Analysis of user Awareness for Saudi State Mobile Applications

Fahad Alturise, Waleed Albattah

Abstract*: *In this article, we analyze the perception of Saudi state application users about password selection from real-world data. A total of 1,082 participants provided information about their behavior on state applications. The study extracts useful information related to the users' weak practices. The findings include useful information representing thousands of minds and individual behaviors in using state applications. As a contribution to the area, it is found that the state applications were developed properly regarding security practices. However, users still represent the weakest party, and they are not aware of the proper practices they should follow. Thus, extensive effort is required to be spent on user education. On the other hand, the diversity of state applications may represent an extra effort to users in the way that they have separate passwords for each application, which makes a unified login portal for all the state applications the appropriate solution.

Keywords*: *State Applications, user awareness, security, password, username

I. INTRODUCTION

In this paper, an awareness analysis is designed to address the challenges that Saudi Arabian people currently face while accessing and using state applications and also to analyze the strength of usernames and passwords for mobile phones. The analysis looks at different scholarly studies on security analysis for Saudi Arabia mobile applications. The resultant data majorly revolves at investigated theoretical analysis; that is, users' awareness in identifying and understanding the official applications on security significance, more so through password and username privacy when using state mobile applications in Saudi Arabia. The general objective of the study is to identify a literature gap in the topic. The world is gradually navigating to a technological era where business, education, meetings, banking, and other credential activities are done online [1]. Over the last decade, mobile applications have rapidly expanded, owing to the heightened use of smartphones. As stated by [2], in the modern world most operations can be done at the convenience of their clients using different online platforms in mobile applications. Unlike a century ago, today, people do not have to queue for a whole day for services that can be done over the Internet. According to [3], technology has played a significant role in providing the infrastructure needed to host, develop, and design mobile applications to be interactive and user-friendly. A growing number of these online applications are the result of the larger number of people who have access to mobile devices such as laptops and mobile phones [4]. Author in[5] stated that the development and emergence of such state mobile applications have revolutionized how people access state services and information. However, according to [6], security concerns such as cybercrimes affect users and may cause devastating effects to them if not well mitigated. In most applications, users must log in using their passwords and usernames to ensure authentication. This verification process is designed to ensure that only the owners can access the application [7]. Leaking of login details to a third party may give them the opportunity to access all the information in the application [8]. As [9] suggest, users who receive password guidelines and are aware of the importance of developing strong passwords create strong authentication codes that are less likely to be hacked. Despite the importance, there is little awareness by the public about the significance of using passwords and usernames as security measures to protect one's data. According to [10] when people use weak passwords or leak their access information to third parties, there is a danger of it leading to cybercrimes. In conjunction, [11] claimed that many people who rely on online transactions had fallen victim to application cybercrimes due to leaking passwords or using relatively weak access passwords. According to recent research, most people are less concerned today with storing their data in systems and whether they might be accessible to unauthorized persons [12]. There is a growing number of fraudsters that hijack individual information secretly and use it for malicious gains. According to [13], users should use strong passwords and unique usernames that cannot be guessed; for instance, using names or telephone numbers should be avoided. Back-up storage space should be maintained so that data can be accessed even if it is lost. Mobile applications are also prone to security threats, especially where fraudsters guess the username and password multiple times. In [14] suggested that the human factor is the weakest security link, as most end-users are not efficient at securing their authentication codes. Application users should continually change their passwords, making it harder for a third party to guess them. A lack of awareness in safeguarding personal usernames and passwords can increase the number of cybercrimes. In a study conducted by [15] on smartphone users' security behavior, they found that most app users have confidence in their data being in the application. According to the research, most application subscribers will provide personal information and other credentials when asked without giving it a second thought. In another study, [16] reveals that most Saudi Arabian people trust state mobile applications. The application enforces the responsibility of creating a strong password and unique username, and thus the user has no personal responsibility to protect the data [15].

Revised Manuscript Received on November 20, 2020.
***** Correspondence Author
Fahad Alturise[1], Computer Department, College of Sciences and Arts, Qassim University, Al-Rass, Saudi Arabia**.** Email: falturise@qu.edu.sa
Waleed Albattah[2], Department of Information Technology, College of Computer, Qassim University,Buraydah 51452, Saudi Arabia; Email:w.albattah@qu.edu.sa

In recent research, results reveal that, despite mobile application end users having the required knowledge, they lack appropriate behavior, such as the adoption of relevant security practices [17]. Mobile security is an integral part of today's information and technology world. According to research by [18] mobile security is concerned with botnets, spyware, malicious links, and malicious applications. In Saudi Arabia, ransomware is termed as the most common threat to cybersecurity, as stated by [19]. Fraudsters and hackers use ransomware to track someone's account created in various mobile applications, and hence access personal information. After gaining access, they can edit, alter, or delete the information with the intention of harming the user. In some cases involving sensitive data, the data can be used against the users' wishes, such as tarnishing their good reputation. Despite securing login accounts with usernames and passwords, [20] states that people should be cautious about the data they share in public and choose mobile applications they can trust with personal information. As a solution, [21] suggest that awareness of ransomware threats and updating security applications could play a significant role in dealing with the situation. Personalized security indicators such as the use of passwords and usernames can also help in detecting Phishing in mobile applications [22]. According to [23], despite the rise in cybercrimes in Saudi Arabia, there is no specific approach to increasing cybersecurity awareness in the region. In addition, the study reveals that, despite the growth in IT experts, the awareness of mobile cybercrimes and the threats associated with them is minimal. Furthermore, the role of government and organizations in ensuring information safety across the Internet and mobile applications is small. There are relatively few federal laws and regulations that seek to address data privacy and security standards, and, as a result, cybercrimes have escalated [21]. It would, therefore, be essential to investigate the identity and understand the awareness of users of official applications in Saudi Arabia about the importance of security, especially through the username and password and privacy when they use state mobile applications, which this paper aims to highlight and address.

II. METHODOLOGY

This study aims to investigate awareness levels regarding username and password used for formal Saudi mobile applications based on research questions in a survey. According to previous studies, questionnaire-based survey studies on information privacy are the most popular method of data gathering. Some studies have included open-ended questions [24] and selective interviews [25] to obtain additional data. A few questionnaires have been paper-based while most were web-based [26-29]. For this study, it was decided to use a web-based approach because many respondents will be able to manage an online questionnaire. Also, our target demographic are people who are eligible to use technology. The questionnaire was developed based on closed-ended questions using some available questionnaires as the development basis [30-32]. The developed questionnaire has been reviewed by professional colleagues in the computer field for confirmation of effectiveness. Furthermore, a statistical consultant and English and Arabic language expert also reviewed it to ensure clarity, proper language structure, and elimination of language ambiguities. A pilot test was performed on seven participants resulting in minor modifications. The participants were presented with 23 closed-ended questions and three demographic questions. All participants were guided to select one or more answer(s) based on the type of the question within a limited frame of options. With a Saudi Arabian population of approximately 30 million, the confidence level of 95% and a margin of error of 5% were found to be appropriate. Thus, a minimum of 385 responses would be required for the survey to be valid.

III. RESULTS AND DISCUSSION

Data are collected by sharing the questionnaire link with people who live in Saudi Arabia. All the participants were provided with Arabic language information sheets and the questionnaire. This survey link was active for two weeks. In this survey, a total of 1,091 questionnaires were returned. After filtering, the researcher included 1,082 (99.2%) complete responses, which were later used for analysis.

A. Demographic characteristics

Out of the 1,082 respondents in terms of gender, 738 (68.2%) were male and 344 (31.8%) were female. Regarding participant qualifications, 130 (12%) had a high school education or less, most respondents had a diploma or bachelor's degree, comprising734 (67.8%), and 218 (20.1%) were in postgraduate degrees. The respondents comprised 129 (11.9%) between 18 and 24 years old, 262 (24.2%) were between 25 and 34 years old, 379 (35%) were between 35 and 44 years old, 228 (21.1%) were between 45 and 54 years old, and 84 (7.8%) were over 55 years old. 218 (20.1%) of participants were specialists in a computer field; however, most participants, 864 (79.9%), were not involved in this field. Table I presents the summary of the demographic profile of the respondents.

B. Information about state applications

The results revealed that Absher was the dominant state application with a response rate of 95.2% (1030). Tawakkalna, one of the newest among the applications, had the second-highest percentage of users at 65.9% (713). Mawid had a response rate of 51.2% (554), 34.9% (378) use KollonaAmn Fifty-seven-point seven percent (624) of participants use identity & authentication management. Najiz had a response rate of 18.6% (201), and finally, about 6.5% (67) of participants use other state applications. Table II represents the findings and rankings of the state applications used by the survey participants. Analysis recorded in Fig. 1 shows that 46.4%)of the people have used state applications for more than four years, (19.6%) have used them for between three and four years, (19.7%) have used them for between 1 and 2 years, (9.4%) have used them for less than a year, and just (4.9%) have used them only over the period of the COVID-19 crisis.

Table- I: Demographic Profile of the Respondents

Variables	Answers	Responses	
		Frequency	Percent
Age	18-24	129	11.9%
	25-34	262	24.2%
	35-44	379	35%
	45-55	228	21.1%
	More than 55	84	7.8%
Gender	Male	738	68.2%
	Female	344	31.8%
Education levels	High School or less	130	12%
	Diploma or Bachelor	734	67.8%
	Postgraduate	218	20.1%
Field of study	Specialist in Computer fields	218	20.1%
	Different field of study	864	79.9%

Table-II: Chosen state applications by the users in the sample

Social Media	Frequency	Percent
Absher	1030	95.2%
Tawakkalna	713	65.9%
Mawid	554	51.2%
KollonaAmn	378	34.9%
Najiz	201	18.6%
Identity & Authentication Management	624	57.7
Other	67	6.5%

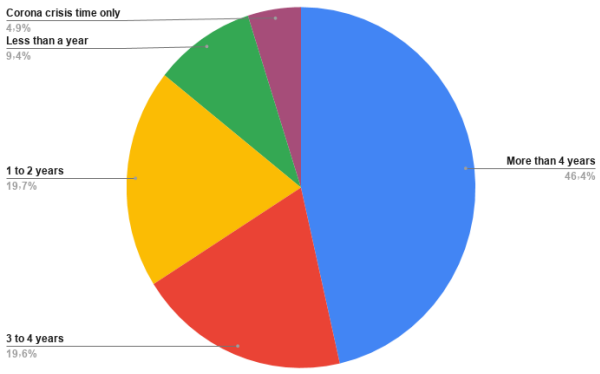

Fig. 1.How long have you been using state applications?

Table III illustrates that 97.3% of users are on smartphones, 44.8% use a laptop, 10.3% use a tablet and only 24.3% are using a desktop for social media.

Table- III: What methods do you use to access state applications.

Device Type	Frequency	Percent
Smartphone	1052	97.3%
Laptop	484	44.8%
Tablet	111	10.3%
Desktop	263	24.3%

Fig. 2 shows the frequency of use of state applications by participants. About 40.2% of participants never use state applications, or they only check their state applications twice a month or less. About 24.9% of participants check state applications more than once a week. About 22.9% of participants use their state applications once a week at most. Finally, 12% of participants use and check state applications at least once a day.

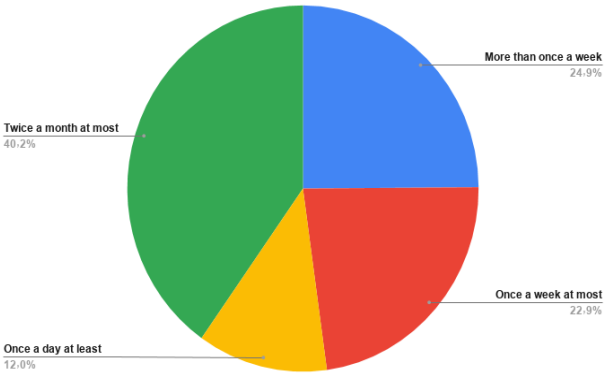

Fig. 2.The frequency of use of state applications by participants.

Fig. 3 illustrates that 86.7% depend on themselves to register for their state application account, whereas 0.9% ask a technical person, 0.6% rely on a service office, and 11.8% rely on friends or family members.

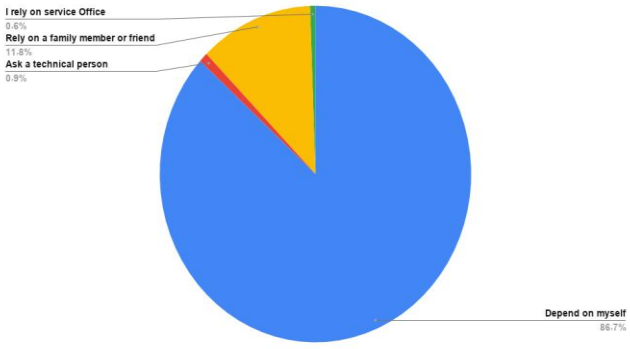

Fig. 3.To register for your account (s) on state applications.

Fig. 4 shows that only 25.2% of participants who get registration help from a technical person change their password after registration, while 74.8% do not.

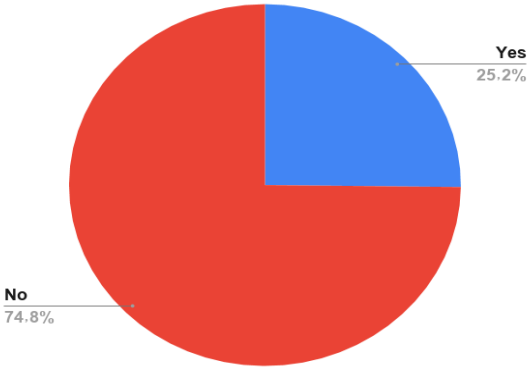

Fig. 4.Change the password after completing the account registration by technical person

Fig. 5 shows that 98.2% using their email address and mobile number to create their account while 1.8% do not.

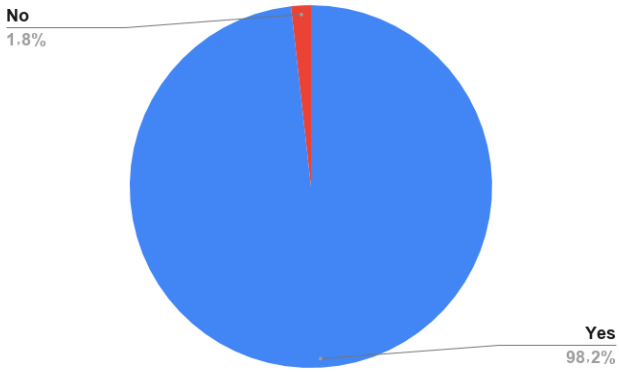

Fig. 5.Using participant's email and official mobile number to create your account.

Fig. 6 shows that 17.7% change their password periodically, and 82.3% do not.

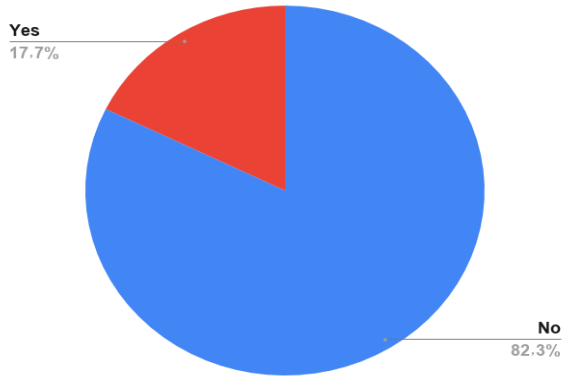

Fig. 6.Periodically change the password for accounts in state applications.

Regarding the frequency of changing the password for state applications, Fig. 7 shows that 12.6% of participants who change their passwords periodically change it monthly, 30.4% change it every three months, 30.4% change it every six months, and 26.7% change it annually.

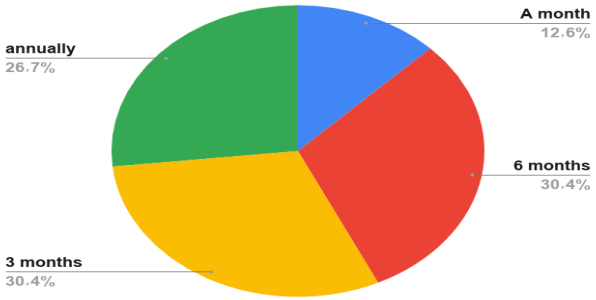

Fig. 7.The frequency that passwords of state applications are changed.

Fig. 8 shows where new users read the terms and conditions or ignore them. It can be clearly seen that 42.4% agree that when they log in as a new user, they ignore terms and conditions and do not even read them. Only 18.2% of people read the full details when they login to a state application, while 39.4% of participants sometimes read the terms and conditions.

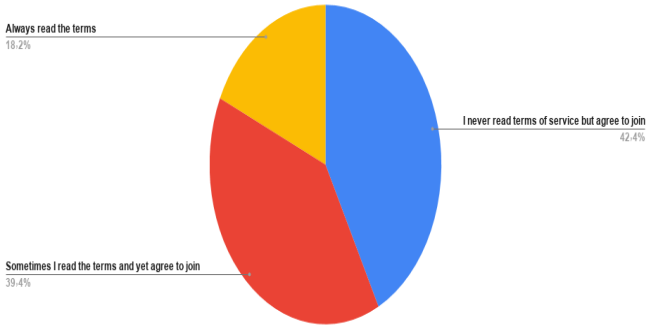

Fig. 8.When you join a state application, what is your best description for being a user?

However, Fig. 9 shows that if anyone discloses their user information, about 57.8% of them think it has a high impact, 27.7% see it as somewhat difficult, 11.5% see it as not very effective, and 3.1% ignore it.

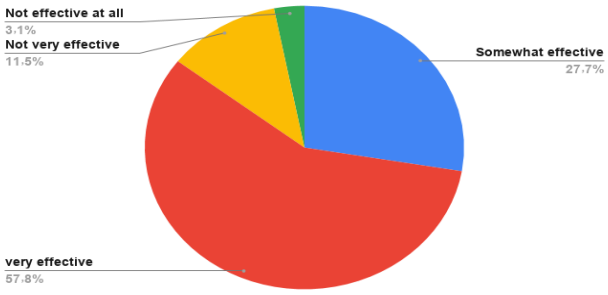

Fig. 9.The effectiveness of disclosure of user information on a state application.

Fig. 10 shows that 98.1% of users agree that their privacy has not been violated before, whereas only 1.9% think that a violation has occurred.

Fig. 11 shows that where a violation has occurred, four participants contacted a government official, three changed their password directly, six discussed it with friends, two contacted a family member, and six did not react and ignored it.

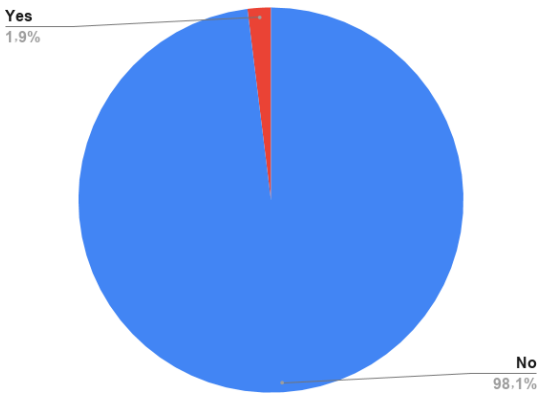

Fig. 10. Has your privacy been violated on state application before?

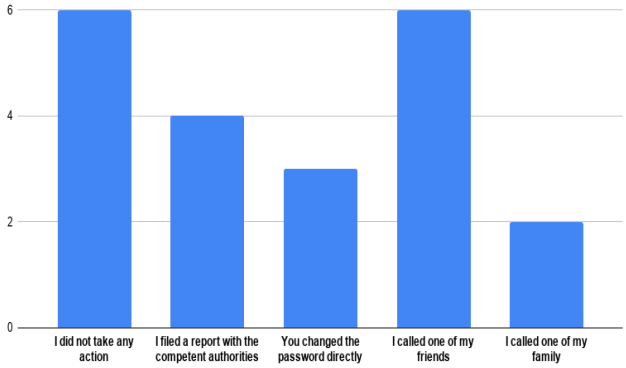

Fig. 11. How did you react to a violation?

As shown in Table IV, most users, 85.6%, use numbers to create their password. The second-highest choice is uppercase letters, with 81.8% using those to create their password. 76.2% of participants use lowercase letters, while 40.7% of users choose symbols to create their password.

Table- 4: Construction of the state application password.

Password Consist	Frequency	Percent
Uppercase letters	885	81.8%
Lowercase letters	825	76.2%
Symbols	440	40.7%
Numbers	926	85.6%

Fig. 13 shows that 52% of participants repeat some of the characters in the username and password, while the rest do not. According to participants, most users have a password of between 8 and 12 characters.

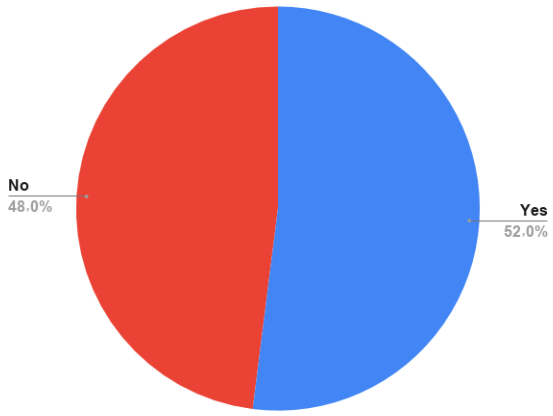

Fig. 12. Do you repeat the use of some characters in the username in the password?

Table V shows that 30.9% of users use letters next to each other on the keyboard to create their password, 28.3% of participants use consecutive numbers, 28.2% use their mobile number or the mobile number of someone close to them, or some part of it, 26.1% of participants use their national ID number, or some part of it, while 13.6% of users use the date or year of their birth as a password or some part of it.

Fig. 14 shows that just 6.2% of users use famous or common words in their password.

Fig. 15 shows the most commonly used words used to create a password. 31.3% of users use their family or tribe name, the second most common word used is a city name with 23.9% doing that. 23.9% of users use a famous character name as a password, or part of it, 10.4% users use a TV program name to create their password, 3% use a website name, 1.5% use a famous player's name, and the same percentage use some other special name.

Table- V: The construction of the state application password.

Password consists of	Frequency	Percent
Letters next to each other on keyboard	334	30.9%
Consecutive numbers	306	28.3%
Mobile number or the mobile number of someone close to you, or part of it	305	28.2%
National ID number, or part of it	282	26.1%
Date or year of birth	147	13.6%
Other	171	17%

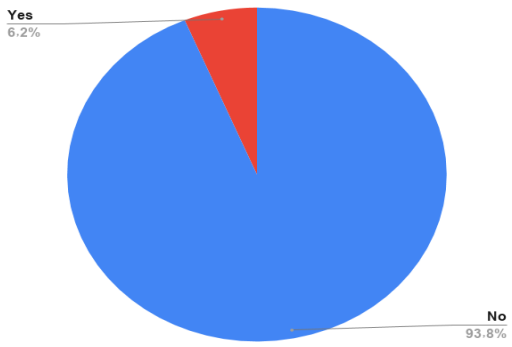

Fig. 13. Using common or famous words in the password

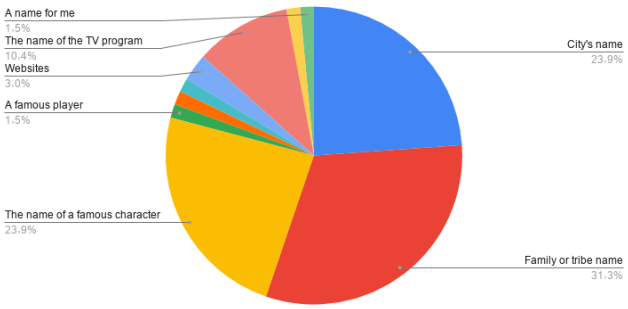

Fig. 14. The common or famous word used in the password.

Figure 16 shows that 73.7% of users use the same password for more than one application.

Fig. 17 shows that 54.2% of users think their password used for state applications is strong, 44.7% think it is medium, and just 1.1% think it is weak.

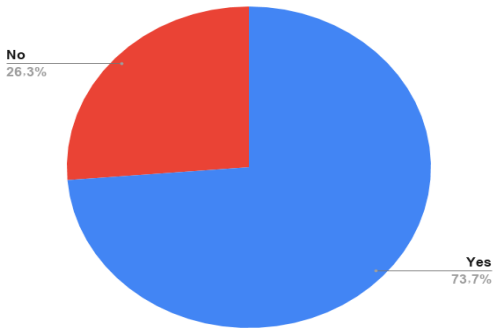

Fig. 15. Do you repeatedly use the same password for more than one application?

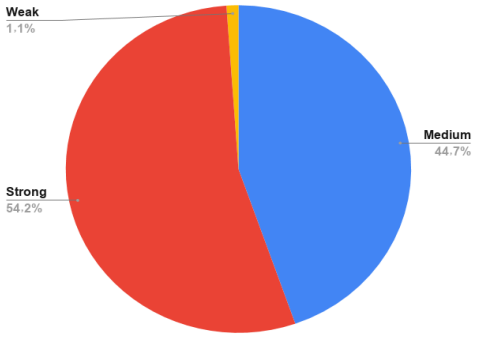

Fig. 16. User opinion about the password they use to log in to state applications.

Table VI shows the reasons preventing users from using a stronger password. Fifty percent of users do not use a strong password because they find simpler passwords are easier to remember. 33.3% of participants get familiar with their current password, 8.3% log in using a two-step verification method, so think they do not need using a strong one, and finally, 8.3% of users do not care about their password.

Table- VI: Reason preventing users from using a stronger password

Reason	Percent
Familiar with current password	33.3%
Login by two-step verification method	8.3%
Ease of remembering	50%
Don't care	8.3%
I don't know how to make my password stronger	0%

From these statistics, we can derive useful discussions. It seems from the analysis that most of the users have a good awareness level about using web applications in general. However, only small percentages are aware of how to protect their privacy. One of the biggest weakness's users have is that about 75% of them do not change their application passwords after they have received assistance from someone else, which makes their passwords very vulnerable. Another concern is that most users do not change their password regularly. This weakness may be related to the fact that these applications do not require users to change their password after a specific period of time. Moreover, about 18% of participants pay attention to the terms and conditions of use provided by the state application during the sign-up process, which makes them miss some valuable information. A positive process that this kind of state application uses is the two-factor authentication, where the user is required to insert a temporary pin sent to a registered mobile number along with doing the normal user authentication, i.e., username and password. This step promotes secure logins. Consequently, only very few users have reported some violation of their privacy. Although developers always use the best security practices during application development, users themselves still represent the greatest challenge to security. Many users are still not aware of the consequences of using weak passwords. About 52% of participants repeat some of the characters in their username and password, 30.9% of users use consecutive letters, and 28% use consecutive numbers to create their password. To summarize, it is found that the state applications were developed properly regarding login authentication. However, users still represent the weakest link. Users are not aware of the correct security practices to follow. On the other hand, the diversity of state applications may represent an extra effort to the users in the way they have separate passwords for each application. One solution for this concern is to have a unified portal for all of the state applications. Hopefully, this could help users to choose proper passwords and pay more attention to the instructions which accompany the applications.

IV. CONCLUSION AND RECOMMENDATIONS

In this article, usernames and passwords in Saudi state applications were analyzed to understand the human perception of password security. The results shed valuable light on the way users choose passwords. Unfortunately, most users are not aware of the fact that passwords can be vulnerable to others. We believe that this paper will assist with the weak practices of using passwords, which make them easily predictable. We believe that an in-depth analysis is required and will be performed in future to seek more possible solutions that can overcome the weakness of user awareness. Based on the results and analysis, as well as our earlier works (Khan &Albattah, 2017; Albattah, 2018) on the analysis of username and password selection, it is strongly recommended that in addition to the standard restrictions given by state application providers on password choice, the following table VII of behaviors are avoided by users during their selection of password.

Table- VII: Common password behaviors

	Common password behavior	Examples
1	Familiar words society	Covid-19, McDonalds
2	Numbers and/or symbols not included	ajsixvr, wkifht
3	Ascending or descending order of numbers	34567, 987654
4	Years and birthdays	1975, 11-10-1995
5	Using "_" and "-"	Dr_Stephens, Prof-Melton
6	Family names	Haagen, Albattah
7	Individual names	Waleed, John, David
8	Feelings	Happyguy, smartman

REFERENCES

1. Clements, J.A. and Boyle, R., 2018. Compulsive technology use: Compulsive use of mobile applications. Computers in Human behavior, 87, pp.34-48.
2. Goth, G. (2012). Mobile security issues come to the forefront. IEEE Internet Computing, 16(3), 7-9.
3. Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. Journal of medical systems, 39(1), 181.
4. De Reuver, M., Nikou, S. and Bouwman, H., 2016. Domestication of smartphones and mobile applications: A quantitative mixed-method study. Mobile Media & Communication, 4(3), pp.347-370.
5. Jain, A. K., &Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. IT Professional, 14(5), 28-33.
6. Holt, T.J., 2016. Situating 1 the problem of cybercrime in a multidisciplinary context. Cybercrime Through an Interdisciplinary Lens, 26, p.1.
7. Geneiatakis, D., Fovino, I.N., Kounelis, I. and Stirparo, P., 2015. A Permission verification approach for android mobile applications. Computers & Security, 49, pp.192-205.
8. Adhikari, R., Richards, D. and Scott, K., 2014. Security and privacy issues related to the use of mobile health apps. ACIS.
9. Yıldırım, M. and Mackie, I., 2019. Encouraging users to improve password security and memorability. International Journal of Information Security, 18(6), pp.741-759.
10. Brar, H.S. and Kumar, G., 2018. Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications, 2018.
11. Nkosi, M. T., &Mekuria, F. (2010, November). Cloud computing for enhanced mobile health applications. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 629-633). IEEE.
12. Goel, A.K., Rose, A., Gaur, J. and Bhushan, B., 2019, July. Attacks, Countermeasures and Security Paradigms in IoT. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 875-880). IEEE.
13. Ruggiero P. and Jon Foote, (2011), Cyber Threats to Mobile, government organization Carnegie Mellon University-US.
14. Hoonakker, P., Bornoe, N. and Carayon, P., 2009, October. Password authentication from a human factors perspective: Results of a survey among end-users. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 53, No. 6, pp. 459-463). Sage CA: Los Angeles, CA: SAGE Publications.
15. Bagga, T., Sodhi, J., Shukla, B. and Qazi, M., 2017. Smartphone Security Behaviour of the Indian Smartphone User. Man In India, 97(24), pp.333-344.
16. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., &Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications, 14(5), 85-91.
17. Aljedaani, B., Ahmad, A., Zahedi, M. and Babar, M.A., 2020. Security Awareness of End-Users of Mobile Health Applications: An Empirical Study. arXiv preprint arXiv:2008.13009.
18. Paul, P. and Aithal, P.S., 2019, October. Mobile Applications Security: An Overview and Current Trend. In Proceedings of National Conference on Research in Higher Education, Learning and Administration (Vol. 1, No. 1, pp. 112-121).
19. Roberta Cozza, (2014), Mobile Communications Devices by Open Operating System, Worldwide, Forecast.
20. Ngai, E. W., & Gunasekaran, A. (2007). A review of mobile commerce research and applications. Decision support systems, 43(1), 3-15.
21. Mitrea, T., Vasile, V. and Borda, M., 2019, June. Mobile Applications-(in) Security Overview. In International conference KNOWLEDGE-BASED ORGANIZATION (Vol. 25, No. 3, pp. 42-45). Sciendo.
22. Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K. and Capkun, S., 2015. Personalized security indicators to detect application phishing attacks in mobile platforms. arXiv preprint arXiv:1502.06824.
23. Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M., 2016, December. A survey of cyber-security awareness in Saudi Arabia. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 154-158). IEEE.
24. Aldhafferi, N., Watson, C., & Sajeev, A. S. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices arXiv preprint arXiv:1305.2770.
25. O'Brien, D., & Torres, A. M. (2012). Social networking and online privacy: Facebook users' perceptions. Irish Journal of Management.
26. Aljohani, M., Nisbet, A., &Blincoe, K. (2016). A survey of social media users' privacy settings & information disclosure.
27. Ibrahim, S., & Tan, Q. (2019). A Sudy on Information Privacy Issue on Social Networks. ISeCure, 11(3).
28. Bhandari, R. S., & Bansal, S. (2019). Privacy Concerns with Social Networking Sites: An Empirical Investigation of Users in National Capital Region (NCR), India. South Asian Journal of Management, 26(3), 68-87.
29. Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., &Kusev, P. (2018). Security and privacy in online social networking : Risk perceptins and precautionary behavior. Computers in Human Behavior, 78, 283-297.
30. Isler, D., Küpçü, A., & Coskun, A. (2018). User Study on Single Password Authentication. IACR Cryptol. ePrint Arch., 2018, 975.
31. Yıldırım, M. and Mackie, I., 2019. Encouraging users to improve password security and memorability. International Journal of Information Security, 18(6), pp.741-759.
32. Hoonakker, P., Bornoe, N. and Carayon, P., 2009, October. Password authentication from a human factors perspective: Results of a survey among end-users. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 53, No. 6, pp. 459-463). Sage CA: Los Angeles, CA: SAGE Publications.

AUTHORS PROFILE

Fahad Alturise is currently working as an Assistant Professor in the Computer Department, College of Science and Arts in ArRass, Qassim University, Saudi Arabia. He has an experience of twelve years in the field of teaching and research. He holds a PhD in Information Technology from Flinders University. His primary research interests include e-learning, e-services, e-government, IOT, ICT adaption, IT security and Software Engineering. He has published 12 papers in international journals/conference proceedings He was a member of the Australian Computer Society (ACS) for 4 years.
Email: falturise@qu.edu.sa

Waleed Albattah has received his Ph.D. from Kent State University, Ohio, USA. Dr. Albattah is a faculty member at Information Technology Department, Qassim University, Saudi Arabia. His research interests are software engineering, software design and agile software development, and software quality. Recently, he has been working on Big data and cloud computing security as well as machine learning projects. He has been granted several project grants from different organizations. He is the former dean of College of Computer at Qassim University, and he is a member of ACM Society SIGSOFT. Email: w.albattah@qu.edu.sa