Research Article

A Study of Password Management Behaviors of Young People

Chatphat Titiakarawongse and Sirapat Boonkrong*
Institute of Digital Arts and Science, Suranaree University of Technology, Nakhon Ratchasima, Thailand

* Corresponding author. E-mail: sirapat@g.sut.ac.th DOI: 10.14416/j.asep.2023.01.001
Received: 3 September 2022; Revised: 26 October 2022; Accepted: 29 November 2022; Published online: 4 January 2023

Abstract
Password-based authentication is still the most widely used authentication method today. Unfortunately, passwords are the main culprit leading to cyberattacks. This study examines the behaviors of young people towards password generation and usage. The young people will ultimately become the future for society. An online survey with a sample of 265 respondents aged 10–24 was conducted between April and August 2021. The research utilized descriptive statistical analyses and compared the responses from young people with older people. The results suggest that although the survey participants seemed to have basic knowledge of creating complex passwords, they still possessed some aspects, which could lead to being a cyberattack target. This preliminary study provides information and increases awareness for policymakers and educators in such a way that it could be used to create an educational program on the importance of managing passwords securely. In addition, the study provides insights into the password management of young people between the ages of 10 and 24.

Keywords: Computer security, Password, Password behaviors, Password management, Young people

1 Introduction

In today's Internet-based or digital environment, it is essential for any computer or information system to be able to identify any individual or entity that attempts to enter and use the system. Therefore, access control mechanisms, i.e. authentication, cannot be overlooked. Although there are several authentication methods [1], such as passwords with something-you-know, something-you-have and something-you-are, (which are all under the something-you-know category) that appear to be the most widely used mechanisms and they play an important role in modern life. For example, they are used for logging into email accounts, mobile banking accounts, organization networks and personal devices.

It is clear that strong and secure passwords should be selected to protect personal accounts and information. Unfortunately, people do not always choose strong and secure passwords. Many people still generate weak and easy-to-crack passwords [2], [3] with the most common ones including "123456", "123456789", "password", "iloveyou" and "Nothing." Many are opting for bad practices for password usage, such as writing their passwords down on a post-it or reusing their passwords across many different accounts.

Both choosing weak passwords and exhibiting bad password practices have led to many high-profile cyberattacks. Cyberattacks began as early as 1998 when the Computer Emergency Response Team (CERT) [4] reported an incident in which there was a leak of almost two hundred thousand passwords and close to fifty thousand of them were cracked. In 2009, one of the largest credential leakages up to that point took place in a major password breach of a website [5]. In 2016, it was reported that almost four hundred million accounts from two well-known social networking sites were hacked and the passwords were leaked. Interestingly and frighteningly, the report suggested that a lot of the leaked passwords had been generated from words in the dictionary and simple patterns of numbers. For example, password with "12345" appeared more than two hundred thousand times and "password"

appeared almost eighteen thousand times [6].

Many organizations and researchers have attempted to help users generate stronger passwords through their password composition policies [7], [8], which not only specify the minimum length but also require users to include specific types of characters and numbers in their passwords. Some have suggested the use of a password manager [9], whose purpose is to help users generate stronger passwords and eliminate password reuse.

While these policies may help improve the security of passwords, they make it more difficult and complex for users to memorize their own passwords. Moreover, nowadays many users are overwhelmed with the number of accounts and passwords they need to use daily, which is largely true for adults and older people whose personal data are subjected to adversarial behaviors [10]. This has led to a question of trying to understand the attitudes and behaviors of users, especially younger generation users, towards their password generation and usage.

The World Health Organization (WHO) defines the term "young people" as those who are between 10 and 24 years old [11]. From this range, young people are students in school and higher education as well as the newly graduated students. They were the focus of this research because they will be the main workforce in the future. It is thus necessary to study and understand their attitudes and behaviors about password generation and usage so that proper awareness, education and even technologies can be designed and put in place to complement the results of this research.

In this research, as a preliminary study, a survey was carried out with over two hundred and fifty participants, two hundred of which were in the young people category as defined by WHO. The rest were in the older category, which was used for a comparative analysis. In general, surveyed participants reported that they had more than one account with the number of passwords not matching to the number of accounts. Many participants have adapted to the advice of generating more complex passwords. A few responsed that they were aware of how to ensure their password security through multi-factor authentication and password managers, while many had never heard of these techniques before.

1.1 *Literature review and related work*

There is a large amount of literature regarding various aspects of password-based authentication. In this section, however, only those that are relevant to our study, such as password security, password management [12] and those looking at perceptions related to passwords, are discussed [13]–[15]. The objective of this work is to build upon the existing work by looking specifically at the younger generation of people and what their perspectives are toward password generation and usage.

1.1.1 Password security

Passwords are the most used method of authentication due to their convenience and low cost. Unfortunately, the strength of password-based authentication mechanisms relies heavily on the strength of the passwords themselves. Weak or easy-to-crack passwords have presented security problems over the years. Having seen this opportunity, attackers have created and applied several different techniques to crack passwords [1]. Some of the more popular ones are as follows.

The first technique is known as a brute force attack, which is when an attacker attempts all possible passwords until the correct one is found. The second one is called the password dictionary attack. This occurs when a list of commonly used passwords is created and stored in a database. Only the passwords in that database or dictionary are tried and used when an attacker attempts to log into a system as someone else.

Consequently, a couple of approaches have been proposed to help to measure the quality and strength of passwords. The first approach was password entropy, which was first introduced by Shannon [16]. Password entropy was defined as the statistical distribution of information, which measured the randomness of the content. This work pioneered password quality measurement, which other researchers built upon. This led to research by Ma *et al.* [17] who suggested that a password should be composed of upper-case letters, lower-case letters, numbers and special characters, which has become a guideline for a more secure password generation method.

Ma *et al.* [17] proposed another approach for evaluating the strength of passwords known as the

effective length. Effective length is an extension to the basic counting of the number of characters in a password. It was suggested that a password complexity index (or a specified value for each character) should be applied to the password so that the effective length, rather than the actual length, could be computed.The two password security metrics in password entropy (components within a password) and password length have, therefore, become parts of this survey, specifically for the password composition stage.

1.1.2 Password management

Passwords are considered the first line of defense for computer and information systems [1]. They help to reduce the risk of unauthorized access. Therefore it is possible to lower the chances of being compromised by generating strong passwords and adopting good password practices. The problem is that users are now facing a lot of burdens in managing their passwords, namely password creation and usage.

Previous studies found through a survey that some people possessed over twenty accounts and hold as many if not almost as many passwords [13]–[15], [18], [19]. Some of these people even use all these accounts and passwords every day. One research suggested that almost half the people participating in the study logged into their accounts over forty times a week [20]. Even though, these studies focused on working aged people they still provided noteworthy statistics for password management behaviors. In contrast, our research focused on the behaviors of young people.

Two survey research [12], [21] were conducted with approximately three hundred people and twenty-seven people, respectively, in workplaces, people appeared to have varying methods for creating passwords. The studies using descriptive analysis, several statistical analyses, such as Pearson's chi-squared test and significance level $\alpha = .05$ showed that although many organizations and websites had password policies that required users' passwords to meet some specific criteria, people still tended to create their password by choosing something that was easy for them to remember. This usually made them vulnerable and easy to guess. Yet, there were people still conforming to better password creation strategies by combining various types of characters and numbers in their passwords [7].

Another study [22] was conducted on several hundred thousand leaked passwords to understand the password usage behaviors of users. It was found that 43–50% of users frequently reused their passwords across multiple accounts. The more passwords that users needed to generate and the more accounts they possessed, the more likely they were to reuse passwords. This behavior is worrying because it is the main cause of a password-related attack known as credential stuffing. This occurs when a user's password is known by an attacker, who will then try to use the same password to log into other accounts belonging to the same user [1]. Another study has gone as far as saying that using the same password for many accounts was like having one key that can unlock many doors [23].

Many organizations' password policy forces users to change their passwords every thirty to sixty days [18], however this is not agreed to all [24]. It had been believed that by changing passwords every so often, attackers would find it more difficult to compromise them. However, there is suggestion to users who frequently change their passwords, that the security of already-strong passwords would be reduced [24]. Regarding to this issue, a study observed that users tended not to change their passwords based on their own decisions. They would only do so when they were forced to in the case of a breach or after forgetting their password [25].

In the context of password recall and memorability, users applied different approaches ranging from relying on their memory to writing down the passwords on pieces of paper or in a note application on their computing device. It was also found that the use of password managers was not common, even though it was a recommended approach [9], [12]. Ray *et al.* [9] conducted interviews with 26 older adults (over 60 years old) to understand the adoption of password managers. It turned out that many had fears of a single point of failure and were worried about the idea of having some entity controlling their private information.

The existing literature studied various aspects of user behaviors towards passwords, but there had not been many that specifically looked at how young people worked on password management. Helkala and Bakås [26] conducted research among employees in Norway

and found that password education and guidance were inadequately given, leading to outdated behaviors. In 2021, however, there was one study that provided an attempt to understand what children thought about passwords [27]. This article appeared to be the first to conduct a survey of third to twelfth graders across the USA. The authors found that children had fewer passwords than adults and had mixed perceptions about passwords. Moreover, their study showed that there were some behaviors that would lead to a lack of security in their passwords. Having said that, our work is different from Theofanos *et al.*'s work [27] in three ways. The first is that our participants were from different parts of the world. Secondly, although the majority of our participants were young, the participants were from a broader range of age groups, namely those who were aged between 10 and 24 years old, as defined by WHO. Third, our coverage of perceptions towards passwords is different. That is, the work of Theofanos *et al.*'s put an emphasis on understanding passwords and password creation whereas our study focused on different aspects, namely password creation, password usage and password security improvement strategies.

2 Materials and Methods

2.1 *Research framework*

The conceptual research framework is depicted in Figure 1. The research began with an online survey designed to investigate perceptions and behaviors of young people towards password creation, usage, and security. The survey was then distributed so that data could be collected and analyzed using descriptive statistical analyses. The perceptions and behaviors of young people towards password management were to be identified afterward.

2.2 *Survey design*

This section describes how the online survey was designed and what it consists of. In order to understand the habits of young people on various aspects of password management, the survey was divided into four parts.

First, the general demographic section required participants to indicate their age group. Even though the focus of the research was on young people aged between 10 and 24, it was important to know because some participants were older, and we could use this information to compare the demographic groups. Second, the password creation section included four questions. The questions probed into general password practices such as whether they used their name or telephone number, used letters only, used numbers only or whether some specific practices were followed. In addition, they were asked about the size of their passwords.Third, password usage looked at how participants used and maintained their passwords. The participants were asked about the number of accounts and passwords they owned, how often they changed their passwords as well as what their password recall strategies were.The final part examined whether participants knew of any additional methods that could improve the security of their passwords. The questions in this part asked about multi-factor authentication and password managers.In total, the online survey used to conduct the research contained fourteen questions. We believe that these fourteen questions were adequate for accomplishing our objective to learn about young people's perceptions towards personal password management.

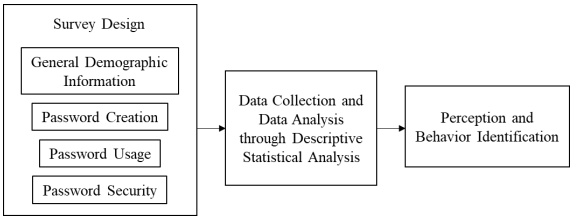

Figure 1: Research Framework.

2.3 *Data collection*

We distributed the online survey on websites including Reddit (https://www.reddit.com) and SurveyTandem (https://www.surveytandem.com). Currently, Reddit has over fifty-two million active users daily on their website. Our survey was posted in the Take My Survey community, which is a broad and non-specific community so that we could get a diversity of people to respond to the survey. SurveyTandem is a platform for finding survey respondents, albeit by answering other people's surveys in exchange. We felt that these survey sites were good platforms to gather responses from mixed backgrounds.

The main source of survey data was via emails. Our research focused on and required responses from people between the ages of 10 and 24, according to WHO's definition of young people. It was, therefore, necessary to target specific respondents and emails were a convenient tool to do so. For this purpose, emails were sent to students in schools and universities in Japan, the UK and various parts of Thailand. This way the data from the target age group and the diversity of respondents could be collected. From these platforms and methods, we were able to gather 265 responses.

It should be noted that the online survey was written in English, which means that many participants were not able to take the survey in their native language. However, the survey questions only consisted of basic English words and phrases, which we believed would be understandable to the participants.

2.4 *Data analysis*

In this section, we describe the analysis of the collected data. Due to the structure and content of the survey, quantitative analyses were carried out in this research. Before carrying out any statistical analyses, it was necessary to clean the collected data so that only usable records remained. By looking at the data obtained from the survey, it was obvious that there were some responses that appeared fraudulent and infeasible. By removing the unusable responses, the validity of our analyses would be improved.

For this research, seven responses were excluded from the study, which accounted for 2.64% of all the collected responses. The reason for exclusion was that there were five participants who said they owned more passwords than the number of accounts they possessed, which appeared to us as infeasible since our study was interested in the current status of password management only. In other words, any old or no-longer-used passwords associated with each account should not be considered. The other two participants just wrote some random characters as their responses to several survey questions. Thus, their responses could not be used in the analyses at all. As a result, 258 responses remained and were included in our analyses.

A descriptive statistical analysis was applied to provide an overview of the survey data. This was done so that the number of responses to each question could be expressed, and basic comparisons between the responses from young people and the older counterparts could be performed. In addition, a significance level $\alpha = .05$ was used in the analyses of the obtained results.

2.5 *Limitations*

There is one limitation to our research that we would like to point out. Even though the data were collected through different online platforms, a large proportion of the obtained data was from Thailand, with few responses from other parts of the world. Therefore, the participants of the survey may not reflect the attitudes and behaviors of the world population. Nevertheless, as a preliminary study, we still believe that our study and findings can provide a better understanding of young people's attitudes, perceptions and behaviors towards their password creation, usage, and management in general.

3 Results and Discussion

Our research focused on understanding how young people generated, used, and managed their passwords. As a result, our online survey included questions that would provide insight into young people's password-related attitudes, perceptions, and behaviors. This section is divided into four parts, which reflect our survey questions and attempt to answer the research questions. These parts include the general demographics of the research participants, password creation, password usage and password security improvements.

3.1 *Research participants*

Although the aim of the research is to understand how young people (10 to 24 years old) behave towards password management, some participants were older. The data from people who were 25 years old and over allowed further analyses of the obtained data.

In total, we were able to collect 265 responses, but it was necessary to remove 7 responses. The sample size used in this study followed precedent from previous studies, which had the following sample sizes: [30] had 231 survey participants, [13] had 240 survey participants, [12] had 339 survey participants, and [17] had 45 survey participants, while [21] carried out 27 interviews. Although the country of origin was not collected as a part of the survey, we were

able to determine from the survey distribution method (emails) and responses (time of response) that most of the research participants were from non-Western countries. The demographics of the research participants are described in Table 1.

Table 1 shows that 199 young people participated in the study, which accounted for 77% of all participants. Out of the 199 young people, 8 were between 10 and 14 years old, 74 were between 15 and 19, and 117 were between 20 and 24. In addition, there were 59 respondents who were 25 years old and older.

Table 1: Demographics of research participants

Gender			Age		
Sex	**Number**	**%**	**Age Groups**	**Number**	**%**
Male	129	50.00	10–14	8	3.10
Female	127	49.22	15–19	74	28.68
Others	2	0.78	20–24	117	45.35
			25 and over	59	22.87

3.2 *Password creation*

For the analyses of the password creation section, we divided it into three parts: password creation strategies, password components and password size.

3.2.1 Password creation strategies

This part shows the strategies that the participants reported to have used when creating their passwords. In general, there were seven techniques that were adopted for password generation. Figure 2 shows the distribution of the participants' reported password creation methods.

The password creation techniques gathered from our study included using people's names, places' names, birthdates, phone numbers, words in English dictionary, and using a password generator. Other methods mentioned by the participants included the use of student or national ID numbers, favorite characters from cartoons or films, and words from other languages (typing with an English keyboard). The number of password generation methods found in our study appeared to be more than that from the research by Habib *et al.* [12], which indicated that there were three main techniques for password creation: using English words, using names, and adding either numbers or symbols. Our study was different from the work

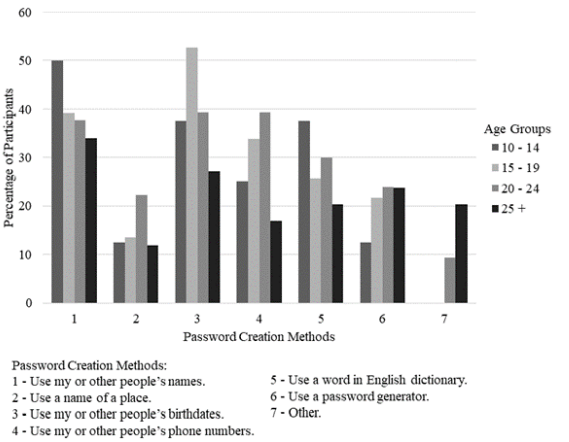

Figure 2: Percentage distribution of participants' password creation methods.

of Theofanos *et al.* [27] where the correspondents' passwords were given to the participants by the school, made by parents or with parents' help, or made by the participants themselves. No other details were given in their study.

There are a few things worth pointing out from the obtained results. First of all, creating a password by including a person's name was popular among young people with 50% of the 10 to 14 years old participants admitting to using this technique. In addition, 39% and 38% of participants who were between 15 and 19 years old and between 20 and 24 years old, respectively, included either their own or someone else's name in their passwords. The obtained percentages appeared to align with the results from Habib *et al.* [12] and Ur *et al.* [28] who also found that using names was the most common password creation technique. Additionally, 34% of the older participants (25 years old and older) used this method to generate their passwords.

Secondly, including someone's date of birth in a password was another popular method. From Figure 2, it can be seen that 53% of the 15 to 19-year-old participants used either their own or other people's date of birth as a part of their passwords. This was followed by the 20 to 24 and 10 to 14 years old groups with 39% and 38% of participants using this technique, respectively. In contrast, this method was only used by 27% of the older participants. Hence, there is a statistically significant difference ($\alpha = .05$) between the young people (10–24 years old) and the older ones (25 and over). Another password creation technique

was the inclusion of phone numbers. Compared with the older age group of those at least 25 years old, the percentage of young participants who chose to include phone numbers for password generation was significantly higher ($\alpha = .05$). In other words, 32.70% of the young correspondents reported that they had included either their own or someone else's phone numbers in their passwords. In contrast, only 17% of the older age group reported having done the same.

The next password generation strategy discovered through the survey was in agreement with the research by Habib *et al.* [12], Ur *et al.* [28] and Bryant and Campbell [15]. This technique involved using words from an English dictionary as a part of the participants' passwords. Habib *et al.* [12] found that approximately 41% of all participants used English words in their passwords. However, the percentage in our research was not as high. On average approximately 31.03% of the young participants (10 to 24 years old) reported that they would include words from an English dictionary in their passwords. The number was even lower in the older age group with only 20.34%. Having said that, this is another method that gives a statistically significant difference ($\alpha = .05$) between young people and their older counterparts.

The least popular password creation method involved the inclusion of place names. Only 16.08% of the 10 to 24 years old and only 12% of the older age group reported using this method. The practice of including place names in passwords was something revealed only in our study and had never been mentioned in previous studies.Moreover, there were other practices reported by some of our participants. It was found that the percentage of the older age group (20.34%) who had used other methods for creating passwords was significantly higher ($\alpha = .05$) than for the younger age groups (3.13%) from which only those between 20 and 24 years old reported to have used other techniques. Some methods mentioned by the participants that fell into this category included the use of student or national ID numbers and words from other foreign languages (using an English keyboard).

3.2.2 Password components

The second part of the password creation section reported what components the participants had included or would choose to include in their passwords. From

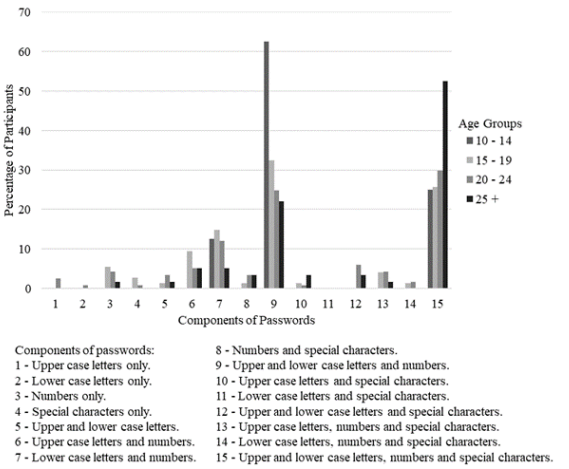

Figure 3: Percentage distribution of participants' password components.

the obtained data, there were fifteen possible ways or combinations of components that were chosen by the participants. These fifteen different combinations can be seen in Figure 3, which also shows the distribution of the participants' chosen components in their passwords.One piece of information from Figure 3 we thought was worth noting was that the combination of lower-case letters and special characters was not the choice of any participants from any age group at all.

Figure 3 also shows that the 20 to 24 age group was the only group that would create or had created their passwords using only either upper-case letters or lower-case letters, albeit with only 2.60% and 0.90%, respectively.

Numbers-only passwords, as suggested by the data, were chosen by a handful of participants in the 15 to 19 years old age group (5.40%), the 20 to 24 age group (4.30%) and the 25 and over age group (1.70%). Nobody from the 10 to 14 age group chose or had chosen only numbers as their passwords.

Special characters-only passwords were another interesting technique, which only used by participants from the 15 to 19 and 20 to 24 years old age groups, with 2.70% and 0.90% of the participants using this method, respectively. On average, it appeared that this special character only method was the least popular among our participants.

The combination of lower-case letters, numbers and special characters was another method chosen only by the participants ages 15 to 19 and ages 20 to 24, with 1.40% and 1.70% of each age group,

respectively. The other type of passwords chosen by these two age groups was using a combination of upper-case letters, lower-case letters and special characters. This combination was chosen only by those in the 20 to 24 and 25 and over age groups, with 6% and 3.40% of the participants from each age group, respectively.

One type of combination chosen by all age groups was a combination of lower-case letters and numbers. On average, this method was significantly more popular ($\alpha = .05$) among young participants (10 to 24 years old) than the older ones (25 years old and over). That is, 13.11% of the participants in the 10 to 24 age group reported to have used this combination, while only 5.09% of the 25 years old and the older group had used this technique.

There were two other types of combinations that were chosen by all age groups and appeared to be the two most popular choices for each age group. The combination of the upper-case letters, lower-case letters and numbers was used by a significantly higher number ($\alpha = .05$) of the young people (10 to 24 years old), while the combination of all types of characters in the upper-case letters, lower-case letters, numbers and special characters was significantly more popular ($\alpha = .05$) for the older age group (25 years old and over). These two types of combinations also gave an interesting result, which can be described as follows.

The number of participants choosing upper-case letters, lower-case letters and number combinations evidently decreased as the ages of the participants increased. In other words, the majority (63%) of the participants from the 10 to 14 age group suggested that they would use or had used this method when creating their passwords. This number went down for those ages 15 to 19 years old (32%) and 20 to 24 years old (25%). The oldest group (25 years old and older) recorded the lowest percentage at 22%.

On the other hand, the combination of all types of characters presented the opposite trend. That is, as the ages of the participants increased, the number of participants choosing to use this method also increased. The data showed that 25% of the 10 to 14-year-olds, and 26% and 30% of the participant's ages 15 to 19 years old and 20 to 24 years old, respectively, reported to have created their passwords using this combination. It was obvious from Figure 3 that the majority or 53% of the older age group of 25 and over would choose or had chosen this type of combination for their password creation.

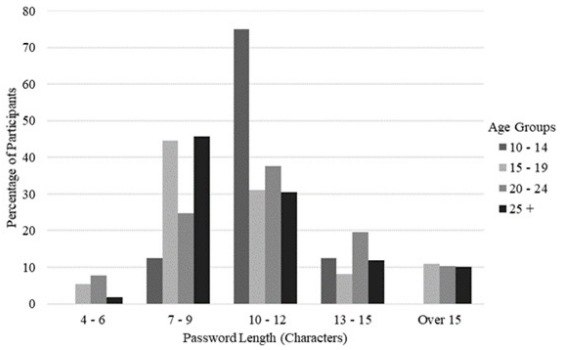

Figure 4: Percentage distribution of participants' password sizes.

It appears that the two most popular password development techniques complement one another. Once the participants became older, the components within their passwords and their combinations became more complex. This suggests that awareness, education, and experience are needed to help people generate more complex passwords. Moreover, the data we collected and analyzed were similar to the study by Habib *et al.* [12], who also found that 59% of their participants would add numbers to their passwords, and 32% would add special characters to increase the complexity. However, Habib *et al.* [12] did not provide any details of how the results were distributed among different age groups.

3.2.3 Password size

The final part of the password creation section is the password size. This part reports on the average password size of our research participants. In general, the responses from the participants were grouped into five size ranges. They were the passwords whose sizes were 4–6 characters, 7–9 characters, 10–12 characters, 13–15 characters and over 15 characters. Figure 4 shows the distribution of our participants' reported password sizes.

It is observed that all password sizes were chosen by all age groups, except for the 4–6 character and the over 15-character passwords, which were not the choices of the participants belonging to the 10 to 14 age group. The 4 to 6 character passwords also represented the smallest numbers of participants with over 15

character passwords having the second lowest numbers of participants. What we found from our survey data aligned with the results from Bryant and Campbell's work [15], which also stated that passwords length between 1–6 characters and between 11 and 26 characters represented the smallest proportions.

The data collected from the survey revealed that for 25 years old and older, passwords consisting of 7– 9 characters were the most popular choice with 45.67% of the participants from that group having passwords of this size. This is an obvious difference from the young people (10 to 24 years old), with approximately 27.29% choosing this password size. That is, there is a clear statistically significant difference ($\alpha = .05$) between these two age groups.

Passwords between 10 and 12 characters provided a very noticeable point to be discussed. Figure 4 shows that approximately 75% of the 10 to 14-year-old participants had created passwords of this size, which was significantly higher ($\alpha = .05$) than any other age group. However, on average, 47.90% of the young participants (10 to 24 years old) had created passwords whose sizes were between 10 to 12 characters long, compared with only 30.51% of the older participants. Finally, the 13 to 15-character passwords were created by 13.42% of young participants. The number for the older group was not significantly different with 11.86% of them having created and used passwords of this size.Those between 10 and 24 years old tended to create passwords sized between 10 and 12 characters, compared with the older participants, almost half of whom suggested that their passwords were between 7 and 9 characters long.

3.3 *Password usage*

The analyses of the password usage section are divided into three parts. It includes a comparison between the number of accounts and the number of passwords (or password reuse), how the participants said they recalled their passwords, and what their password update behaviors were.

3.3.1 Password reuse

Our survey did not ask the participants directly whether they had used the same passwords for multiple accounts. What we did instead was ask about the number of password-protected accounts and the number of passwords they owned. The data are displayed in Figure 5 and Figure 6, respectively.

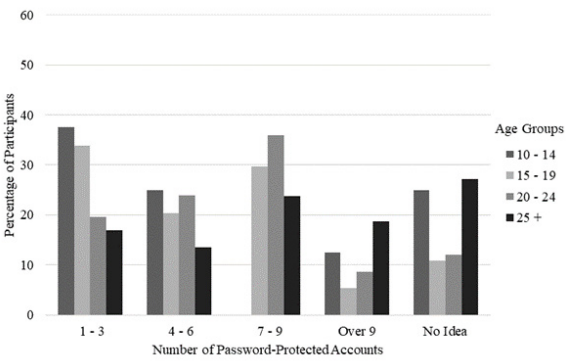

Figure 5: Percentage distribution of the number of password-protected accounts owned by participants.

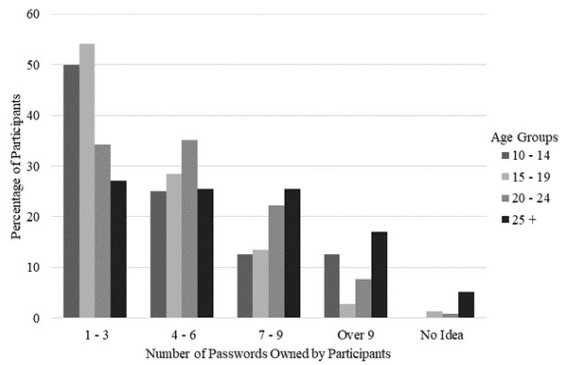

Figure 6: Percentage distribution of the number of passwords owned by participants.

Whether or not there was password reuse can be observed by comparing the data in Figures 5 and 6. For the number of password-protected accounts, on average 30.31% of the young participants owned between one and three password-protected accounts, while 16.95% of the participants 25 years old and over owned the same amount, which made the number for the young people significantly higher ($\alpha = .05$) than that of the older ones. The young participants aged between 10 and 24 years old who owned between four and six accounts accounted for 23.07%, whereas the number was 13.56% for those 25 years old and over. The number of young participants that owned between seven and nine accounts slightly decreased to 21.88%. However, this number increased for the older participants at 23.73%.

The number of participants both young and old owning over nine password-protected accounts went down to 8.82% and 18.64%, respectively. What we can observe here is that the older participants seemed to have significantly more accounts ($\alpha = .05$) than the younger people. Our data also revealed that significantly more people ($\alpha = .05$) in the older age group had no idea how many accounts they owned in contrast to the young ones (10 to 24).

Let us now look at the number of passwords reportedly owned by the participants in Figure 6. Ideally, the number of passwords owned by the participants should match the number of accounts they possessed. However, the difference between Figure 5 and Figure 6 can be spotted straightaway.

It appears that the graph in Figure 6 is left-hand heavy. In detail, on average 46.08% of the young participants (10 to 24 years old) owned only between one and three passwords, while 27.12% of the 25 years old and older owned the same amount. There was, therefore, a statistically significant difference ($\alpha = .05$) between the two groups. This was in stark contrast to the data shown in Figure 5, where only approximately 30.13% of the young people and 16.95% of the older ones owned between one to three accounts. Therefore, this implies that many of our survey participants had conducted a fair amount of password reuse, with those who were between 10 and 24 constituting a higher number than the older participants.

Other studies, including those by Habib *et al.* [12] and Bryant and Campbell [15], also reported that there was a moderate amount of password reuse. Habib *et al.* [12] found that almost 50% of their participants had reused their passwords, whereas Bryant and Campbell's data showed only around 25%. Although our research found some patterns for password reuse, the number did not seem to be as high. Moreover, our study investigated the difference between different age groups while other researchers only studied the behaviors at workplaces and email usage.

In addition, Figure 6 shows that the percentage of participants decreased as the number of possessed passwords increased. This is especially true for young participants. On the other hand, there was only a slight decrease in the percentage of those who were 25 and older as the number of passwords increased. A significantly higher ($\alpha = .05$) percentage of those 25 and over said they possessed over nine passwords.

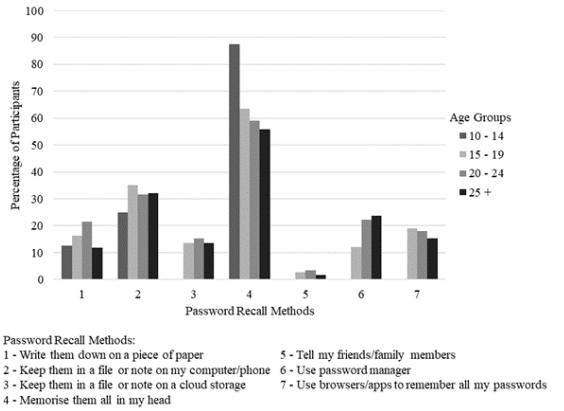

Figure 7: Percentage distribution of participants' password recall methods.

3.3.2 Password recall

This part studied how our participants recalled their passwords. In general, there were six password recall techniques reportedly adopted by the participants. Figure 7 shows the distribution of our participants' password recall methods.

It is clear from Figure 7 that the most popular password recall method among our participants was memorizing the passwords. The survey data revealed that on average 70% of the young participants chose to adopt this method for their password recall. In contrast, only 55.93% of those 25 and over chose to memorize passwords. It is noted that more than half of the participants from all age groups reported recalling passwords from memory. However, the pattern shown in Figure 7 revealed that as the participants got older, it became less likely that they would still use memory as their password recall method.

This particular result of our survey appeared to align with that of Habib *et al.* [12] and Theofanos *et al.* [27] who also suggested that the most common password recall technique used by more than half of their research participants was memorizing the passwords. However, our research provided more insight in that a significantly higher ($\alpha = .05$) number (70%) of those aged between 10 and 24 years old memorized their passwords rather than using other methods.

We combined the survey results of methods (methods 1–3 from Figure 7) for writing down passwords to obtain the following. The note-taking method was on the whole used by 56.92% of the young

participants and 57.63% of the 25 and over age group. This means that on average there was no significant difference between young people and older people in adopting this password recall strategy. Although our study recorded over half the participants using the note-taking method, our numbers were not as high as the survey done by NIST [29], which found that over 80% of their survey respondents stored their passwords either on paper or electronically. However, the results from [27] suggested that only 38.83% of their participants wrote down passwords.

There were two other recall techniques used by the participants. One was using dedicated password manager software (category 6). Overall, password managers were used less by the young participants (11.46%) compared with 23.73% of the 25 and over age group. Thus, it could be concluded that the use of password managers increased as age increased.

Making use of the Web browser's ability to remember passwords (category 7) was a choice for a few of our participants, where the percentages from the young correspondents and older age groups were not significantly different. Furthermore, the use of a Web browser's password remembering function had a downward trend as the participants became older.

3.3.3 Password update

This part describes how often, if at all, our participants changed or updated their passwords. Figure 8 shows the distribution of the participants' password update frequency.

Our data revealed a similar behavior pattern for both young participants who were between 10 and 24 years old and older participants aged 25 and over. That is, there were more participants who admitted to never changing their passwords than any other frequencies (on average, over 32% of both age groups). The second most common response was to update their passwords once every ten months and over, where the data obtained from the survey were almost the same for both the young (21.27%) and older participants (22.03%).

Furthermore, it can be seen in Figure 8 that there was an upward trend in updating passwords at a frequency of once every five to seven months. It appears that the number of participants who updated their passwords once every five to seven months increased as age increased. Also, it can be seen that significantly more people ($\alpha = .05$) from the older aged group who tended to use their password for this same duration before changing them.

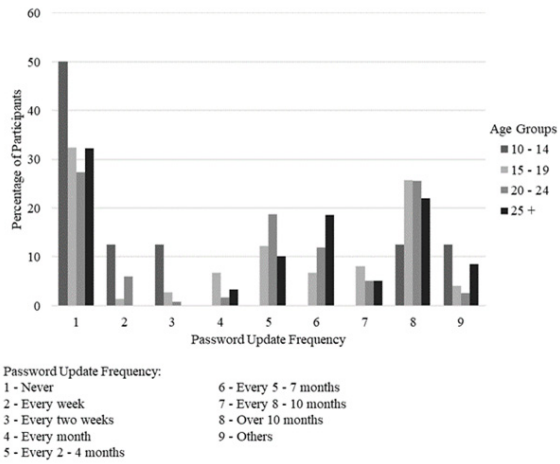

Figure 8: Percentage distribution of participants' password update frequency.

Other update frequencies were only represented by a small number of participants. For example, only 2.89% of the young people and 3.39% of the older people said that they changed their password every month. None of the participants from the older age group reported changing their passwords every one or two weeks, while 6.61% and 5.32% of the young participants reported doing so, respectively. In addition, both the younger and older participants reported that there were events that would trigger them to change their passwords. These triggers included being alerted to unusual activity on their account and when they forgot their passwords. This finding appears to be aligned with the previous work of [25], which also suggests that people tend to change passwords when there is a security alert trigger.

3.4 *Password security improvement*

The final section of the results and analysis is concerned with awareness of security improvements in passwords. The participants were asked whether they were familiar with or had used two-factor authentication and password managers, which could assist them with having a more secure authentication process. Figure 9 shows the number of participants who had used two-factor authentication.

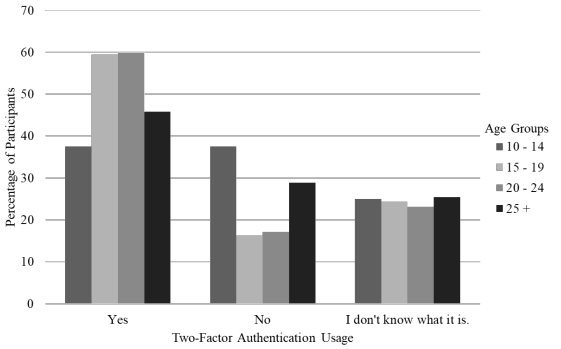

Figure 9: Percentage distribution of participants' usage of two-factor authentication.

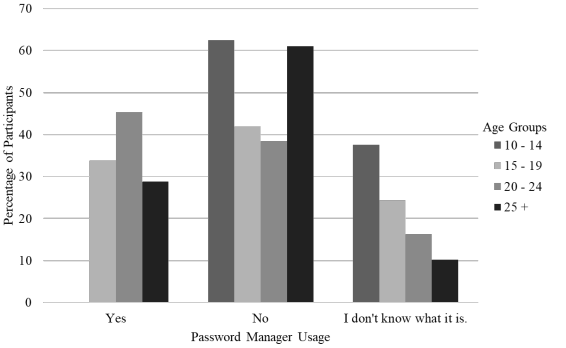

Figure 10: Percentage distribution of participants' usage of password managers

The survey data revealed that the number of young participants (52.26%) who had used or were using two-factor authentication was higher than for the older group (45.76%). Our data represented a very different value from the research by Ion *et al.* [30] who found that only 20% of their participants had used two-factor authentication to help them stay safe. This implies that over time a higher percentage of younger people were willing to adopt new technology that makes their passwords more secure.

Our data showed that 37.5% of the youngest participants seemed to know of two-factor authentication but chose not to use it. This number was significantly different ($\alpha = .05$) between the 15 to 19 and 20 to 14 age groups with values of 16.22% and 17.09%, respectively. Meanwhile, 28.81% of the older participants (25 and up) had decided not to use two-factor authentication even though they knew the technology existed.

A similar amount of young and older participants admitted that they had no idea what two-factor authentication was with 24.13% and 25.42% being unaware, respectively.In addition to asking the participants about two-factor authentication, they were also asked about their password manager usage. Figure 10 shows the number of participants who had used this type of system.

For password managers, it was interesting to see that the participants from the 10 to 14 and the 25 and over age groups showed almost the same amount at 62.50% and 61.02%, respectively, for knowing of password managers but not using them. However, if we looked at the average (47.62% for the 10 to 24 years old participants and 61.02% for the older ones), we would see that although they knew what a password manager was, more participants from the older age group chose not to use it. Although the participants in our older group were relatively younger than those in the study of Ray *et al.*'s [9], which focused on users aged 60 and up, they appeared to follow the same pattern in choosing not to use password managers. That is, the respondents from both our study and Ray *et al.*'s study suggested that substantial numbers of participants used alternatives when it came to password management and recall, one of which was the note-taking method as described in the Password Recall section. However, Ray *et al.* provided several reasons as to why older people did not use password managers, which included the disruptive nature of password managers, to which some said they were "time-wasters", they lacked self-efficacy, and they lacked trust in the technology.

There were zero participants from the 10 to 14 age group that reported having used or using a password manager, which led us to an average of 26.36% of the younger participants who said that they were using a password manager at the time of the survey. This was to be compared with 28.81% of the older survey respondents who reportedly were using the technology at the time. These numbers showed an improvement from the study of Ion *et al.* [30], which suggested that only 12% of general users had used a password manager. This again suggests a positive development in technology adoption in all age groups as the year's progress.

Finally, there were participants who admitted that they had not heard about password managers prior to the survey. This accounted for 26.02% from the young age groups (10 to 24 years old) and 10.17%

Table 2: Summary of statistically significant differences in password management behaviors between younger and older participants

Password Management	Behaviors	Responses	Age Groups		*p*-value
			10–24	25+	
Password Creation	Creation Strategy	Use birthdates	43.17%	27.12%	0.0087
		Use phone numbers	32.70%	16.95%	0.0050
		Use words from dictionary	31.03%	20.34%	0.0418
		Others*	3.13%	20.24%	0.0001
	Components	Lower-case letters, numbers	13.11%	5.09%	0.0240
		Upper and lower-case letters, numbers	39.91%	22.03%	0.0030
		Upper and lower-case letters, numbers, special characters	26.86%	52.54%	0.0001
	Password Size	7–9 characters	27.29%	45.76%	0.0033
Password Usage	No. of Accounts	1–3 accounts	30.31%	16.95%	0.0131
		Over 9 accounts	8.82%	18.64%	0.0217
		No idea (cannot remember)	15.93%	27.12%	0.0271
	No. of Passwords	1–3 passwords	46.08%	27.12%	0.0027
		Over 9 passwords	7.63%	16.95%	0.0224
		No idea (cannot remember)	0.74%	5.09%	0.0336
	Password Recall	Memorize passwords	69.99%	55.93%	0.0197
		Use password manager	11.46%	23.73%	0.0114
	Password Update	Every week	6.61%	0.00%	0.0045
		Every two weeks	5.35%	0.00%	0.0095
		Every 5–7 months	6.24%	18.64%	0.0039
Password Security Improvement	Password Manager	No idea what a password manager is	26.02%	10.17%	0.0018

*means using national identification number, words in other languages (typed with English keyboard), favorite characters from books or films, and favorite films.

from the 25 and over age group, which means that significantly more young people ($\alpha = .05$) had no idea what a password manager was. These data represented a promising trend by showing the fact that the number of participants not knowing what a password manager is decreased as age increased.

Overall, our research revealed that there were bad practices adopted by our participants, in particular the younger ones. Young participants reported composing their passwords using names, birthdates and telephone numbers more often than the older participants. Furthermore, the participants who were between 10 and 24 tended to create less-complex passwords than their older counterparts. A significantly higher numbers of young participants seemed to possess a fewer numbers of passwords, which suggested that they reused passwords more often than the older age group. In terms of improving password security, there were no significant differences between the young and older participants when it came to two-factor authentication. However, with password managers, the percentage of younger people who had never heard of password managers was significantly higher than that of older people.

To gain more insight, especially for comparison between younger and older participants, Table 2 summarizes the password management behaviors, namely password creation, password usage and password security improvements that are significantly different [31] (p-value < 0.05) between young participants (10 to 24 years old) and older participants (25 years old and over) based on the number of responses from each group.

4 Conclusions

The objective of the research was to assess the perceptions and behaviors towards password generation and usage among young people. As a byproduct of data collection, the obtained data allowed a comparison

between young and older people. The focus of the research was on young people (WHO having defined young people as people aged between 10 and 24) because they were seen as future citizens and the future workforce. It would, therefore, be imperative to understand their behaviors. As a result of the research, we are better prepared to encourage better security strategies for future generations. Moreover, the research was conducted to gain insight into the three main aspects of passwords: password generation, password usage and password security improvements.

Our research, which obtained information from a broad group of participants, found that the people who were between 10 and 24 years old were more likely to adopt bad practices for password generation and usage than their older counterparts, albeit there were similarities in some respects.

While we feel that the obtained results are useful, they should admittedly be viewed with caution due to the limited numbers of respondents. However, despite the limitation in the number of participants, we still believe that the data obtained in this study offers new insights and valuable information. Having said that, in future research, it would be interesting to look at other sources of data such as from social media so that the amount of data could be increased.

For our final point, we would like to emphasize that our research was anchored in three main aspects of password perceptions and behaviors of young people, namely password creation, password usage and password security improvement. As such, the obtained results are intended for policy makers, educators, and practitioners so that they become more aware of the problems that exist for the younger generation. The results from this study, such as the insecurity of password reuse and the adoption of two-factor authentication and password managers, could be included in educational materials. Consequently, it is hoped that the data obtained from this study would form the basis for offering improved educational programs focusing on adopting better passwords and authentication practices, so that the risk of cyberattacks could be reduced in the future.

Acknowledgments

We extend our sincere thanks to all who participated in the survey.

Author Contributions

C.T.: Questionnaire generation, research design, reviewing and editing the manuscript; S.B.: Research design, data cleansing, data analysis, writing the original and revised drafts. All authors have read and agreed to the published version of the manuscript.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S. Boonkrong, "Methods and threats of authentication," in *Practical Cryptography Methods and Tools*. Berkeley, California: Apress, 2021, pp. 45–70.

[2] NordPass, "Top 200 most common passwords of the year 2020," 2021. [Online]. Available: https://nordpass.com/most-common-passwords-list/

[3] D. Malone and K. Maher, "Investigating the distribution of password choices," in *The 21st International Conference on World Wide Web*, 2012, pp. 301–310.

[4] Computer Emergency Response Team (CERT), "IN98.03: Password cracking activity," Software Engineering Institute, Carnegie Mellon University, USA, 1998.

[5] Imperva, "Consumer password worst practices," The Imperva Application Defence Center (ADC), USA, 2014.

[6] C. Shu, "Passwords for 32M twitter accounts may have been hacked and leaked," 2021. [Online]. Available: https://techcrunch.com/2016/06/08/twitter-hack/

[7] R. Shay, S. Komanduri, A. Suriti, P. Huh, M. L. Mazurek, S. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, "Designing Password policies for strength and usability," *ACM Transactions on Information and System Security*, vol. 18, no. 4, pp. 1–34, 2016.

[8] S. Komanduri, R. Shay, P. G. Kelly, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: Measuring the effect of password-composition policies," in *The SIGCHI Conference on Human Factors in Computing Systems*, 2011, pp. 2595–2604.

[9] H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, "Why older adults (don't) use password managers," in *The USENIX Security Symposium*, 2021, pp. 73–90.

[10] H. Y. Huang and M. Bashir, "Surfing safely: Examining older adults' online privacy protection behaviors," in *The Association for Information Science and Technology*, vol. 15, pp. 188–197, 2018.

[11] World Health Organisation (WHO), *Young People's Health - A Challenge for Society. Geneva*, Switzerland: World Health Organisation, 1986.

[12] H. Habib, P. Emani-Naeini, S. Devlin, M. Oates, C. Swoopes, L. Bauer, N. Christin, and L. F. Cranor, "User behaviors and attitudes under password expiration policies," in *The Fourteenth USENIX Conference on Usable Privacy and Security*, 2018, pp. 13–30.

[13] T. Hussain, K. Atta, N. Z. Bawany, and T. Qamar, "Password and user behavior," *Journal of Computers*, vol. 13, no. 6, pp. 692–704, 2017.

[14] D. T. Fredericks, L. A. Futcher, and K. L. Thomson, "Comparing student password knowledge and behaviour: A case study," in *The Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 2016, pp. 167–178.

[15] K. Bryant and J. Campbell, "User behaviours associated with password security and management," *Australasian Journal of Information Systems*, vol. 14, no. 1, pp. 80–100, 2006.

[16] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[17] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in *The Fourth International Conference on Network and System Security*, 2010, doi: 10.1109/NSS.2010.18.

[18] D. Florêncio and C. Herley, "Where do security policies come from?," in *The Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–14.

[19] S. Pearman, J. Thomas, P. Emani-Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, "Let's go in for a closer look: Observing passwords in their natural habitat," in *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 295–310.

[20] B. Grawemeyer and H. Johnson, "Using and managing multiple passwords: A week to a view," *Interacting with Computers*, vol. 23, no. 3, pp. 256–267, 2011.

[21] E. Stobert and R. Biddle, "The password life cycle: User behaviour in managing passwords," in *The Tenth USENIX Conference on Usable Privacy and Security*, 2014, pp. 243–255.

[22] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *2014 Network and Distributed System Security (NDSS) Symposium*, 2014, pp. 23–26.

[23] University of Illinois, "Why you should use different passwords," 2021. [Online]. Available: https://security.illinois.edu/content/why-you-should-use-different-passwords

[24] S. Bellovin, "Unconventional wisdom," *IEEE Security & Privacy*, vol. 4, no. 1, p. 88, 2006.

[25] P. A. Grassi, J. L. Penton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y. Y. Choong, K. K. Greene, and M. F. Theofanos, "NIST special publication 800-63B: Digital authentication guideline," *National Institute of Standards and Technology (NIST)*, USA, 2017.

[26] K. Helkala and T. H. Bakås, "Extended results of norwegian password security survey," *Information Management & Computer Security*, vol. 22, no. 4, pp. 346–357, 2014.

[27] M. Theofanos, Y. Y. Choong, and O. Murphy, "Passwords keep me safe' – Understanding what children think about passwords," in *The Thirtieth USENIX Security Symposium*, 2021, pp. 19–35.

[28] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "I added '!' at the end to make it secure: Observing password creation in the lab," in *The Eleventh USENIX Conference on Usable Privacy and Security*, 2015, pp. 123–140.

[29] Y. Y. Choong, M. F. Theofanos, and H. K. Liu, "NISTIR 7991: United States federal employees' password management behaviors - A department of commerce," *National Institute of Standards and Technology (NIST)*, USA, 2014.

[30] L. Ion, R. Reeder, and S. Consolvo, "No one can hack my mind: Comparing expert and non-expert

security practices," in *The Eleventh USENIX Conference on Usable Privacy and Security*, 2015, pp. 327–346.

[31] A. Barron, *Inference for Categorical Data, Introduction to Statistics*. USA: Yale University, 1997.