The Emotional Impact of Multi-Factor Authentication for University Students

DAVIS ARNOLD, Abilene Christian University, USA
BENJAMIN BLACKMON, Abilene Christian University, USA
BRENDAN GIPSON, Abilene Christian University, USA
ANTHONY MONCIVAIS, Abilene Christian University, USA
GARRETT POWELL, Abilene Christian University, USA
MEGAN SKEEN, Abilene Christian University, USA
MICHAEL THORSON, Abilene Christian University, USA
NATHAN WADE, Abilene Christian University, USA

Abilene Christian University recently rolled out multi-factor authentication (MFA) to the entire student body. Previous work has found frequent negative reactions and dissent experienced in university settings in regard to MFA. This can lead to decreased compliance or the use of less secure passwords to compensate. We hypothesize these responses are tied to the emotional impact of using required MFA for critical tasks. We present an empirical study on user perception of adopting two-factor authentication (n=465). Our findings indicate that, due to the time sensitive nature of many tasks that required MFA, university students are likely to experience strong negative emotions towards MFA that drastically lower their perceptions of its utility and usability. However, our findings also show that these negative emotions can be at least partially mitigated when users feel more personally secure due to MFA, which can in part be controlled by rollout strategy and communication.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: multi-factor authentication, usable privacy and security, emotions

ACM Reference Format:
Davis Arnold, Benjamin Blackmon, Brendan Gipson, Anthony Moncivais, Garrett Powell, Megan Skeen, Michael Thorson, and Nathan Wade. 2022. The Emotional Impact of Multi-Factor Authentication for University Students. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3491101.3516809

1 INTRODUCTION

Authentication is part of our everyday world of websites and apps, yet it remains difficult and often insecure. Passwords are often difficult to remember due to administrative and technical requirements on what they can contain and how often they are changed [6]. Many password meters provide bad advice because they are not data-driven [13]. To make matters worse, even users with strong passwords can still be hacked via sophisticated phishing attacks [7, 14]. In response to these threats, multi-factor authentication (MFA), a security practice where a user has to use one of multiple MFA methods in order to verify their identity, is becoming more prominent. This is done to prevent unauthorized access

Manuscript submitted to ACM

to these systems through a layered defense where even if one vector is compromised, others remain secure. While the practice offers a significant increase in security, it does not come without a cost in both time and user frustration [2, 15].

As with any security practice, user buy-in is crucial for its ultimate success. For instance, unusable password policies can lead users to write them down on paper, which possibly circumvent the point of passwords [5, 10]. However, very little has been written about the factors that can lead to resistance of MFA. Beginning in April 2021, Abilene Christian University (ACU) rolled out MFA for all faculty, staff, and students. This made MFA mandatory for accessing all online university resources, including access to the university learning management software (myACU). However, many university courses regularly utilize a lockdown browser for certain assignments, which requires MFA for every use. Many students have expressed great displeasure at the additional required step of logging into their university accounts, especially for timed activities such as quizzes and tests. The rollout of MFA presented an excellent opportunity to study its emotional impact on students.

We present an empirical study to determine university students' perceptions of and emotional reactions to multi-factor authentication on the Abilene Christian University online system. We conducted a survey and analyzed students' responses to questions about their experiences with MFA at ACU. Our analysis answers the following research question with regard to university students:

- **RQ**: To what extent are university students impacted emotionally by required multi-factor authentication?

Contribution: We provide two important contributions in this paper. Most importantly, this paper is the first to empirically investigate the emotional impact of required MFA on university students. Whereas other studies have found it annoying [2] or frustrating [1], we are the first to specifically look at which emotions arise from the process and how they are linked to perceptions of usability of MFA. Second, we provide concrete ideas for mitigating the negative emotional impact we have observed.

Impact: As demonstrated in Section 2, MFA is an important measure in modern online security, but it is often resisted by users. A better understanding of why this happens can help provide better rollouts and better communication to increase user acceptance and use of MFA. This can lead to globally safer user experiences and more secure systems.

2 BACKGROUND

Multi-factor authentication is a security model with at least one additional step beyond inputting a username and password to safely access a website or application. It is mainly designed to limit the damage caused by password breaches and both online and offline cracking attacks. However, it has long been known that a poor user experience for privacy and security can lead to worse security outcomes [16]. Indeed, users often find the additional burden of MFA to significantly negatively impact user experience [3]. MFA is most often implemented with physical tokens, email or SMS messages, or phone calls. Recent work has shown that university students found mandatory MFA to be annoying, but not unreasonable, and even led to MFA adoption on other platforms [2].

A recent study by Abbot and Patil examined the impact of two-factor authentication on user experience in the context of a university [1]. The study was conducted after MFA was made mandatory for faculty, staff, and students. To measure the impact of two-factor authentication on university employees and students, the researchers utilized a questionnaire on UX and security perceptions of the university's authentication system. The study also examined authentication logs to determine which type of MFA implementation had the fewest failed attempts and could therefore be seen to have the fewest UX barriers. They found that people had no complaints using two-factor authentication for certain systems containing sensitive information, but resented two-factor authentication being required to log into all

university resources. While Abbot and Patil mainly focused on the balance between user experience and security, they suggested future work explore the emotional impact of mandatory MFA. We follow that call.

3 METHODOLOGY

We constructed a survey to collect students' attitudes on MFA and its recent implementation on the ACU online system and sent it out in one wave. All data was de-identified before analysis. The survey contained a consent form, questions about student year and chosen authentication method, and nine questions to discover students' attitudes towards MFA. Questions 1-2 (see Table 1) were in yes/no format, and 3-7 (see Table 2) were on a five-point Likert scale. Questions 3-7 were adapted from the Discrete Emotions Questionnaire (DEQ) [4] to a short survey style in the context of usable privacy and security. In order to generate maximum responses, we kept the survey short and put in one question for each type of emotion other than sadness as we did not expect MFA to generate feelings of emptiness, loneliness, or grief. We included two happiness questions in a attempt to balance out the negative emotions. The survey was sent out to all on-campus full-time students by the Vice President of Student Life at ACU in an email.

All research methods were examined and approved by the ACU ethics institutional review board (IRB). Student's participation was voluntary, included informed consent, and incentivized with prize drawings. Each member of ACU's SIGCHI local chapter completed the university's required training in research ethics before accessing any identifiable human data. The members trained on ethical issues related to human subjects and proper and full disclosure of risks, benefits, and consent for our study.

Limitations - The primary limitation to our study is that of sample selection bias. Perhaps the people who have stronger opinions about MFA were more likely to take the survey. We avoided this by having neutral wording in the solicitation email, having a neutral third party send out the solicitation, and offering prizes for participation. A secondary limitation is in our adaptation of the DEQ, which may not have captured the full range of emotions.

	Question	% Yes	% No
1.	Do you think the extra effort of multi-factor authentication is worth the potential increase in security for your ACU account?	38.1%	61.9%
2.	Has multi-factor authentication prevented you from accomplishing a time sensitive task?	57.6%	42.4%

Table 1. Questions and results of the Yes/No portion of the survey

	Question	Mean	SD
3.	I feel frustrated when asked to complete a multi-factor authentication on myACU. (Dg)	3.15	1.18
4.	I feel more secure using multi-factor authentication for my ACU account. (R)	2.29	1.07
5.	I feel like using multi-factor authentication is doing my part to make myself more secure. (H)	2.75	1.18
6.	I feel like using multi-factor authentication is doing my part to make ACU more secure. (H)	2.98	1.24
7.	I have felt stressed because of required multi-factor authentication for myACU. (F)	3.42	1.33
8.	I have felt anxious because of required multi-factor authentication for myACU. (Ax)	3.00	1.43
9.	I have felt anger because of required multi-factor authentication for myACU. (Ag)	3.60	1.30

Table 2. Questions and results of the Likert scale portion of the survey with answers from "Strongly Disagree" to "Strongly Agree." From Discrete Emotions Questionnaire: Ag=Anger, Ax=Anxiety, Dg=Disgust, F=Fear, H=Happy, R=Relaxation

Factor #	Factor Name	Dependent Variable	Independent Variable	p-value	F-value
1	Anger	Anger	MFA is Worthwhile (Q1)	p < 0.001	359.833
			Stress (Q7)	p < 0.001	216.609
			Frustration (Q3)	p < 0.001	121.66
			Anxiety (Q8)	p < 0.030	5.297
			Time Sensitive Task Prevented (Q2)	p < 0.060	3.664
2	Worthwhile	MFA is Worthwhile	Feeling of Security (Q4)	p < 0.001	212.739
			Security for Self (Q5)	p < 0.001	55.734
			Security for University (Q6)	p < 0.020	6.662
3	Apprehension	Time Sensitive Task Prevented	Stress (Q7)	p < 0.001	121.025
			Anxiety (Q8)	p < 0.002	10.877
			Frustration (Q3)	p < 0.002	10.794
			Anger (Q9)	p < 0.200	1.828

Table 3. Results of the exploratory factor analysis with three factors and the multivariate ANOVA tests run on each factor. Independent variables are labeled with the questions from which they are drawn in Tables 1 and 2.

4 RESULTS AND DISCUSSION

A total of 465 students responded to our survey. A large majority of the students were undergraduate, with 26.9% (125) first-year students, 25.2% (117) second-year students, 22.4% (104) third year students, 16.1% (75) fourth-year students, and 9.5% (44) fifth-year and above students. The respondents reported using one or more of the following authentication methods: 92.1% (429) use a text message, 14.8% (69) use the Microsoft Authenticator app, 11.6% (54) use a phone call, and 2.6% (12) use an alternate email. Note that these percentages do not equal 100% as some respondents use more than one method. The response data to the questions are listed in Tables 1 and 2 and analyzed further below.

We examined the survey data in relation to our research question and analyzed the data to determine the reasons for students' reactions to MFA. First, we ran an exploratory factor analysis with varimax rotation on all of the attitude-related survey questions plus the question on the prevention of a time-sensitive task. After examining these analyses with three, four, and five factors, we determined three factors to have the best fit. All loadings totals for each of the factors were above 1, the cumulative variance accounted for was 64.2%, and X^2 (12, n = 465) = 19.86. p = 0.0698. We find that three factors are sufficient for this data. Cumulative variance can be low in social sciences [12], averaging 56.6% in a multi-disciplinary meta-analysis of exploratory factor analysis and factor loadings [8]. The high cumulative variance of our results indicates strong correlation within our proposed factors. We then performed ANOVA testing on each of the factors to find the strength of the correlations. We present the results of these tests in Table 3.

4.1 Factors

4.1.1 Anger (Factor 1). A lack of belief that MFA is worthwhile, stress, and frustration are all strong predictors of anger towards MFA. While anxiety is also correlated with anger (p < 0.030), the F-value indicates it is weak. Unexpectedly, being prevented from completing a time sensitive task is not a strong predictor of feelings of anger toward MFA. As we will see below in Factor 3, this causes different emotions. Many users believe that the idea of online security is someone else's problem [11] and could therefore believe it is not worthwhile for them to personally perform. If someone holds this idea and is asked to perform MFA multiple times per day, this could explain the strong correlation in our study to

anger. The fact that stress and frustration are such strong predictors of anger is interesting. Colnago et al. [2] do not mention anger at all, even though they do discuss frustration. Abbott and Patil [1] found that just 4% of their 1,600 chat transcripts with users about MFA mentioned anger, but do not discuss it further. Neither mention stress at all. User stress predicting anger is understandable because being required to complete MFA multiple times per day can compound little stressors into bigger ones in a phenomenon known as 'security fatigue' [11].

4.1.2 Worthwhile (Factor 2). The perception of the worth of MFA relies mostly on the feelings of security ($p < 0.001$) and one's contribution to their own security ($p < 0.001$). Interestingly, contributing to the university's security does contribute to the perception that MFA is worthwhile ($p < 0.02$), but the students' personal security has a much stronger correlation. Previous research has highlighted that users do not understand the security gains from adding MFA to their accounts. Redmiles et al. reported that users did not see the need to go through the hassle of MFA on their emails or social media accounts, but only saw value in using it for their bank accounts [9]. This is despite the danger of a compromised email account or the social ramifications of a hacked social media account spewing inappropriate or dangerous content. In other words, users must be personally convinced that MFA is important and necessary for them to find it a worthwhile shift in usability [1]. With all of this in mind, it seems that users cannot be relied upon to participate in MFA in good faith for the sake of the organization.

4.1.3 Apprehension (Factor 3). By far, stress ($p < 0.001$) is the most highly correlated emotion with being prevented from completing a time-sensitive task, with much weaker correlations with anxiety and frustration. A majority of students (57.6%) reported that MFA has prevented them from completing at least one time-sensitive task, such as taking a quiz or exam, submitting a large project, or completing a number of other assignments. All of these experiences can negatively affect a student's grades. Placing that kind of risk on a task with such a high failure rate (10% in [1]) can lead to a high emotional impact related to apprehensive feelings and then behaviors.

Colnago et al. reported users found MFA annoying, however, they had mostly positive perceptions due to the surprise found by users in its ease to implement [2]. Annoyance in their study did not seem linked to a negative overall experience and certainly not to apprehensive feelings. However, we found that negative emotions, such as stress, anxiety, and frustration, directly contributed to a student's negative experience and perception that MFA was worthwhile. These different results could be explained by experimental factors such as differences in MFA rollout or student body. However, they could also be explained by the fact that Colnago et al. only investigated annoyance and not the emotional impact of the rollout. Colnago et al. also reported that users developed negative perceptions when tasks were disrupted, which agrees with our results when students' time sensitive tasks were interrupted.

5 CONCLUSION

In this paper, we presented an empirical study to determine the emotional impact brought about by the implementation of required MFA at the university level. This was done through the analysis of student responses to a survey that measured their general opinions of MFA. Our findings show a direct emotional impact on students caused by the implementation of MFA, with students feeling an increase in stress, anxiety, and frustration which is linked to the prevention of the completion of time sensitive tasks. Additionally, when users did not feel that MFA made them more personally secure, they were less likely to find it worthwhile, a feeling correlated with increased anger. While MFA may be beneficial in mitigating security vulnerabilities, the emotional impact of MFA affects its perceived usability and therefore user adoption and continued participation. Even if required, if users feel the total burden is too high, they may attempt to alleviate that in areas they can control, such as password strength. IT Departments can mitigate these risks

in two ways. First, through clear communication of the personal value of increased security to required accounts, which has already been shown to be helpful [9]. Second, IT departments can provide more ways to avoid MFA preventing a user from completing a time-sensitive task. For instance, since campus IT knows a students' schedule, MFA could be disabled while in class. It could also be disabled while signed into the campus WiFi (not guest), which is already another factor of authentication.

Future work could further investigate and compare the usability of specific authentication methods compared to the types of associated emotions their uses evoke. While our study examined the general usability of the system as a whole, there may be large differences between authentication methods. Further research may also explore which MFA rollout strategies best mitigate the emotional impact and lack of usability experienced by the participants. This could inform IT organizations' decisions on types of communication, communication content, and supported authentication methods.

REFERENCES

[1] Jacob Abbott and Sameer Patil. 2020. How mandatory second factor affects the authentication user experience. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[2] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–11.

[3] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2013. A comparative usability study of two-factor authentication. *arXiv preprint arXiv:1309.5344* (2013).

[4] Cindy Harmon-Jones, Brock Bastian, and Eddie Harmon-Jones. 2016. The discrete emotions questionnaire: A new tool for measuring state self-reported emotions. *PloS one* 11, 8 (2016), e0159915.

[5] Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez. 2012. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE symposium on security and privacy*. IEEE, 523–537.

[6] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the sigchi conference on human factors in computing systems*. 2595–2604.

[7] John Marsden, Zachary Albrecht, Paula Berggren, Jessica Halbert, Kyle Lemons, Anthony Moncivais, and Matthew Thompson. 2020. Facts and Stories in Phishing Training: A Replication and Extension. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–6.

[8] Robert A Peterson. 2000. A meta-analysis of variance accounted for and factor loadings in exploratory factor analysis. *Marketing letters* 11, 3 (2000), 261–275.

[9] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages.. In *SOUPS*.

[10] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the sixth symposium on usable privacy and security*. 1–20.

[11] Brian Stanton, Mary F Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security fatigue. *It Professional* 18, 5 (2016), 26–32.

[12] Howard E Tinsley and Diane J Tinsley. 1987. Uses of factor analysis in counseling psychology research. *Journal of counseling psychology* 34, 4 (1987), 414.

[13] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, et al. 2017. Design and evaluation of a data-driven password meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3775–3786.

[14] Rick Wash and Molly M Cooper. 2018. Who provides phishing training? facts, stories, and people like me. In *Proceedings of the 2018 chi conference on human factors in computing systems*. 1–12.

[15] Jake Weidman and Jens Grossklags. 2017. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. 212–224.

[16] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX security symposium*, Vol. 348. 169–184.