Barriers and Motivations for Young Adults' Adoption of Multi-Factor Authentication (MFA)

Saoud Sultan A. Al-Kuwari
saoud.s.r.a.al-kuwari@northumbria.ac.uk

Abstract:

This study explores the reasons why young adults use or don't use Multi-Factor Authentication (MFA), which is an important tool for keeping online accounts safe from cyber threats. Even though MFA is known to be very important, many young people don't use it regularly. Through interviews, this research finds out how people feel about MFA, the problems they face, and some possible solutions. The results show that while people know MFA makes their accounts more secure, they don't use it because it's hard to set up, has usability problems, and because of bad experiences like account lockouts. On the other hand, people are motivated to use MFA to protect their personal data, stay safe from hackers, and feel more secure overall. Making MFA easier to set up, using biometrics like fingerprints, and having better ways to recover accounts can help more people start using it. This study gives suggestions on how to make MFA better and easier, so it can be used more by young people to create a safer online world for them.

1 INTRODUCTION AND RELATED WORK

Today, cyber threats like phishing, identity theft, and data breaches are everywhere. These threats make it very important to keep online accounts safe. Multi-Factor Authentication (MFA) is one way to add extra protection. MFA means using more than one step to log in, like a password and a code sent to your phone or using your fingerprint. It makes hacking harder, but still, many people, especially young adults, don't use it enough. This is surprising because young adults are good with technology. You would think they use MFA more, but many don't, and their accounts stay at risk.

Figure 1 Basic methods in MFA

This research is about why young people don't use MFA or why some do. Some studies have already looked at this. Colnago et al. (2018) found that MFA is very good at stopping hackers, but people think it's too much trouble to use. For example, having to wait for a code or

losing access to MFA if you lose your phone makes people frustrated. Pratama and Firmansyah (2021) said most people don't use MFA until they lose something important, like access to their accounts or data. This shows that people only act when it's too late.

Young people, like students, know that hacking is a big problem. However, even when they know the risks, they don't always use MFA. Kävrestad et al. (2024) studied how young people, who grew up with the internet, and older people, who didn't, use MFA. They found that young people like MFA options that are simple, like using fingerprints or face scans. These feel fast and easy to them. But when MFA is hard to set up or understand, they don't bother with it. Zaxmy (2022) looked at IT students who know a lot about technology. Even they don't use MFA much because they find it annoying or hard to manage.

Libicki et al. (2011) explained another big problem: people worry about what happens if they lose access to their MFA. For example, if someone forgets their password or can't get a code, they feel stuck and may stop using MFA altogether. Duo Security's report by Anise and Lady (2017) also said that bad experiences with MFA, like getting locked out of accounts or struggling with setup, make people avoid it. These negative experiences stay in their minds, even if they know MFA is safer.

All these studies are useful, but most don't look deeply at young adults and their personal reasons for using or not using MFA. Some focus on general problems, but they don't explain what makes MFA work or fail for young people. This research will look closely at young adults to understand their challenges and motivations. By focusing on their views, the goal is to find ways to make MFA easier and more useful for this group. This could help improve adoption rates and make online accounts safer for everyone. By answering this question, the study aims to provide actionable recommendations for enhancing MFA adoption rates. It will focus on improving user education, simplifying MFA systems, and integrating features that align with user preferences, ultimately contributing to a more secure digital landscape for young adults. Through this approach, the study not only builds upon existing research but also offers a fresh perspective on the unique challenges and opportunities associated with promoting MFA adoption among this critical demographic.

2 METHODOLOGY

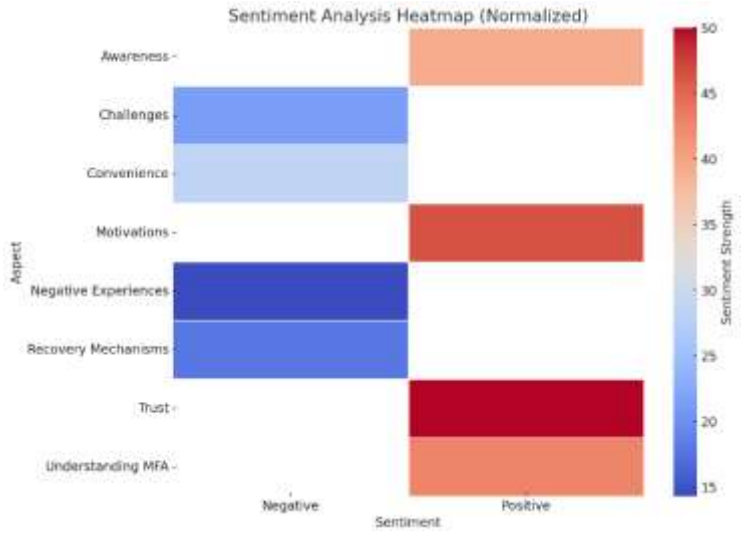
The study explored the barriers and motivations influencing young adults' adoption of Multi-Factor Authentication (MFA) through semi-structured interviews with participants aged 18 and above. Participants were recruited based on their active use of online accounts offering MFA and their willingness to discuss their experiences. The interviews, lasting approximately 20 minutes each, focused on participants' understanding of MFA, adoption behaviors, preferences, and challenges. Responses were noted, transcribed, and analyzed using thematic analysis to identify recurring patterns and insights.

Ethical considerations were central to the study design. Participants were provided with detailed information about the study's purpose, procedures, and their rights. Informed consent was obtained, including permission to record interviews for analysis. Data confidentiality was ensured by anonymizing participant information with unique codes. Ethical approval was granted by the Department of Computer and Information Sciences ethics committee, ensuring the study met high ethical standards.

3 RESULTS

The findings of this study reveal significant insights into young adults' perceptions and adoption of Multi-Factor Authentication (MFA). Participants largely understood MFA as a security measure designed to enhance the protection of online accounts by requiring multiple verification steps. This understanding often stemmed from personal experiences, such as setting up work emails or online banking, where MFA was mandated.Despite this awareness, the adoption of MFA was inconsistent. While some participants had enabled MFA on critical accounts like banking and email, others avoided using it altogether. This disparity was influenced by several challenges, including the perceived inconvenience of MFA processes, difficulties in remembering codes or passwords, and frustrations caused by

negative experiences such as account lockouts or lost credentials. These barriers highlight the practical difficulties users face, which undermine the perceived benefits of MFA.



Conversely, motivations for adopting MFA included the desire to protect sensitive information from unauthorized access and cyber threats, as well as the peace of mind that comes with enhanced security. Biometric options such as fingerprint and facial recognition were particularly appealing to participants due to their perceived convenience and ease of use.

Recurring themes from the data emphasized the critical role of usability, security awareness, and recovery mechanisms. While users associated MFA with stronger security, the complexity of its processes often outweighed the benefits in their daily decision-making. A lack of robust account recovery options further deterred widespread adoption, as participants feared losing access to their accounts if they encountered issues with MFA.

4 DISCUSSION

The results of this study show some really important things about why young adults use or don't use Multi-Factor Authentication (MFA). Most people in the study said they know MFA is good for security, but how easy or hard it is to use really affects if they use it. Many said that if MFA is too annoying or takes too much time, they don't bother even if they know it keeps them safe. This is a big problem because hacking and cyber-attacks are getting worse, and we need strong security like MFA to stop them.One thing that stood out was how much people liked biometric MFA, like using fingerprints or face scans. They said it feels simple and fast, so they don't mind using it. But there were also a lot of bad experiences shared, like getting locked out of accounts because they forgot codes or lost their phones. These things made them not want to try MFA again. This shows that MFA systems need better ways to help people recover their accounts and easier setups to make people trust them more.

These findings match other studies. For example, Colnago et al. (2018) found people don't like MFA when it feels hard or annoying to use, even though it gives better security. Pratama and Firmansyah (2021) said most people only start using MFA after something bad

happens, like getting hacked, because they think it's too much trouble to use before that. This proves that if MFA was easier, more people, especially young adults, might start using it before something bad happens.

Biometric options are also a favorite in other research. Kävrestad et al. (2024) said young people like things like fingerprints or face recognition because they feel modern and simple, much easier than passwords or codes. Even tech-savvy IT students, according to Zaxmy (2022), avoid MFA when it's frustrating or takes too much time. Libicki et al. (2011) also explained that if people have bad experiences with MFA, like getting locked out, they stop trusting it and don't want to use it again. This is the same as what people in this study said.

This study adds to what we already know by focusing on young adults, who are not usually studied in cybersecurity research even though they use the internet a lot. While other research talks about usability and security, this study shows how even people who care about security won't use MFA if it's too hard or inconvenient. It also shows that systems need to have better recovery options and fit better into people's daily lives. If MFA becomes easier and more user-friendly, more young adults will use it, and their online accounts will be safer.

5 REFLECTIONS

Doing this study on barriers and motivations for young adults' adoption of Multi-Factor Authentication (MFA) was both challenging and rewarding. The process gave me insights into how research works and also helped me understand my own strengths and weaknesses. In this reflection, I will share what went well, what could have been better, what I learned, and what I will do differently in the future.

One thing that went well was the interview process. I used a semi-structured interview style, which worked well because it gave participants the chance to share their experiences in detail. For example, many participants talked about their frustration with MFA recovery systems, and this would not have come out with a fixed-question survey. This made me realize the value of letting people talk freely during interviews. Another thing that went well was following ethical guidelines. I made sure participants gave their consent, knew their responses would be anonymous, and understood their right to stop at any time. This helped build trust and made people comfortable sharing honest opinions. The way I analyzed the data also worked well. I read through all the responses carefully, grouped similar ideas together, and found themes like "usability," "security awareness," and "negative experiences." This made it easier to see patterns and understand what participants were saying. I was also happy with the diversity of participants. Even though the sample size was small, I included people with different levels of technical knowledge. This gave me a broader view of how young adults think about MFA.

Some things did not go as planned. Recruitment was one of the hardest parts. I thought it would be easy to find participants, but it was not. This was because I had not done something like this before and did not realize how much time and effort it would take. As a result, I mostly asked people I knew, which made the group less diverse. For example, I had fewer participants from non-technical backgrounds, which might have affected the findings. Another issue was time management. I underestimated how long it would take to analyze the data. I spent a lot of time reading and coding the interviews, which made me feel rushed when writing the report. I think using data analysis tools could have saved me time. Some of the interview questions also could have been better. A few questions were not clear enough, and participants sometimes misunderstood them. This made their answers harder to analyze. For example, one question about challenges with MFA was interpreted differently by different participants. I should have tested the questions more carefully before starting the study.

I learned a lot from this project. First, I realized how important it is to plan everything in detail, especially recruitment. If I had started candidates head hunting earlier or used better strategies, I could have included more participants from different backgrounds. Second, I learned the value of flexibility. While analyzing the data, I had to adjust my themes and methods as new patterns appeared. This taught me that research is not always straightforward, and it is okay to change plans when needed. Third, I learned the importance of ethical research. Being transparent and respectful to participants made the process smoother and more reliable. It also made me feel more confident about my work. Finally, I learned that balancing detail and efficiency is important. I enjoyed doing the analysis thoroughly, but it took too much time. Next time, I will use tools or methods to work faster without losing quality.

In my final year project, I will make some changes based on what I learned. First, I will plan the recruitment process better. I will start earlier and use more ways to find participants, like reaching out through social media or organizations. Second, I will use data analysis software to save time and analyze qualitative data faster and more accurately. Third, I will test my research tools more carefully. For example, I will pilot interview questions with a small group first to make sure they are clear and effective. Fourth, I will focus on managing my time better. I will set clear deadlines for each stage of the project and stick to them. This will help me avoid feeling rushed at the end.

6 REFERENCES

- Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's not actually that horrible": Exploring adoption of two-factor authentication at a university. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–11. HTTPS://DL.ACM.ORG/DOI/PDF/10.1145/3173574.3174030

- Pratama, A. R., & Firmansyah, F. M. (2021). Until you have something to lose! Loss aversion and two-factor authentication adoption. Applied Computing and Informatics. HTTPS://WWW.EMERALD.COM/INSIGHT/CONTENT/DOI/10.1108/ACI-12-2020-0156/FULL/HTML?UTM_SOURCE=CHATGPT.COM

- Kävrestad, J., Fernow, R., Lööf, D., & Birath, M. (2024). Multi-factor authentication adoption: A comparison between digital natives and digital immigrants in Sweden. In Human Aspects of Information Security and Assurance (pp. 323–338). Springer. HTTPS://LINK.SPRINGER.COM/CHAPTER/10.1007/978-3-031-72559-3_22?UTM_SOURCE=CHATGPT.COM

- Zaxmy, J. (2022). What are the motivations and barriers for incorporating multi-factor authentication among IT students? [Master's thesis, University of Skövde]. HTTPS://WWW.DIVA-PORTAL.ORG/SMASH/GET/DIVA2%3A1678668/FULLTEXT02.PDF?UTM_SOURCE=CHATGPT.COM

- Libicki, M. C., Balkovich, E., Jackson, B. A., Rudavsky, R., & Webb, K. W. (2011). Influences on the adoption of multifactor authentication. RAND Corporation. HTTPS://WWW.RAND.ORG/PUBS/TECHNICAL_REPORTS/TR937.HTML?UTM_SOURCE=CHATGPT.COM

- Anise, O., & Lady, K. (2017). MFA adoption: Experiences, challenges, and perceptions of multi-factor authentication. Duo Security. HTTPS://DUO.COM/BLOG/STATE-OF-THE-AUTH-EXPERIENCES-AND-PERCEPTIONS-OF-MULTI-FACTOR-AUTHENTICATION?UTM_SOURCE=CHATGPT.COM