**RESEARCH ARTICLE**

# Exploring and Adoption of Two Authentication Factors: Formation of Competence

***Abdullah Alammari*** [*]***, Marwan Albahar*** [**]

[*]**Faculty of Education, Curriculums and Teaching Department, University of Umm Al-Qura, Makkah, Saudi Arabia;** [**]**Department of Computer Science, Umm Al-Qura University, Mecca, Saudi Arabia.**

## Abstract

**Although the further protection provided by two-factor authentication (2FA) is significant, its adoption is reportedly still low. In order to better comprehend the adoption of 2FA and its barriers, A questionnaire was published at Umm Al-Qura University (UQU) to develop an in-depth understanding of the UQU cybersecurity context. We aimed at thoroughly investigating which set of factors are most likely to impact the adoption of 2FA at university. This would help transfer expertise to select effective factors, which would help to see the overall precision of 2FA regardless of the motivation or context of use. Furthermore, we present quantitative analysis using a factor analysis tool, and we have found mainly three factors, which confirm the positive impression of the technology among the 2FA users. These factors include ease of use, cognitive effort, and trustworthiness. Finally, we focused on the development of the competence of the UQU community to maximize adoption of essential cybersecurity best practices.** ***ASEAN Journal of Psychiatry, Vol. 23(4), April 2022: 1-5.***

**Keywords: Authentication Factors**

## Introduction

More recently, with the remarkable development in the computer security field single-factor authentication such as traditional login/password is considered insufficiently secure for many important security applications such as logging in to mail accounts, commercial websites online, social networks, official secure networks, and financial accounts, etc. This protection approach is easy prey for cybercriminals. Where simple, clear, and easy-to-guess passwords are discovered, such as age and names, are effortlessly found using computerized secret key collecting programs. Worse, some users reuse the password for their multiple accounts. Consequently, several logins can be compromised within seconds, and secret data like personal and financial details are under increasing threats [1]. Because of increasing evident problems in passwords, numerous individuals and organizations have transformed into 2FA to enhance the security of the existing password. 2AF adds a supplemental security layer to the authentication process that carries out it difficult for attackers to access for the users' devices or accounts over the Internet because recognizing the victim's password alone is not sufficient to exceed authentication verification [2]. 2FA system requires users to provide two types of the following authentication factors which are something knew for example password or PIN, some- thing possessed such as hardware token or a phone, and something inherent indicates to biometrics, like a fingerprint or retina pattern [3]. Numerous 2FA methods are within use. Like SMS, TOTP time-based one-time password besides the generators of hardware code such as RSA SecurID. Previous approaches require entering a single-use code from the user furthermore to their password. These codes are delivered to the user through a separate channel. 2FA provides protection against remote attackers owing to attackers are unable to hack the accounts of users using passwords alone [4]. This reasons why some large companies including Facebook, Google, and Microsoft, applied an optional two-factor authentication as part of authentication and defense operations against widespread spoofing attacks. Even though the utilize of 2FA is not novel - Google started 2FA more than five years of age and Automated Teller Machines (ATMs) have employed a card something you have and PIN code something you know for decades-2FA adoption for systems of computer is not widespread. Recent reporting indicates that less than 10% of the accounts of Google users utilize 2FA and in 2016 Dropbox informed that less than 1% of users use 2FA

[5]. This paper presents a large-scale study about adopting 2FA which included 200 faculty, staff, and students at Umm Al-Qura University (UQU). The study was conducted in February 2021, to build the necessary competence in cyber- security by promoting and disseminating good practice in cybersecurity, and to explore the behaviors and views related to the 2FA, that it will become mandatory for the employees of the university and presenting insights about what motivates adoption across different types of users faculty, staff, and students who could have various viewpoints concerning the added security significance. The results of the study have identified mainly three factors, using factor analysis. It has been interpreted concerning different items loaded under each of the three constructs. These factors are namely, Ease of Use, Trustworthiness and Cognitive efforts.

**Background**

The extensive research that highlights their usability and security weaknesses [6] is still considered as the traditional form of online user authentication method. This is due to the fact that the majority of breaches and unauthorized access events occurred as a result of default, compromised, or weak passwords. For information systems, authentication is a vital component as it prevents stored information and devices from unauthorized access and fake user identity validation. Colnago et al. have affirmed that password breaches, either because of increasingly sophisticated phishing attacks or due to database leaks, compromise the authentication credentials. This is because text-based passwords are stored in a sensitive, verifiable table that incorporates all registered users' passwords. Although these passwords are stored in salted hash, if the server responsible for authentication is compromised, the passwords of all users will be exposed. One of the ways to reduce password violations is to protect passwords with additional authentication factors. For this purpose, organizations and industrial specialists have started exploring 2FA in order to reinforce current password security [7]. 2FA is an upgraded authentication mechanism that protects users from losing their passwords either because of phishing or password database leakage. Attackers who have gained access to the victim's password need to run through an additional authentication channel that will generate a one-time token. The on-time token helps in ensuring that the user is authentic. 2FA, because of its robustness, portability, and simplicity, has received major attention [8, 9]. 2FA systems are adopted into the contexts in which users put different values on the security of their accounts, which becomes more important from a practical point of view.

**Literature Review**

Numerous studies show the importance of implementing two-factor authentication to increase security. One such study was a survey of online banking users [10]. Demonstrated that two-factor authentication is nearly as usable as single-factor authentication, indicating that two-factor authentication is considered more secure. Besides, the research indicated how to smoothly switch from a single-factor system to a two-factor system without making any alterations, patches, or updates to the old system. The work most directly associated with our work is the Duo adoption study in the environment of the university. Colnago et al. conducted two large-scale surveys for faculty and students at Carnegie Mellon University (CMU) about the Duo 2FA system deployed at the university to explore user behaviors, opinions about adoption, and sentiments of users towards 2FA before and after Duo became compulsory for the employees of the university. The results showed that although most users found Duo irritating, they found it simple to use. The experience of using 2FA and CMU Duo often produced affirmative perceptions where the participants recognized the security benefits of utilizing 2FA. Also, they identified some recurring problems with Duo that resulted in more negative perceptions such as not having the phone nearby and less secure practices that the 2FA could help identify and mitigate such as credential sharing. Finally, they provided recommendations for institutions and developers that are considering 2FA adoption. A similar study on Duo 2FA was conducted at Brigham Young University (BYU) by Jonathan Dutson et al. with 4,275 staff, students, and faculty after the BYU university adopted it. The findings were diverse. Most of the participants sensed safety when utilizing the Duo. They also sensed it was simple to use. Numerous participants were disappointed that they were obligated to use the system. About one-half of the participants preferred not to use the Duo. At the same university, Ken Reese et al. conducted an IRB-approved study about 2FA for two weeks with 72 participants to compare the usability of common 2FA methods, which are U2F security keys, SMS, push, TOTP, and pre-generated codes, by making the participants log in to a site that simulates banking almost every day and completing a specific task banking. Participants generally gave high scores for the methods studied, and many expressed interests in utilizing 2FA to provide further security concerning their sensitive online accounts. In the same context, authors in presented an in-depth study with 21

individuals on the usability of 2FA in online banking in the United Kingdom as part of the login to the banking website, smartphone application log in, and payment preparation. Participants utilized a variation of the two-factor systems, including hardware code generators, card readers, phone calls, SMS, and smartphone applications, which create single-use codes. The results showed that the participants did not like the hardware code generators, as they faced a wide range of usability problems. In this circumstance, some individuals changed banks because they had difficulty utilizing tokens. In contrast, De Cristofaro et al. surveyed the Mechanical Turk participants and found that SMS or e-mails were the second most common factor for financial or personal websites and that device tokens were the most common at work.

**Context**

The demographics of the 200 study participants are reported in Figure 1. The survey results indicated that around 83% of the participants were male, while the remaining 17% were female. Moreover, the majority of the respondents revealed that their age lies between 25 to 34 years. 15% of the respondents were aged between 35 to 44 years range, while only 5% and 3% are found to be between 45 to 54 years and 18 to 24 years, respectively. Similarly, when asked about the educational background, the findings indicated that most participants had an undergrad degree 54%, while 21% had completed college. Around 9% were in high school, and only 6% had a PhD. On the other hand, the respondents also indicated information about their familiarity with computer science and computer security. The findings from the same suggest that 80% of the respondents were familiar with computer science, while only 51% knew about computer security.

**Methodology**

Based on the aim of the study, the methodology used for this research is quantitative. Both descriptive and correlational designs have been used. Under the quantitative research approach, the instrument chosen for the collection of the data is a questionnaire survey. The survey mainly comprises open-ended and closed-ended questions. The survey had been distributed among the participants using the online survey distribution among different students and teachers' social media groups. The sample size of the study is 200 participants, which mainly includes faculty, staff, and students at the university. The collected information is then analyzed using frequency analysis and factor analysis.

**Figure 1: Demographic analysis**

| | |
|---|---|
| **Gender** | |
| Male | 83% |
| Female | 17% |
| **Age** | |
| 18–24 | 3% |
| 25–34 | 77% |
| 35–44 | 15% |
| 45–54 | 5% |
| 55–65 | 0% |
| 65+ | |
| **Education** | |
| Less than high school | 9% |
| Some college | 21% |
| Undergrad | 54% |
| Some grad school | 5% |
| Master's degree | 5% |
| PhD | 6% |
| **Familiar with Computer Science?** | |
| Yes | 80% |
| No | 20% |
| **Familiar with Computer Security?** | |
| Yes | 51% |
| No | 49% |

**Results**

With the help of factor analysis, the quantitative analysis of collected information has mainly identified three main factors. Table 1 indicates the factor loading determined by the statistical tool. It can be seen that there are mainly three factors' groups, which indicate the users' and non-users' perceptions of the two-factor authentication. The following table indicates the value of the loading extracted for each of the 15 items of the survey under the three main variables. It is important to note that the higher the absolute value of the loading, the more the item contributes to a specific factor or variable. In the current case, the researcher has mainly suppressed the loading to less than 0.4. So, values that have higher than 0.4 loadings are factored together within the three variables. Factor 1 is labelled "Ease of Use." Under this factor, seven items have been loaded. It has been found that the items, including convenient, quick, enjoyable, reused, helpful, user-friendly, and no-enjoy, are loaded under the factor of ease of use. However, one of the items

no enjoy reflects a negative loading, implying its negative relationship with the main variable. The second derived factor is labelled "cognitive perceptions of 2FA." The items loaded under this factor need instruction, concentration, stress, relaxation, and frustration. It can be seen that all these items are positively related to the main variable factor. The third derived factor is called "trustworthiness." The results indicate that only two items are loaded under this variable. It has been found that the respondents trusted the 2FA and found it very secure. The loading values of above 0.8 confirm the grouping of these items under the third factor. The commonalities of each item reflect the amount of variance explained by each item within the extracted factors. The table, as mentioned earlier, reveals that all of the items explain more than 50% of the variation, except for three items concentrate, match, and easy.

**Table 1. Table Factor Analysis**

| | **Loadings** | | |
|---|---|---|---|
| | **Factor 1: Ease of Use** | **Factor 2: Congitive Efforts** | **Factor 3: Trust** |
| Convenient | 0.91 | 0.05 | -0.02 |
| Quick | 0.84 | -0.12 | -0.15 |
| Enjoy | 0.77 | 0.15 | 0.12 |
| Reuse | 0.75 | 0.04 | 0.19 |
| Helpful | 0.72 | 0.02 | 0.17 |
| No Enjoy | -0.52 | 0.22 | -0.16 |
| User Friendly | 0.42 | -0.19 | 0.37 |
| Need Instructions | 0.15 | 0.8 | -0.12 |
| Concentrate | 0.03 | 0.64 | 0.14 |
| Stressful | -0.41 | 0.51 | 0.01 |
| Match | -0.3 | 0.42 | -0.15 |
| Frustating | -0.47 | 0.47 | 0 |
| Trust | 0.08 | -0.04 | 0.8 |
| Secure | -0.02 | 0.03 | 0.82 |
| Easy | 0.27 | -0.28 | 0.31 |
| Eigenvalues | 7.52 | 1.78 | 1.03 |
| % of Variance | 32 | 15 | 14 |
| Total Variance | | 61% | |

## Conclusion

The study's primary goal was to investigate the factors that influence the perception of 2FA users at the university in terms of their usability and overall implementation, as well as to develop the necessary cyber security competence by promoting best practices in cyber security. A quantitative survey of 200 university students was conducted, and factor analysis was used to determine the study's main variables. In addition, we highlighted three main factors, under which 14 out of the 15 items of the survey were loaded accordingly. Based on the findings and the positive attitude of the participants toward the 2FA, it is recommended that the university contribute to improving the excellence of educators and academics in the UQU community as well as increase the competitiveness of educational programs in cyber security by introducing new courses that align the university context with best practices and implementing them across the university.

## References

1. Jessica Colnago et al. "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. 2018; 1–11.

2. Joseph Bonneau, Soren Preibusch. "He password thicket: Technical and market failures in human authentication on the web". In: In Proc. 2010.
3. Eric Grosse, Mayank Upadhyay. "Authentication at Scale". In: IEEE Security & Privacy. 2013; 11(1): 15–22.
4. Bruce Schneier. "Two-factor authentication: Too little, too late". In: Communications of the ACM 2005; 48: 4.
5. Thanasis Petsas, Giorgos Tsirantonakis, Sotiris Ioannidis, Elias Athanasopoulos. "Two-factor authentication: Is the world ready?: quantifying 2FA adoption. In: Proceedings of the Eighth European Workshop on System Security. 2015; 4:1-7.
6. Maha MA, Pam Mayhew. "Security and usability of authenticating process of online banking: User experience study". In: 2014 Inter- national Carnahan Conference on Security Technology (ICCST). 2014; 1–6.
7. Ziqing Mao, Dinei Florencio, Cormac Herley. "Painless migration from passwords to two factor authentication". In: 2011 IEEE International Workshop on Information Forensics and Security. 2011; 1–6.
8. Jonathan Dutson, Danny Allen, Dennis Eggett, Kent Seamons. "Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication". In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW). 2019; 119–128.
9. Kat Krol. "They brought in the horrible key ring thing!" Analyzing the Usability of Two-Factor Authentication in UK Online Banking". In: arXiv preprint arXiv:1501.04434. 2015.
10. Emiliano DC, Honglu Du, Julien Freudiger, Greg Norcie et al. "A comparative usability study of two-factor authentication". In: arXiv preprint arXiv: 1309.5344 2013.

**Corresponding Author:** ***Abdullah Alammari, Faculty of Education, Curriculums and Teaching Department, University of Umm Al-Qura, Makkah, Saudi Arabia.***

***E-mail: bbcsdpub@gmail.com***

**Received:** 24 March 2022**,** Manuscript No. AJOPY-22-55144**; Editor assigned:** 28 March 2022**,** PreQC No. AJOPY-22-55144 (PQ)**; Reviewed:** 14 April 2022**,** QC No: AJOPY-22-55144**; Revised:** 21 April 2022**,** Manuscript No. AJOPY-22-55144 (R)**; Published:** 28 April 2022**,** DOI: 10.54615/2231-7805.47335.