EAI Endorsed Transactions
on Creative Technologies

Research Article **EAI.EU**

Is My Password Strong Enough?: A Study on User Perception in The Developing World

Tangila Islam Tanni[1], Tanjin Taharat[2], Muhammad Shakil Parvez[3], Sarker T. Ahmed Rumee[3,4,*] and Moinul Islam Zaber[3,4,5]

[1]School of Science and Engineering, University of Liberal Arts Bangladesh, Dhaka-1209, Bangladesh
[2]Therap (BD) Limited, Dhaka-1213, Bangladesh
[3]Department of Computer Science and Engineering, University of Dhaka, Dhaka-1000, Bangladesh
[4]The Data and Design Lab, Dhaka, Bangladesh
[5]United Nations University, E-government Operating Unit (UNU-EGOV), Guimarães, Portugal

Abstract

INTRODUCTION: The first line of defense in the cyber world is strong and difficult to predict passwords. However, users often choose highly predictable passwords based on personal information, dictionary words, birth date, etc.
OBJECTIVES: The primary objective is to ascertain password choice and practices of users of developing countries.
METHODS: Most of the existing studies are done in the developed world and our exhaustive search failed to find similar research in the context of developing countries. Here, we conducted detailed surveybased scrutiny about the password-based security perceptions of Bangladeshi nationals, which include 881 participants, primarily students, and professionals.
RESULTS: Most of the users were found to have bad practices, for example, having personal information(56%), password reuse(69%), having commonly used patterns(81.3%). Students from technical backgrounds fared well compared to non-technical backgrounds as expected. However, some professionals (especially Bankers) surprisingly chose weaker passwords even though dealing with sensitive data.
CONCLUSION: We also make a few recommendations to improve awareness.

Received on 05 December 2021; accepted on 08 February 2022; published on 11 February 2022

Keywords: Password strength, User perception, Password policy, Security, Usability, Memorability

doi:10.4108/eai.11-2-2022.173452

1. Introduction

In the era of modern technology, the way people communicate and interact has been revolutionized. Nowadays, internet users have to create and maintain multiple online accounts to enjoy various services. With billions of users, the capability to authenticate users into various web-based systems and protecting privacy is highly crucial. Due to the greater engagement of mass people in online life, concerns about the security of confidential data such as personal identification information (PII) and financial records are growing.

Compromising authentication information may jeopardize the user and as a whole the corresponding system itself. In most cases, the security of the entire system relies on the strength of a user's password. A good password needs to be easy-to-remember but hard-to-guess [1]. However, this requirement also implies that, due to a lack of knowledge about the essential features of a strong password, people may not be able to choose passwords intelligently to protect them sufficiently.

Password-based authentication is in use for a long time and the popular among wide user bases. However, as we are meeting rapid adoption of new technologies such as cloud applications, social networking sites, we often need to remember quite a few usernames and passwords daily, which is not always easy [2]. A recent study revealed that on average, a user maintains 25 online accounts [3]. As a result, often the same password or slightly modified one is used for multiple accounts, making them vulnerable to attackers [4].

This paper tries to ascertain the understanding of password vulnerability among the users of the developing world. In this context, the users are from Bangladesh - a rapidly developing country in the global south. We have adopted a survey-based method to understand people's perceptions

[*]Corresponding author. Email: rumee@cse.du.ac.bd

of passwords. Although many researchers have conducted similar research on users from the developed countries [5–7], the findings may not be directly applicable to the developing world. Education, income, exposure to technologies, and prevalence of technology in society may shape how people perceive technology. Many also argue that the "digital divide" about access to, use of, or impact of information and communication technology, plays an important role in shaping people's perception. However, this scenario is changing as indicated by the study of World Bank, which shows that most of the Internet users in the developing countries have joined since the year 2005. Though it has been more than a decade, technology adoption is still in its early years for mass people in developing countries and the online services/applications are yet to raise privacy awareness among users [8, 9].

The newly joined groups of Internet users hold a majority part as inexperienced. Even though the user number jumped out rapidly, it's not rich enough when we compare it to the total population. The large number of users who lack experience may expose behaviors that may impact thoroughly and put the security at stake. Such as engaging in risky online behavior, replying to emails from suspicious sources, password creation, as well as management citeref18. Recently, Bangladesh has suffered several cyber-attacks and bank-heists. With the rise of the number of users, these attacks are becoming more common. Hackers penetrated the system of the central bank of Bangladesh by manipulating vulnerability in the SWIFT network. This made the bank lose 81 million [10].

In this work, we hypothesize that the reason for this personal inhibition may be due to a lack of awareness of what to expect in the cyber world and how to protect security and privacy from possible ICT vulnerability. Lack of knowledge in how to protect oneself from cyber vulnerability may deter one from exposing sensitive data. Contrarily, this lack of care may indirectly indicate that the users do not find cyber presence as sensitive as it should be.

To understand the current situation, in this research we try to understand the perception of the password used by the users in Bangladesh. For this, we performed a detailed user survey of 881 people from a variety of educational and technical backgrounds. Our participants include students (both ICT major and other disciplines), doctors, engineers, government employees, military personnel, and baking officials. They gave their opinion through both online and offline survey questionnaires, designed specifically to discover user behavior, conception, and practices in choosing their passwords in various online or offline accounts.

Analyzing the survey we got interesting results that will help the policymakers to understand user perceptions towards password-based authentication and will help redesign their system or place additional hints or restrictions to make sure good passwords are chosen by the user. Some of the key findings of this research are listed below:

- Perception of passwords among students and professionals in Bangladesh is not satisfactory, which could be improved with better awareness training and campaign.
- A significant number of users (approximately 56%) included personal information and other commonly guessable patterns in their passwords, many of them from technical backgrounds and well aware of the pitfalls of weak passwords.
- More than 69% of users were found to have reused their password and this is not expected to go down dramatically with more awareness. Policies can be developed to allow users to reuse passwords in certain accounts and prohibit in security-critical services.
- Students with technical subject major especially Computer Science or related discipline created comparatively better passwords than the students from other backgrounds. Given the widespread use of computing technology in all areas of the education pipeline, this outcome was unexpected and was more related to the overall country (here Bangladesh) specific statistics.
- Professionals who participated in our study (doctors, engineers, government employees of various positions, banking officials) showed interesting behavior too. The most surprising was the easily crackable passwords created by the bankers, which is alarming as they often deal with sensitive personal information. It was also found that they created bad passwords even with certain password guidelines enforced by the organization. This finding suggests that password rules alone is not enough, and should be applied with additional warning and awareness program.

The rest of the paper is organized as follows: section 2 discusses related research, section 3 introduces overall workflow and the design of questionnaire used for the user survey. In section 4, we describe in detail the findings of this study including the demographics and analysis of the observed data. Finally, the paper concludes in section 5 with a summary of the findings and few recommendations for policy formulation and better password security awareness buildup.

2. Related Work

Researchers have put in significant effort into understanding various aspects of passwords: what makes a password strong, how to remember strong passwords, the composition of good passwords, how user choose their passwords, etc. Here, we limit our discussion to a few closely related work that are particularly focused on understanding users' behavior and perception towards passwords.

2.1. Perception of Password Strength

To enhance security, strong passwords are the obvious choice. Researchers found that sometimes passwords are constructed naively by users and they also know it. Sometimes users think they are creating a good password, which is not strong [7].

Morris and Thompson were one of the first to perform a detailed study on password strength [11]. They collected 3289 passwords from various users over a long period. Among these, about 89% of the passwords were underperforming and poor.

Tobias et al.[12] even created an online game to understand user perception towards password strength. In, [13] researchers investigated the effect on users' conception by improved graphical representation of password meters output. On the other hand, Yimin et al.[14] came up with an effective but lightweight method to estimate password strength by the meters.

More recently, in their work [7, 15], Jason and Nikki surveyed more than 400 people from a different socioeconomic, educational, and technical backgrounds to find whether users can distinguish between strong and weak passwords. Based on their findings most user groups could recognize weak passwords, but they often failed to identify the stronger ones. Apart from that, they found the technical background of the participants did not affect their perceptions about good(strong) passwords.

System generated random passwords very strong from a security perspective, however, suffer measurably in memorability issue. Mahdi et al. [16] designed a visual cue-based game model to show that user perception towards random passwords can be increased by ensuring much better usability and memorability. The graphical scheme is also used by the researchers in [17–20] to show better remembrance of strong passwords. A study on a wide group of users reveals that they remember graphical passwords for a longer period [21].

2.2. Password Habits and Common Practices

Often vulnerabilities and privacy violations arise from not only weak perception about password strength, but also bad habits and practices [4].

Reuse of same or almost identical passwords in multiple websites is one of the very common practices, yet a major cause of vulnerability [6]. In their study [3], Florencio and Herley reported that on average every user had about 25 accounts and 6.5 passwords, each of which is shared across 3.9 sites. The study also exacted that passwords containing only lowercase letters dominate at all lengths and most of the people use longer lowercase passwords and hardly use uppercase or special characters. Password reuse itself is a major cause of personal data breaches as reported in [22–25] etc.

The survey conducted by Brown and Bracken which evaluated the generation and use of passwords showed that students use around 8.18 passwords on average. These passwords are inherited on a scale of two-third by personal characteristics, with most of the remainder relating to relatives, friends, or lovers. It was also found that almost all the subjects use passwords more than once, again two-third of these passwords are used by duplicating. A third of the subjects forget passwords and more than half keep records of it [26].

Nowadays most services are online and accessed through a browser. People often allow browsers to remember the password to avoid typing it all the time. This is one of the bad practices and has serious consequences if done in public spaces(computers, mobile devices, or the network itself), which is a common behavior even with proper warnings in place [27, 28].

Adam and Sasse [29] conducted a detailed study on password-related user behaviors such as password construction, frequency of use, password recall, and in particular memorability issues. Their report mentioned that the introduction of restrictions for creating more secure password content may cause the production of passwords that may give a hard time to memorize. This may lead to an increase in password disclosure, thereby causing a lot of users to avoid such restrictions to produce passwords easier to memorize. Although these findings are almost two decades old, from the security awareness perspective, users (mostly non-technical) still make similar mistakes [30–32], and often need an additional level of warnings or nudges [33].

In another study [34], Kanich and Mirkovic studied the semantic structure, strength, and reuse of real passwords, as well as conscious and unconscious causes of unsafe practices, whereas about 50 participants took part. Their

findings include that the main causes for password reuse are misconceptions about risk, and preference for memorability over security.

Lorrie Faith Cranor along with her team conducted several studies of password-related behaviors, such as best password policies, user behavior towards password, password recall, and also suggested how a user can make stronger passwords. Their work [35] found out that most of the users have serious misconceptions about what a good(strong) password should contain. Later on, they also discovered that stronger passwords are correlated with a higher rate of errors entering them [36].

3. Methodology

In this work, we conducted a survey (both online and offline option was given) involving 881 people of Bangladeshi nationals. The participants include undergraduate students of public and private universities, doctors, engineers, bank officials, and military personnel. The survey was designed to collect data on users' password handling, composition, reuse behavior, and user sentiment about password strength. In this section, we discuss the core architecture of the study: survey setup and questionnaire design for data collection.

3.1. Survey Setup

Figure 1 shows a high-level overview of the workflow followed to design this survey.

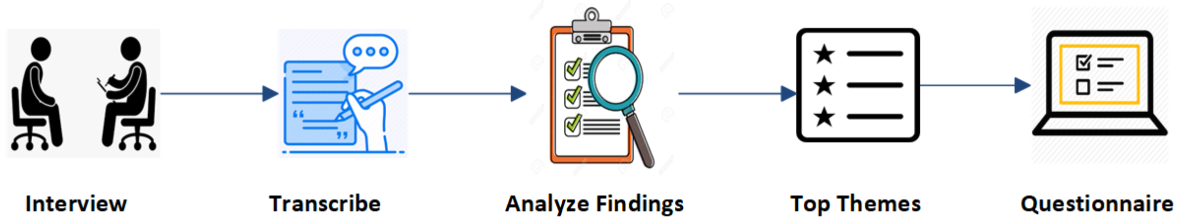

Figure 1. Steps Followed in Survey Questionnaire Design

At first, we conducted semi-structured interviews of a select group of participants involving at least two from each of the target user demographic and professionals listed in Table (1). They were asked about the various aspects of their password usage behaviors and security awareness relating to that.

Next, all the recorded interviews were transcribed resulting in an anonymized text version of the responses.

After that, we thoroughly analyzed the transcripts and mined the key terms and factors which repeatedly came up during the interviews. These frequently occurring themes laid the foundation of the questionnaire used in our survey.

3.2. Questionnaire Design

Based on findings from the semi-structured interviews and general survey guidelines, we designed a questionnaire to perform the aforementioned study. The formation and design of this questionnaire are discussed in more detail below.

Demographic Questions. In the first part, the participants were asked a few basic questions about their background information (age, gender, occupation, degree pursued, major of study, number of years spent at the university, etc.). Demographic questions are a very important part of our questionnaire because they will help us to find out how user's perception varies along with these demographic factors. Also, we asked our participants if they have a degree/job/training in computer science and/or engineering, information technology, or a related field.

Question on Usage of Computer and Internet. Most of the users in Bangladesh are novice users and are recently exposed to the Internet, which has grown exponentially in recent years. Due to a lack of awareness about privacy and security, these new Internet users (on the scale of millions) lead Bangladesh to a vulnerable state. In this part of our questionnaire, participants were asked few elementary questions about computer and Internet usage. Participants were also asked where they typically access the Internet, how they authenticate/identify themselves, which is the most used device, and how long they have been using computers and the Internet.

Questions on Participants Perceptions and Password Practices. Here, participants were asked 18 questions in total. The queries focused on various issues related to password composition, length, usage pattern, and their relation with password memorability, difficulty in remembering passwords, etc. In general, the questionnaire intends to find out the following critical information from the participants.

a. Password reuse: Using the same password for multiple accounts increases the probability of an important account falling victim to attackers. Participants were asked if they have the same passwords for multiple accounts or modify existing passwords to reuse them.

b. Length of password: Length conquers complexity. Allowing passwords to remain short and complex makes them more vulnerable to attack than simply requiring easier-to-remember, longer passwords. We wanted to know if participants understand this fact by asking them how many characters a strong password should contain.

c. Composition of password: The strength of a password is the function of length, complexity, and unpredictability. We asked our participants 2 questions to understand their sentiment about a different factor that determines password strength, such as the use of symbol, digit, lower case, and upper case letters. They were also asked about the combination of these factors in their password. For example, some people may use only digits, some others may use a combination of lowercase and uppercase letters.

d. Things that should not be in a strong password: If a password contains personal information (name, phone number, address, etc.), dictionary words, keyboard patterns, it becomes vulnerable no matter the complexity. We asked our participants if they think it is okay for a standard password to contain these things.

e. Password pairs: 10 password pairs were given to the participants and they were asked to choose the stronger one from each pair. Here, we wanted to find out if they knew certain things that make passwords predictable, such as capitalizing randomly the middle of the word is better than capitalizing the first letter of a word, easy substitutions like replacing "a" with "@" should be avoided, etc.

Open Ended Questions. At the end of our questionnaire, we asked our participants to create a password that must

Table 1. Total number of people who participated in the survey. The sample is biased towards students in the public and private universities of the country assuming that students will be more exposed to newer technologies and hence may have clearer view of password vulnerability.

Profession	Number of Participant
University Students	718
Doctors	30
Military Personnel	28
Government Employees	40
Engineers	35
Bank Employees	30
Total	881

be strong enough (hard) to crack and also easy to remember. We used the Likert [37] method to find out how confident they are about their created passwords. In addition to this, we asked another question to find out if they use passwords of the same strength in all of their accounts or they use a strong password (according to their knowledge) in a few of them.

3.3. Conducting Survey

We started with collecting information from a variety of university students and professionals from various departments. Around 80 participants took part in our survey through Google form. We used snowball sampling to spread the form. While collecting and managing the data would have been easier online, but we got poor responses while collecting data online. Then we decided to do the survey offline, by giving the printed version of the questionnaire.

Around 800 people participated in our survey offline. They were given a printed version of the form.

4. Description of The Demographics and Analysis

This section discusses the participants' demographic of the survey and a detailed analysis of the findings. This study was conducted on a group of participants from Bangladesh, a rapidly developing country. Here, at first, the user demographics are mentioned, followed by our findings on password usage behavior and security perception. Then we present a detailed analysis of the passwords created by the participants, which reveal a lot about the overall user behavior and know-how about the passwords.

4.1. User Demographics

The total number of people who participated in this survey is 881. Among them, 718 are students and 163 are professionals. Our participants are from various professions. Table 1 shows overall statistics of participants along with their professions.

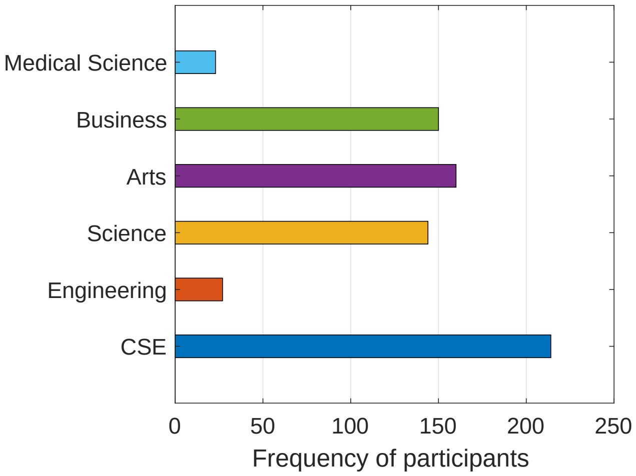

Figure 2. Student participants grouped by major area

Most of them are students of public and few private universities of Bangladesh. We also collected data from medical students studying at various medical colleges all over the country.

As a whole, students who participated in our survey fall into 6 different major areas: engineering, science, computer science or relevant discipline, business, medical studies, and arts. Their distribution is shown in Figure 2.

Apart from the students, we surveyed employees of different state-owned commercial banks of Bangladesh. The users were selected from the 8 branches of three such banks situated in Dhaka and Mymensingh district. Army officers who participated in this survey are relatively young, whose ranks were captain, second lieutenant, and major. Other significant demographic of the users were engineers, doctors, and government employees working in diverse capacities and positions.

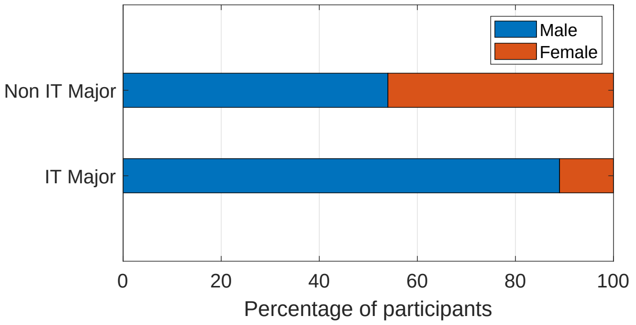

Figure 3. Gender distribution of student participants

Among 881 participants, 465 are male and 336 were female. However, among the student participants, male to female radio widely varies depending on their major as shown in Figure 3.

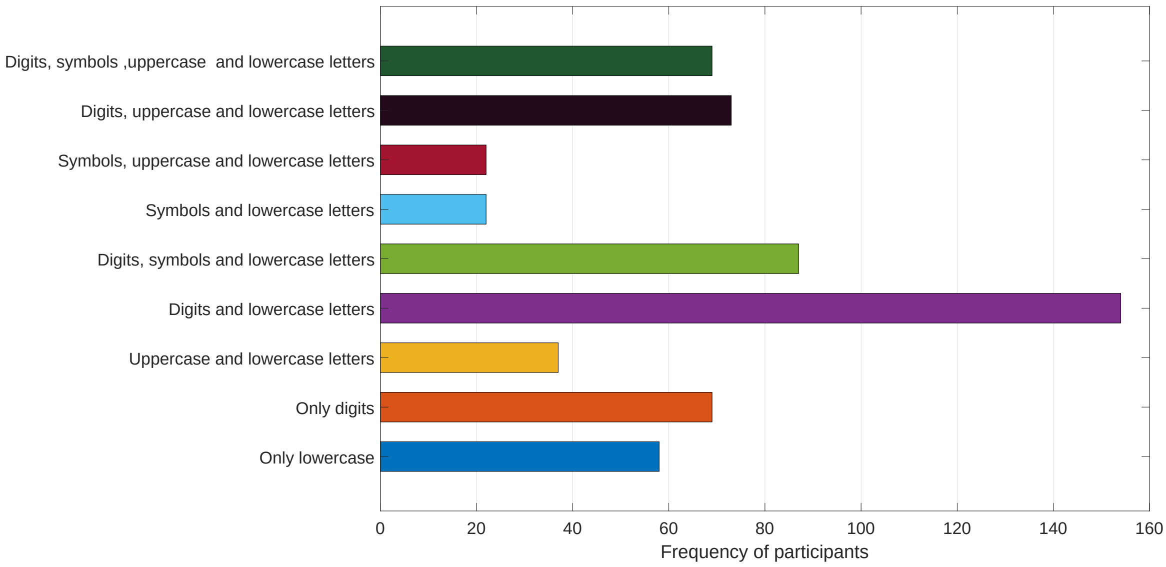

Figure 4. Character composition of the participants' passwords

The given graph shows the percentage of these categories. However, these two demographic factors are not independent. We applied Fisher's exact test of independence [38] with the data, and p value of .0001, which implies that it is extremely statistically significant.

4.2. Study Findings: User Perceptions and Practices

In the questionnaire, we asked participants to create a password according to their knowledge which is strong enough to crack and also easy to remember. We got a total of 745 responses for this. Here, the results of our analysis on passwords created by the survey participants are discussed.

In questions number 13-32 we tried to find out password perception and practices of the participants, such as password reuse habits, what standard length of a strong password should be, if they think it is okay to have certain things in their passwords, etc. Using the responses received through the questionnaire, we evaluate users' perceptions about passwords using the following criteria. Here, it is to be noted that not all participants answered all questions in the questionnaire, which resulted in differences in the number of responses analyzed for each criterion.

Password Construction Behavior. Password strength is mostly dependent on the character composition. Larger the variations password contents: use of lower case, uppercase letters, symbols, digits, etc., higher the entropy. High entropy means an attacker has to try many more combinations before making a successful guess of the password [39, 40]. Figure 4 illustrates the password compositions of our survey participants. The patterns observed in terms of position of these characters are further highlighted in Figure 5.

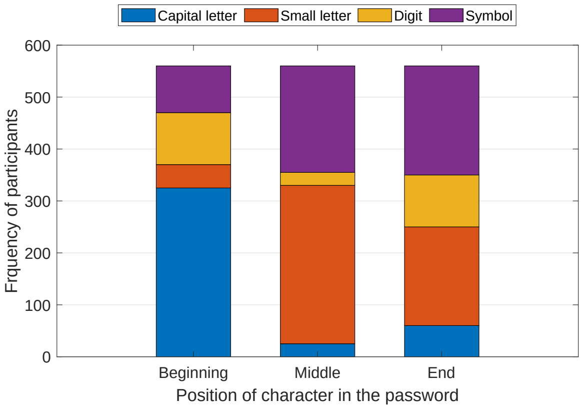

Figure 5. Potential position of various character types

We asked participants what is the domain of their passwords, that is what are the factors their password is consists of. Most possible combinations were given as options along with popular ones, for example- only lower case letters, digits along with lower case letters, etc.

It is observed that the most popular domain for a password is using only digits with lowercase letters. Among participants, 168 of them (approximately 25%) said their passwords consist of only digits and lowercase letters. Only using lower case letters with digits does not contribute much to entropy. The password of 8 characters, including only digits and lowercase letters, has a poor entropy (in the range 25-35, depending on the position of characters) and is considered as weak by various password meters available online based on the guideline given by NIST (National Institute of Standards and Technology, USA) ([41]).

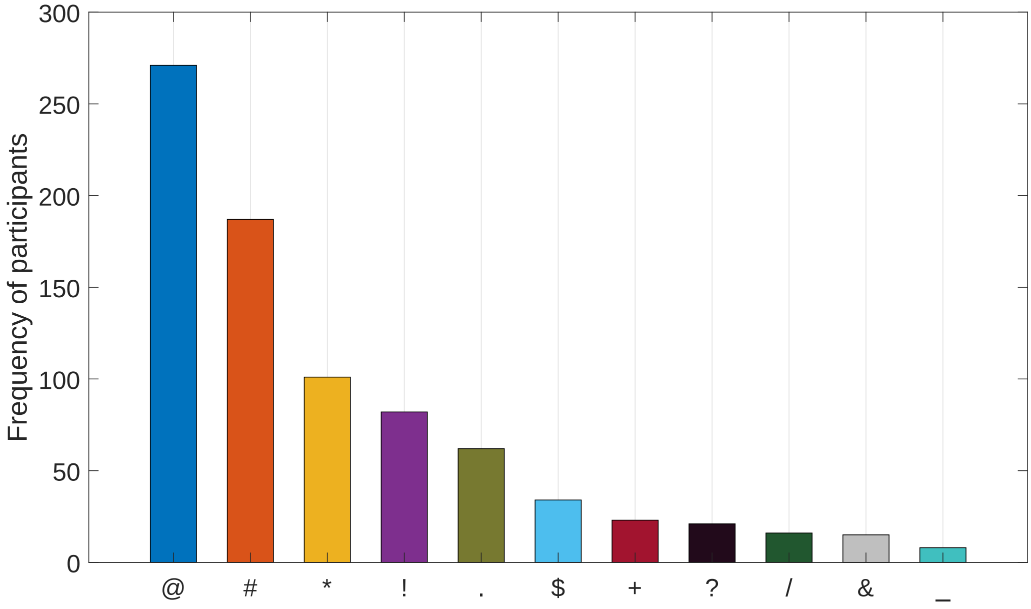

Figure 6. Most frequently used symbols in passwords

The second most popular answer was lower case letters with symbols (approximately 14%). Surprisingly, 4th popular answer was only digits. Approximately, 13% of the participants use only digits in their password, which makes the password extremely weak as a password containing 8 digits only can't have entropy more than 15 which is much below the standard entropy of a strong password.

More than 64% of participants used upper case letters at the beginning. Most participants (59%) used lower case letters in the middle. At the end of the password, using symbols and lower case letters is common. Hence we can come to the conclusion that more than 50% passwords follow the structure: $uppercase + lowercase + lowercase$ or the structure: $uppercase + lowercase + symbol$. By using structured brute force attacks, the time required to crack the passwords can be minimized significantly.

Frequently Used Symbols. We analyzed the passwords to find out what are the most frequently used symbols. And the result is shown in Figure 6.

The most used symbol is '@', found 271 times which is more than one-third of the total number of passwords we have in our collected data. The symbol '@' in passwords is included in most cases following the structure of the email address. As for example, a common pattern is- "$name + @ + institution'sname$". The second most frequently used symbol is '!'.

The word password itself was present 26 times. The result shows that 81.3% of passwords are extremely easy to guess even the passwords having satisfactory entropy values.

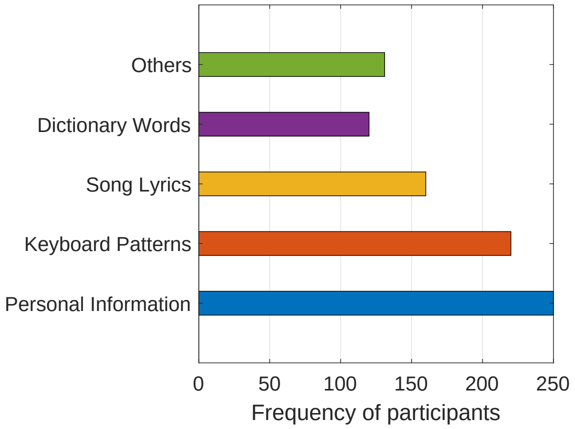

Figure 7. Frequently used in surveyed passwords

Frequently Used Patterns. We have analyzed collected passwords to find frequent patterns in them. The result is shown in Figure 7.

Dictionary words are most common in passwords. Total 343 dictionary words are found, which consists of 46% of passwords. Surprisingly, the second most common pattern is personal names. Among 745 passwords, 155 (approximately 21%) of them have personal names (participants' names, names of their spouses, children, etc.) in them. The result is alarming, as personal names can be easily known by attackers.

Other common patterns found in the passwords are- recent year (e.g 2019, 2020) information and common (contiguous characters on the keyboard) keyboard sequences.

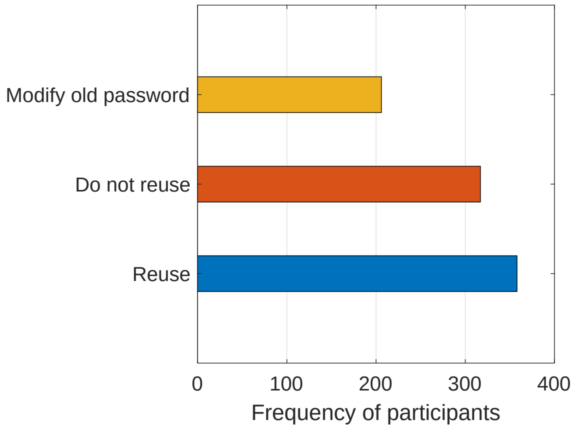

Figure 8. Password reuse behavior of participants

Apart from those, the number of Bengali (mother tongue of participants) words written using English alphabet characters were approximately 9%.

Password Reuse Habits. Reusing passwords is a common habit [42]. In the 16th question of the questionnaire, we asked participants if they reuse their passwords in multiple accounts. The result (Figure 8) found is alarming.

Here, we observe that more than 69% of participants either reuse their passwords unchanged or by modifying the existing ones. Taking into fact that this scenario is quite common in most of the users, they are highly vulnerable to attack and personal data breaches easily.

Perception of Password Strength. We asked participants if they feel like it is okay to include certain things in their passwords. The options include personal information (name, phone number, institution name, etc.), song lyrics, dictionary words, keyboard patterns. Surprisingly, 256 participants said that it is absolutely fine to include personal information in their password, which is approximately 30% of the participants. The second popular answer was including keyboard patterns in passwords (qwerty, 123456, zxcvbn, etc.), the exact number is 223 which is 26% of the total participants. The only 14% of the participants said that they think none of these should be in a password. Hence, we see that the most terrible practices are the most popular ones.

We found out that participants have some basic knowledge of the characteristics of good passwords: Capitalizing randomly the middle of the word is better than capitalizing the first letter of a word, using only lower case letters is better than using only digits, dictionary words should be avoided to create a strong password, using common keyboard patterns (qwerty, 12345678, qazwsx, etc.) makes it easier to guess, etc.

Password Memorability. If people do not have to remember passwords, the strength of the password would be maximum [1]. We asked participants if they face difficulties remembering their passwords.

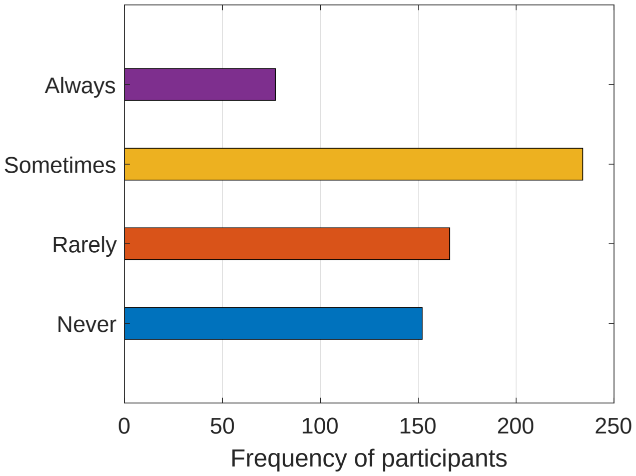

Figure 9. Difficulties in remembering password

Among the 881 participants, 629 persons answered the question: how often do you face difficulty remembering your password. Figure 9 shows the distribution of the responses. So, we can conclude that almost 50% of our participants faced difficulties recollecting their passwords at least sometimes, which is significant.

However, participants were found to have some misconceptions as well. For example, the majority of the participants did not know that easy substitution is predictable for the attacker, such as replacing ‘a’ with ‘@’ or ‘to’ with ‘2’. Participants also thought that adding digits at the end rather than a random letter makes it stronger [43].

4.3. Correlation between password strength and demographics

We find an interesting relationship between password strength with various demographic factors. Here, at first, the methodology for password strength measurement is discussed. Then, we portray how strength varies among different participants based on their discipline.

Password strength calculation. Password strength is the measure of the resistance of a password against guessing and brute force attacks [44]. In the previous section, we mentioned entropy as a measure of password strength, which is not adequate in all cases. Cracking a password by brute force means all possible values are taken as equally important, although they are not. Entropy is a good measure of password strength when all choices made are random. The password created by humans are not random, there are some patterns that most people follow. Some guesses have a good chance of success than others [45].

Modern password cracking involves smart guessing of passwords. Machine learning is used to guess passwords, the huge amount of training data is given to crack a password in the order of guesses that has the highest probability of success in minimum time. Hence, we measured the strength of the passwords with the help of a password meter named *zxcvbn* which measures the strength using machine learning.

The meter “zxcvbn” is created by Dropbox and is one of the most accurate password strength calculators. It is trained using 31k passwords and is capable of detecting popular names, patterns, easy substitutions (p@$$word, f@ceb00k), etc. We found the source code on github.com. We downloaded the python version of it and ran it on our computer. Each password is given as input, and output consists of the number of guesses/times required to break the password, suggestions on how to improve it, etc. For our convenience, we decided to take 10 base logarithms of the number of guesses as to the measure of strength.

Variation of password strength among students of different faculties. We calculated the password strengths of students of different faculties and find out the percentage of passwords cracked after a given number of guesses. The graph given in Figure 10 clearly shows the difference in password strength among students of four groups. 100% passwords of humanities students are guessed after 1017 guesses, although only 72% passwords of CSE majors are discovered after mentioned amount number of guesses.

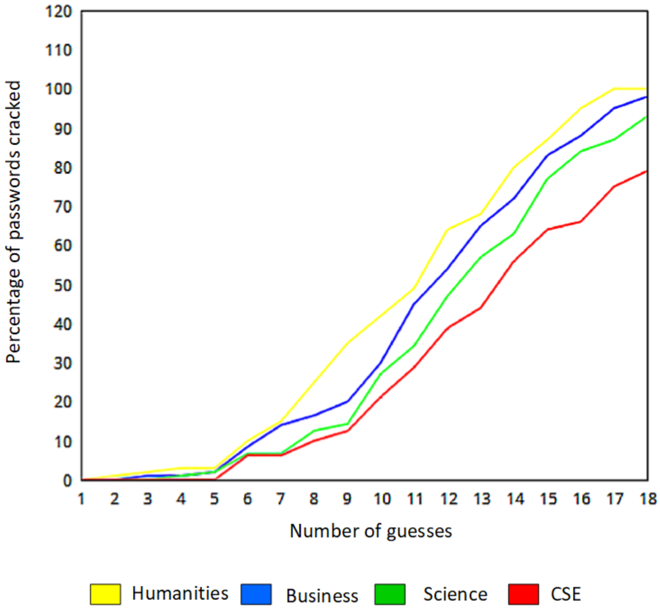

Figure 10. Student participants grouped in their respective subject of study

We conclude that CSE majors use the strongest passwords, followed by science, business, and humanities, agreeing mostly to the general perception [7].

Variation of password strength among professionals. Professionals in this survey were divided into 5 major groups- doctors, army officers, engineers, government officials, bankers. We calculated the mean password strength of each group. We decided to take the median as the measure of central tendency because by using the median we can eradicate the influence of extreme values.

Table 2. Mean Password Strength of Various Professionals.

Profession	Strength(Measured in Median)
Engineers	13
Doctors	12
Military Personnel	11
Government Employees	12
Bank Employees	8

The result is shown in Table 2. Mean password strength was greater for the engineers compared to, which is expected. However, bankers had the least mean password strength, which was surprising given the fact that bankers often handle very sensitive customer data. To investigate this unusual finding, we further interviewed some of the bankers at one of the banks we have surveyed. They informed us that they use a software named *Temenos Transact* [46].

The password policy of *Temenos Transact* requires their passwords to be at least 8 characters and they must include digits, symbols, upper case, and lower case letters. In this study, most of them(bankers) created passwords with barely meeting minimal recommendations, which had - length 8, common patterns, and one symbol, one digit at the end.

4.4. User Feedbacks

Designing and providing user feedback was an important part of our project. After participants completed the survey questionnaire, they were given detailed feedback on the quality of their created passwords.

We designed the feedback to create awareness in them. Good answers to all of the questions were given in the feedback along with suggestions on creating and managing passwords. Our participants came from various sectors, most of them don’t have any degree/job in computer science or related fields so we tried to explain in the easiest way why using a strong password is important. We also told them about common wrong perceptions and how they can make their password unpredictable.

Practices that should be avoided are also presented in the feedback, for example why they should never use the same passwords for more than one accounts, and they should always avoid including personal information and dictionary words in their password. In the end, in our feedback, we provided a method to create memorable passwords developed by security expert Bruce Schneier [47].

5. Conclusion and Policy Implications

Basing on a survey conducted by more than 800 individuals, we report public perception of passwords among students and professionals in Bangladesh. We collected data from December 2018 to February 2019.

Our findings further confirm the fact that users often face difficulties remembering their passwords. More than 50% of survey participants faced problems recalling passwords at least sometimes, which led them to use weak easily memorable passwords. Also, password reuse habit is found to be very common among users. More than 69% of users have either reused their passwords or modified the old passwords to create new ones. The percentage is significantly high, and there is very little chance that it will decrease with time (with the increased usage of the Internet, the number of accounts users have to maintain is also increasing). So, instead of telling users not to reuse their passwords, it will be more effective if we tell them to identify important accounts from unimportant ones and never reuse passwords in an important account.

A significant number of users (approximately 56%) included personal information, easily typed keyboard patterns in their passwords, which is alarming. In the feedback provided to the participants, we mentioned never to use certain things in their passwords. More awareness programs should be done in this matter.

We analyzed passwords created by our participants and the result is quite interesting. The use of Bengali words written in English is very common. ‘Bangladesh’, ‘1971’, ‘1952’, ‘manikgonj’ (name of a district) were present several times. These words are very relevant and popular in the context history and geography of Bangladesh. Although password meters created by researchers of developed countries will identify these passwords as strong, a smart attacker can easily take advantage of commonly used words in this geographical area.

Most of the passwords fall under some common configurations, where some patterns are found to be repeated. In this study, by analyzing collected passwords, we found two configurations to be prominent and approximately 50% passwords follow that structure. These well-known configurations can easily be subject to structured brute force attacks and should be avoided.

Passwords created by the students and professionals also showed a stark contrast to what we thought the outcome would be. We had divided the students into six groups and compared the percentages of passwords cracked in each group after a certain amount of guesses. We find that the humanities group created the weakest password and the CSE major students came up with the strongest ones, which was expected. However, surprisingly, passwords created by bankers had the least mean strength compared to other professions in the study. It was also discovered that the password policy used in those banks is not sufficient to eradicate the wrong perception among the bankers. Organizations should be more aware of training employees on security awareness and come up with systems that encourage better password choices.

Our concluding remark is the overall perception of passwords among students and professionals in Bangladesh is not satisfactory. Hence raising awareness among the people by conducting awareness programs could be one way to let people know about these vulnerabilities. New applications may be designed that will include a context-dependent password meter. This was prompted by the fact that although lots of password meters are available in online application stores, most of them cannot detect common Bengali words(written in English letters in passwords) that we found in our study. Such applications may help common users by showing the strength of the given password in their languages and provide suggestions based on their given password.

The findings indicate that the users in Bangladesh may not be aware of the vulnerabilities that they are bringing in into the networks. Lack of awareness regarding what constitutes a strong password may also indicate either the users rely on the systems to protect them at times of security breach or they do not give enough importance to security and privacy in cyberspace. This indicates that governments, service providers, and consumer societies should take greater steps to increase awareness among people.

As a whole to ensure digital privacy and enhancing the benefits of various online services to people, a human-centric behavioral approach towards security and privacy should be taken into consideration. We hope that as Bangladesh is a developing country its experience may be similar to countries that are striving forward.

References

[1] Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004) Password memorability and security: Empirical results. *IEEE Security & privacy* **2**(5): 25–31.

[2] Raponi, S. and Di Pietro, R. (2020) A longitudinal study on web-sites password management (in) security: Evidence and remedies. *IEEE Access* **8**: 52075–52090.

[3] Florencio, D. and Herley, C. (2007) A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*: 657–666.

[4] Dastane, O. (2020) The effect of bad password habits on personal data breach. *International Journal of Emerging Trends in Engineering Research* **8**(10).

[5] Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L. *et al.* (2015) A spoonful of sugar? the impact of guidance and feedback on password-creation behavior. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*: 2903–2912.

[6] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. *et al.* (2010) Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*: 1–20.

[7] Pittman, J.M. and Robinson, N. (2020) Shades of perception-user factors in identifying password strength. *arXiv preprint arXiv:2001.04930* .

[8] ((accessed December 1, 2020)), How mobile app user behavior differs according to the region., http://engineering.purdue.edu/~mark/puthesis/.

[9] Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., Chen, J. *et al.* (2011) Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions*: 39–44.

[10] (2016 (accessed December 1, 2020)), Bangladesh bank heist: Lessons learned, https://www.bankinfosecurity.com/bangladesh-bank-heist-lessons-learned-a-9064.

[11] Morris, R. and Thompson, K. (1979) Password security: A case history. *Communications of the ACM* **22**(11): 594–597.

[12] Seitz, T. and Hussmann, H. (2017) Pasdjo: quantifying password strength perceptions with an online game. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*: 117–125.

[13] Golla, M., Hahn, B., zu Selhausen, K.M., Hosseini, H. and Dürmuth, M. (2018) Bars, badges, and high scores: On the impact of password strength visualizations. *Who Are You?! Adventures in Authentication (WAY)* .

[14] Guo, Y. and Zhang, Z. (2018) Lpse: lightweight password-strength estimation for password meters. *computers & security* **73**: 507–518.

[15] Pittman, J. and Robinson, N. (2020) Do users correctly identify password strength? In *Journal of The Colloquium for Information Systems Security Education*, **8**: 6–6.

[16] Haque, S.T., Al-Ameen, M.N., Wright, M. and Scielzo, S. (2017) Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2017), USEC*, **17**.

[17] Thorpe, J. and Van Oorschot, P.C. (2004) Towards secure design choices for implementing graphical passwords. In *20th Annual Computer Security Applications Conference* (IEEE): 50–60.

[18] George, C., Khamis, M., Buschek, D. and Hussmann, H. (2019) Investigating the third dimension for authentication in immersive virtual reality and in the real world. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)* (IEEE): 277–285.

[19] Nasrullah Al-Ameen, M., Wright, M. and Scielzo, S. (2015) Towards making random passwords memorable: Leveraging users' cognitive ability through multiple cues. *arXiv e-prints* : arXiv–1503.

[20] Al-Ameen, M.N., Fatema, K., Wright, M. and Scielzo, S. (2015) The impact of cues and user interaction on the memorability of system-assigned recognition-based graphical passwords. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*: 185–196.

[21] Tullis, T.S., Tedesco, D.P. and McCaffrey, K.E. (2011) Can users remember their pictorial passwords six years later. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems*, 1789–1794.

[22] Jaeger, D., Pelchen, C., Graupner, H., Cheng, F. and Meinel, C. (2016) Analysis of publicly leaked credentials and the long story of password (re-) use. *Hasso Plattner Institute, Universidad de Potsdam. Disponible en https://bit.ly/2E7ZT01* .

[23] Ramanujam, A.S.A., Aarthi Valliammai, K., Akhil Krishna, T. and Rajasekaran, T. Prevention of data stealing using password managers .

[24] Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. (2014) The tangled web of password reuse. In *NDSS*, **14**: 23–26.

[25] Wang, C., Jan, S.T., Hu, H., Bossart, D. and Wang, G. (2018) The next domino to fall: Empirical analysis of user passwords across online services. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*: 196–203.

[26] Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. (2004) Generating and remembering passwords. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition* **18**(6): 641–651.

[27] Oesch, S. and Ruoti, S. (2020) That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In *USENIX Security Symposium*.

[28] Hallett, J., Patnaik, N., Shreeve, B. and Rashid, A. (2021) " do this! do that!, and nothing will happen" do specifications lead to securely stored passwords? *arXiv preprint arXiv:2102.09790* .

[29] Adams, A. and Sasse, M.A. (1999) Users are not the enemy. *Communications of the ACM* **42**(12): 40–46.

[30] Taneski, V., Heričko, M. and Brumen, B. (2014) Password security—no change in 35 years? In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (IEEE): 1360–1365.

[31] Erceg, A. (2019) Information security: threat from employees. *Tehnički glasnik* **13**(2): 123–128.

[32] Alomari, R., Martin, M.V., MacDonald, S., Bellman, C., Liscano, R. and Maraj, A. (2017) What your brain says about your password: Using brain-computer interfaces to predict password memorability. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)* (IEEE): 127–12709.

[33] Guo, Y., Zhang, Z., Guo, Y. and Guo, X. (2020) Nudging personalized password policies by understanding users' personality. *Computers & Security* **94**: 101801.

[34] Hanamsagar, A., Woo, S., Kanich, C. and Mirkovic, J. (2016) How users choose and reuse passwords,". *Information Sciences Institute* .

[35] Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N. and Cranor, L.F. (2016) Do users' perceptions of password security match reality? In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*: 3748–3760.

[36] Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G. *et al.* (2013) Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*: 173–186.

[37] Joshi, A., Kale, S., Chandel, S. and Pal, D.K. (2015) Likert scale: Explored and explained. *British Journal of Applied Science & Technology* **7**(4): 396.

[38] ((accessed November 1, 2020)), Fiesher's test of independence, http://www.biostathandbook.com/fishers.html.

[39] TAHA, M.M., ALHAJ, T.A., MOKTAR, A.E., SALIM, A.H. and ABDULLAH, S.M. (2013) On password strength measurements: Password entropy and password quality. In *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)* (IEEE): 497–501.

[40] KOMANDURI, S. (2016) Modeling the adversary to evaluate password strength with limited samples .

[41] GRASSI, P.A., FENTON, J.L., NEWTON, E.M., PERLNER, R.A., REGENSCHEID, A.R., BURR, W.E., RICHER, J.P. *et al.* (2020) Digital identity guidelines: Authentication and lifecycle management [includes updates as of 03-02-2020] .

[42] BROWN, A.S., BRACKEN, E., ZOCCOLI, S. and DOUGLAS, K. (2004) Generating and remembering passwords. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition* **18**(6): 641–651.

[43] UR, B., KELLEY, P.G., KOMANDURI, S., LEE, J., MAASS, M., MAZUREK, M.L., PASSARO, T. *et al.* (2012) How does your password measure up? the effect of strength meters on password creation. In *21st {USENIX} Security Symposium ({USENIX} Security 12)*: 65–80.

[44] DELL'AMICO, M., MICHIARDI, P. and ROUDIER, Y. (2010) Password strength: An empirical analysis. In *2010 Proceedings IEEE INFOCOM* (IEEE): 1–9.

[45] MARQUARDSON, J. (2012) Password policy effects on entropy and recall: Research in progress .

[46] ((accessed December 1, 2020)), Temenos transact core banking software, `https://www.temenos.com/products/transact/`.

[47] SCHNEIER, B. (2004) Customers, passwords, and web sites. *IEEE Security & Privacy* **2**(4): 88.