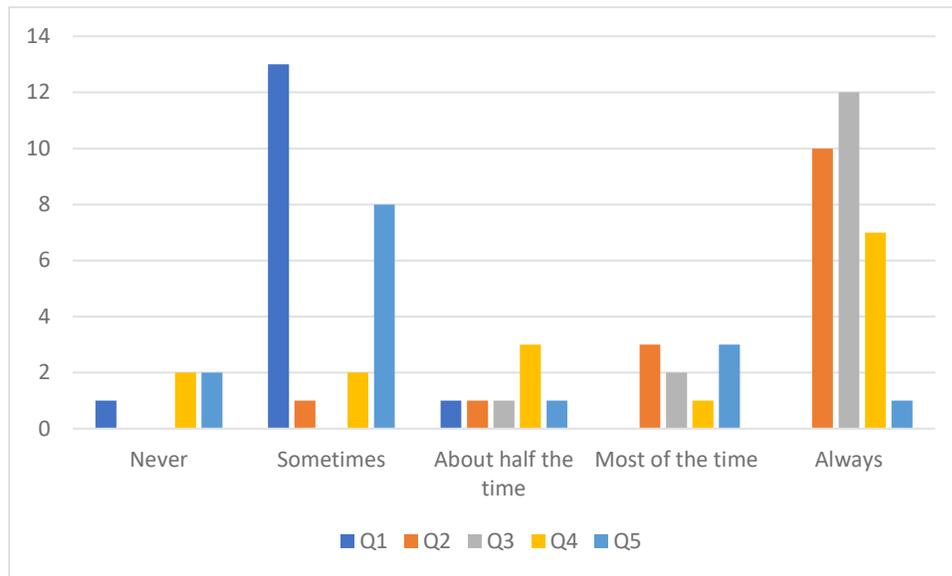


Figure 8: Distribution of non-MFA student responses on the questions in Table 5.

5 Discussion of Results

After an analysis of the data, the following items can be discussed.

5.1 Differences Between MFA Students and Non-MFA Students

There were several differences found between MFA and non-MFA students. It was determined that there was no difference between technical and non-technical colleges when it came to their students use of MFA. There was a positive correlation between the number of hours spent on the internet everyday by MFA and non-MFA students, with MFA students typically spending longer on the internet everyday than non-MFA students. Gender was also a factor that was looked at, and it was determined that

there was a slight difference in male and female use of MFA, though the difference was not notable enough to be statistically significant, but the trend was that men used MFA on the internet more than women did.

5.2 Websites' MFA

There did seem to be a slight indication that websites that stored what would be considered more “private” information had more students enabling the MFA feature on their account. The example looked at for this situation was LastPass, which is a password manager. Apple ID was another website that had a larger proportion of their users using the MFA feature than other websites.

5.3 Students' Privacy Behavior

In general, the students that participated in this study said that privacy was important to them, and most of them believed that enabling MFA on their internet accounts would increase the security of those accounts. Despite this, however, almost one-third of the participants did not enable any kind of MFA on their online accounts. Another observation that was made was that MFA students might possibly be making fewer passwords than non-MFA students, contradicting the idea that MFA students in general have better privacy practices online than non-MFA students.

5.4 Limitations

Though the sample was representative of BYU's population in certain aspects, there were many demographics that were not addressed in this study, so the study sample might not completely represent BYU's student population. Also, it is possible that non-MFA students were under sampled, as there were at least ten fewer non-MFA responses than MFA responses. Since a survey was used as the data collection tool, there is likely some survey-bias in the responses.

6 Conclusion

Only 34% of the students sampled in this study that own an account with Google have enabled Google's MFA feature on their account. Top website providers like Google, Facebook, Amazon, etc. have a long road ahead in order to increase the adoption of MFA among their users. The findings in this research may provide insight into increasing MFA accounts.

The purpose of this research was to explore the usage of MFA among students' internet accounts. Though there were limitations to the study, there were some important findings. Companies like Google and others could use LastPass and Apple ID's MFA onboarding as an example. More research will need to be done however on why certain website providers have more MFA accounts than others. That was briefly discussed in this study, but the subject in its entirety was outside the scope of the subject of this study.

Another insight obtained from this study is that perhaps an increased focus in educating females (and everyone) on the threats of cyber crime would be effort well-placed. Ultimately, this study suggests that more extensive sampling needs to be done in order to determine the degree to which MFA is being enabled on online accounts.

REFERENCES

- [1] V. Zimmerman and N. Gerber, “The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes,” *International Journal of Human-Computer Studies*, vol. 133, pp. 26-44, January 2020.
- [2] B. Bhana and S. Flowerday, “Passphrase and keystroke dynamics authentication: Usable security,” *Computers and Security*, vol. 96, September 2020.
- [3] A. Jansone, K. Lauris, and I. Šaudinis, “Multi factor authentication as a necessary solution in the fight with information technology security threats”, in *Proc. of the 10th Int. Scientific and Practical Conf.*, vol. III, pp. 114-120, June 2015.
- [4] W. Kang, H. Liu, W. Luo, and F. Deng, “Study of a Full-View 3D Finger Vein Verification Technique”, *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1175-1189, July 2019.
- [5] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, “Usable security: User preferences for authentication methods in eBanking and the effects of experience,” *Interacting with Computers*, vol. 22, pp. 153-164, October 2009.
- [6] J. Dutson, D. Allen, D. Eggett, K. Seamons, “Don’t punish all of us: Measuring User Attitudes about Two-Factor Authentication,” in *2019 IEEE European Symposium on Security and Privacy Workshops*, 2019.
- [7] P. Ackerman, “Impediments to Adoption of Two-factor Authentication by Home End-Users,” in *SANS Institute Information Security Reading Room*, September 2014.
- [8] Y. Albayram, M. M. H. Khan, and M. Fagan, “A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA),” *International Journal of Human-Computer Interaction*, vol. 33, pp. 927-942, April 2017.
- [9] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, N. Christin, “It’s not actually that horrible: Exploring Adoption of Two-Factor Authentication at a University,” April 2018.
- [10] *Facts & Figures*. Accessed on: May 29, 2021. [Online]. Available: <https://www.byu.edu/facts-figures>

APPENDICES

Appendix A: Survey Questions

What is your gender
Which college at BYU are you in
What year are you in school
On average, how many hours do you spend on the internet every day
Do you have an account with any of the following websites/applications
Do you use the optional multi-factor (two-factor) authentication feature with any of the following websites
For the websites where you use multi-factor authentication, why do you use it
For the websites where you use multi-factor authentication, what are some of the reasons you use it?
For the websites where you don't use multi-factor authentication, why not
For the websites where you don't used multi-factor authentication, what are some of the reasons you don't
Have you ever tried using multi-factor authentication for any of the sites you own accounts with, but then stopped using it
Why did you stop using multi-factor authentication on those sites
What are some of the reasons you stopped using multi-factor authentication on those sites
Have you ever used multi-factor authentication before?
In the past week, how often have you used multi-factor authentication
Do you feel that using two-factor authentication keeps your account more secure
Rate how secure you feel about the following types of
o Accounts with multi-factor authentication enabled
o Accounts without multi-factor authentication
How important is your privacy
Indicate yes or no on the questions below
o Do you ever check to see if the devices logged in to your account are yours?
o Have you ever seen devices logged into your account that weren't yours?
o Do you stay logged in to your accounts?
o Are your devices password protected?
o Do you use multi-factor authentication for your devices?
o Do you save credit card information on your accounts?
How often do you forget your passwords, causing you to create new ones
On sites that don't have password requirements, how often do you use the following principles when making a new password?
o More than 8 characters
o Includes numbers
o Includes special characters
o Makes a different password for every account
Do you worry about getting hacked
Have you, or anyone you know, been hacked
How serious was the hack
Do you wish you used better privacy practices online

Rate how you feel on the following statements.
<input type="radio"/> I find multi-factor authentication to be annoying
<input type="radio"/> I find multi-factor authentication to be convenient
<input type="radio"/> I find multi-factor authentication to be inconvenient
<input type="radio"/> I don't have time to use multi-factor authentication